



Τ.Ε.Ι. ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

Προσεγγίζοντας την κυβερνοασφάλεια βάσει των απειλών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

της

ΒΛΑΧΟΠΟΥΛΟΥ ΕΛΕΝΗ

(ΑΜ:2012162)

ΕΠΙΒΛΕΠΩΝ: Ιωάννης Α. Πικραμμένος, Δρ. Μηχ. ΕΜΠ

ΣΠΑΡΤΗ, ΜΑΙΟΣ 2018



Τ.Ε.Ι. ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

Προσεγγίζοντας την κυβερνοασφάλεια βάσει των απειλών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

της

ΒΛΑΧΟΠΟΥΛΟΥ ΕΛΕΝΗ

(ΑΜ:2012162)

ΕΠΙΒΛΕΠΩΝ: Ιωάννης Α. Πικραμμένος, Δρ. Μηχ. ΕΜΠ

ΣΠΑΡΤΗ, ΜΑΙΟΣ 2018

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

"Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάση επιστημονικής παράφρασης.

Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων.

Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας."

Όνομα και Επώνυμο Συγγραφέα (Με Κεφαλαία): ΒΛΑΧΟΤΟΧΛΟΥ ΕΠΕΝΗ

Υπογραφή (Ολογράφως, χωρίς μονογραφή): Βλαχοτοχλού Επένη

Ημερομηνία (Ημέρα – Μήνας – Έτος): 21 Μαΐου 2018

ΕΥΧΑΡΙΣΤΙΕΣ

Με την εκπόνηση της πτυχιακής μου εργασίας ,η οποία αποτελεί την ολοκλήρωση
ενός σημαντικού κύκλου της ζωής μου, θα ήθελα να ευχαριστήσω τον επιβλέποντα
καθηγητή μου κ. Πικραμμένο Ιωάννη για την αμέριστη βοήθεια του και την
οικογένεια μου που με στήριξε καθ' όλη την διάρκεια αυτής της προσπάθειας.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜ'ΕΝΩΝ

1	Εισαγωγή	8
1.1	Πεδίο εφαρμογής	12
1.2	Ορισμός	12
1.3	Η ανάγκη για πολιτισμό στον κυβερνοχώρο	13
2	Δημιουργία επιχειρηματικής υπόθεσης για την εφαρμογή ενός προγράμματος CSC	14
3	Ανάπτυξη και εφαρμογή ενός επιτυχημένου προγράμματος CSC	16
4	Ένας οδηγός εφαρμογής για τα προγράμματα CSC	18
4.1	Σχέδιο βήμα προς βήμα για την εφαρμογή ενός προγράμματος CSC	19
4.1.1	Βήμα 1: Ρυθμίστε την κεντρική ομάδα εργασίας CSC	19
4.1.2	Βήμα 2: Επιχειρηματική κατανόηση και αξιολόγηση κινδύνου	20
4.1.3	Βήμα 3: Ορίστε τους κύριους στόχους, τα κριτήρια επιτυχίας και το κοινό-στόχο	22
4.1.4	Βήμα 4: Υπολογίστε την τρέχουσα κατάσταση και κάντε μια ανάλυση κενού ανάμεσα στην τρέχουσα κατάσταση και τους στόχους σας	22
4.1.5	Βήμα 5: Επιλέξτε μία ή περισσότερες δραστηριότητες	23
4.1.6	Βήμα 6: Εκτελέστε την επιλεγμένη δραστηριότητα	23
4.1.7	Βήμα 7: Επαναλάβετε τη μέτρηση της τρέχουσας κατάστασης και αναλύστε τα αποτελέσματα	24
4.1.8	Βήμα 8: Εξετάστε και εξετάστε τα αποτελέσματά σας πριν αποφασίσετε για την επόμενη ενέργεια	24
5	Οργανωτικές απαιτήσεις για μια επιτυχημένη CSC	25
5.1	Δημιουργία περιβάλλοντος ευαισθητοποίησης	26
5.2	Συναρμολόγηση ομάδας CSC	27
5.2.1	Ρόλοι και ευθύνες	28
6	Στοιχεία και πόροι για επιτυχημένα προγράμματα CSC	31
6.1	Βασικά στοιχεία για την κατασκευή προγραμμάτων CSC	31
6.1.1	Δραστηριότητες υλοποίησης CSC	31

6.2	Μέτρηση προγραμμάτων CSC	35
6.2.1	Διάφορες προσεγγίσεις για την ανάπτυξη της τρέχουσας κατάστασής σας	
	36	
6.2.2	'Καλές' έναντι 'κακές' μετρήσεις για τη μέτρηση της επιτυχίας	42
6.2.3	Παραδείγματα «καλών» μετρήσεων που χρησιμοποιούν οι οργανισμοί	44
7	Καλές πρακτικές από τις αναπτυγμένες πρωτοβουλίες CSC	47
7.1	Καλές πρακτικές που στοχεύουν διαφορετικά επίπτεδα αρχαιότητας σε έναν οργανισμό	47
8	Η περίπτωση για την εφαρμογή μιας κουλτούρας στον κυβερνοχώρο	50
8.1	Οικονομικό κόστος επιθέσεων και απειλών	50
8.2	Καθοδήγηση και αντίκτυπος πολιτικής	51
8.3	Νομικές πτυχές: υποχρεώσεις / ή κανονιστικές και νομικές πτυχές	53
8.4	Η σημασία των ανθρώπινων παραγόντων στην ασφάλεια του κυβερνοχώρου	55
9	Οργανωτικοί παράγοντες που επηρεάζουν τους πολιτισμούς στον κυβερνοχώρο	57
9.1	Οργανωτική κουλτούρα	57
9.2	Η ευρύτερη στρατηγική στον τομέα της ασφάλειας στον κυβερνοχώρο	58
9.3	Διασυνοριακή οργάνωση - οι ρόλοι που πρέπει να διαδραματίσουν οι διαφορετικές ομάδες	59
9.3.1	Ο ρόλος της ανώτερης διοίκησης	59
9.3.2	Ο ρόλος των CISOs	59
9.3.3	Ο ρόλος της μεσαίας διοίκησης	60
9.3.4	Ο ρόλος της πληροφορικής	61
9.3.5	Ο ρόλος της νομιμότητας / συμμόρφωσης	61
9.3.6	Ο ρόλος του ανθρώπινου δυναμικού	62
9.3.7	Ο ρόλος του μάρκετινγκ / των εσωτερικών επικοινωνιών	62
9.4	Εγκρίθηκαν επιχειρηματικά μοντέλα και μοντέλα απασχόλησης	63
10	Μη οργανωτικοί παράγοντες που επηρεάζουν τους πολιτισμούς στον κυβερνοχώρο	64

10.1 Ανθρώπινοι παράγοντες που επηρεάζουν τις καλλιέργειες ασφάλειας στον κυβερνοχώρο	65
10.1.1 Ψυχολογικοί παράγοντες	65
10.1.2 Συμμόρφωση και προσωπικότητα	66
10.1.3 Το κοινωνικό περιβάλλον	67
10.2 Εξωτερικοί παράγοντες	68
10.2.1 Εθνικοί πολιτισμοί	68
11 Υπάρχουσες πρακτικές και πόροι	69
11.1 Ευαισθητοποίηση, εκπαίδευση και επικοινωνία	69
11.1.1 Η σχέση μεταξύ του πολιτισμού της ασφάλειας στον κυβερνοχώρο και της ευαισθητοποίησης της ασφάλειας πληροφοριών	71
11.1.2 Εργαλεία, πλαίσια και μεθοδολογίες	71
11.1.3 Μέτρηση επιτυχημένης απόδοσης	73
12 Συστάσεις	75
13 Βιβλιογραφία	77

Περίληψη

Προκειμένου να συμβάλουμε στην προώθηση τόσο της κατανόησης όσο και της υιοθέτησης των προγραμμάτων Cyber Security Culture εντός των οργανισμών ,η παρούσα εργασία βασίζεται σε πολλαπλούς κλάδους ,συμπεριλαμβανομένων των οργανωτικών επιστημών ,της ψυχολογίας ,του δικαίου και της ασφάλειας στον κυβερνοχώρο. Συμπληρώνεται από τις γνώσεις και τις εμπειρίες που έχουν συγκεντρωθεί από τα υφιστάμενα προγράμματα CSC που εφαρμόζονται σε οργανισμούς και περιλαμβάνει καλές πρακτικές ,μεθοδολογικά εργαλεία και καθοδήγηση βήμα προς βήμα για όσους επιθυμούν να ξεκινήσουν ή να ενισχύσουν το δικό τους πρόγραμμα στον τομέα του πολιτισμού στον κυβερνοχώρο.

1 Εισαγωγή

Η έννοια της Πολιτιστικής Ασφάλειας (CSC) αναφέρεται στις γνώσεις, τις πεποιθήσεις, τις αντιλήψεις, τις νοοτροπίες, τις υποθέσεις, τους κανόνες και τις αξίες των ανθρώπων σχετικά με την ασφάλεια στον κυβερνοχώρο και τον τρόπο με τον οποίο εκδηλώνονται στη συμπεριφορά των ανθρώπων με τις τεχνολογίες της πληροφορίας. Το CSC περιλαμβάνει γνωστά θέματα, όπως τα πλαίσια ευαισθητοποίησης στον κυβερνοχώρο και την ασφάλεια των πληροφοριών, αλλά είναι ευρύτερο τόσο από πλευράς εφαρμογής όσο και από πλευράς εφαρμογής, με στόχο την ενσωμάτωση των καθηκόντων, των συνηθειών και της συμπεριφοράς του υπαλλήλου σε θέματα ασφάλειας των πληροφοριών, ενσωματώνοντάς τα στις καθημερινές τους ενέργειες.

Για να βοηθήσει στην προώθηση τόσο της κατανόησης όσο και της υιοθέτησης των προγραμμάτων CSC στους οργανισμούς, η έκθεση αυτή αντλεί από πολλαπλούς κλάδους, συμπεριλαμβανομένων των οργανωτικών επιστημών, της ψυχολογίας, του δικαίου και της ασφάλειας στον κυβερνοχώρο. Συμπληρώνεται από τις γνώσεις και τις εμπειρίες που έχουν συγκεντρωθεί από τα υφιστάμενα προγράμματα CSC που εφαρμόζονται σε οργανισμούς και περιλαμβάνει καλές πρακτικές, μεθοδολογικά εργαλεία και καθοδήγηση βήμα προς βήμα για όσους επιθυμούν να ξεκινήσουν ή να ενισχύσουν το δικό τους πρόγραμμα στον τομέα του πολιτισμού στον κυβερνοχώρο.

Υπάρχουν πολλοί οδηγοί πίσω από την άνοδο της CSC ως αναγνωρισμένη ανάγκη εντός των οργανισμών. Αντανακλά την αποδοχή ότι ο τρόπος με τον οποίο μια οργάνωση συμπεριφέρεται εξαρτάται από τις κοινές πεποιθήσεις, αξίες και ενέργειες των υπαλλήλων της και ότι αυτό συμπεριλαμβάνει τη στάση τους απέναντι στην ασφάλεια στον κυβερνοχώρο. Υπάρχει η αναγνώριση ότι οι εκοτρατείες ευαισθητοποίησης στον κυβερνοχώρο δεν παρέχουν, αφ

'εαυτής, επαρκή προστασία από τις εξελισσόμενες επιθέσεις στον κυβερνοχώρο. Υπάρχει επίσης η αναγνώριση ότι τα τεχνικά μέτρα ασφαλείας στον κυβερνοχώρο δεν υφίστανται σε κενό και πρέπει να λειτουργούν αρμονικά με άλλες επιχειρηματικές διαδικασίες, ώστε να αποφευχθεί η αδυναμία των εργαζομένων να επιλέξουν μεταξύ «να κάνουν τη δουλειά τους» ή «να κάνουν τη δουλειά τους», συμμορφώνονται με τις πολιτικές ασφάλειας ». Τέλος, πρόκειται για την απάντηση στην άποψη ότι οι άνθρωποι αντιπροσωπεύουν τον πιο αδύναμο κρίκο στις αλυσίδες ασφάλειας στον κυβερνοχώρο και αντικαθιστώντας το με ένα περιβάλλον όπου οι εργαζόμενοι γίνονται ισχυρά ανθρώπινα τείχη προστασίας από επιθέσεις στον κυβερνοχώρο.

Σε αυτό το πλαίσιο, έχει γίνει έρευνα στον τομέα του πολιτισμού στον τομέα της ασφάλειας στον κυβερνοχώρο, προκειμένου να παράσχει αυτή την καθοδήγηση, που εφαρμόζεται σε οργανισμούς ανεξάρτητα από τη δομή, το μέγεθος ή τη βιομηχανία. Αυτό επιτυγχάνεται με την παρουσίαση εργαλείων και πρακτικών σχεδιασμένων ώστε να είναι συμφραζόμενα με τις ανάγκες και τις περιστάσεις των μεμονωμένων οργανισμών. Παρόλο που απευθύνεται σε όσους απασχολούνται σε καθήκοντα ασφαλείας ή / και έχουν επιφορτιστεί με την αύξηση του ορίου ανθεκτικότητας στον κυβερνοχώρο όλων των εργαζομένων, η γλώσσα έχει δημιουργηθεί για να εξασφαλίσει ότι όλοι οι εργαζόμενοι, ανεξαρτήτως ρόλου ή αρχαιότητας, μπορούν να κατανοήσουν επαρκώς το τι απαιτείται να παράγουν και να ξεκινήσουν το δικό τους πρόγραμμα CSC. Περιλαμβάνονται οι ακόλουθοι πόροι:

- Ορθές πρακτικές που εντοπίστηκαν από εκείνες τις οργανώσεις που έχουν ήδη εφαρμόσει ώριμα προγράμματα CSC και συγκεκριμένα έχουν κατηγοριοποιηθεί και προσαρμοσθεί σε διαφορετικά ακροατήρια εντός ενός οργανισμού από ανώτερα στελέχη στην ομάδα ασφάλειας πληροφοριών.

- Για να διευκολυνθεί η ανάπτυξη και η υλοποίηση ενός προγράμματος για τον πολιτισμό στον κυβερνοχώρο, παρουσιάζεται ένα πλαίσιο υλοποίησης οκτώ σταδίων παράλληλα με λεπτομερείς οδηγίες για κάθε ένα από τα συστατικά βήματα. Το παρόν Πλαίσιο καλύπτει ολόκληρο τον κύκλο ζωής των προγραμμάτων πολιτισμού για τον πολιτισμό στον κυβερνοχώρο.
- Μέθοδοι για την παραγωγή μιας CSC για έναν οργανισμό, καθώς και οδηγίες για κατάλληλες μετρήσεις για τη μέτρηση του αντίκτυπου των δραστηριοτήτων CSC. και
- Στρατηγικές για την οικοδόμηση μιας ισχυρής επιχειρησιακής υπόθεσης για την κατανομή των εσωτερικών πόρων προς τις μελλοντικές δραστηριότητες στον τομέα του πολιτισμού στον τομέα της ασφάλειας στον κυβερνοχώρο.

Η μελέτη θα εντοπίσει ορθές πρακτικές, μεθοδολογικά εργαλεία και καθοδήγηση βήμα προς βήμα για όσους επιθυμούν να ξεκινήσουν ή να ενισχύσουν το δικό τους πρόγραμμα στον τομέα της πολιτιστικής ασφάλειας στον κυβερνοχώρο, περιλαμβανομένων πόρων για την παραγωγή επιχειρηματικών υποθέσεων για την εξασφάλιση χρηματοδότησης για ένα τέτοιο πρόγραμμα. Η επιτυχία ενός προγράμματος CSC βασίζεται σε ορισμένα βασικά στοιχεία, τα οποία προσδιορίζονται και περιγράφονται παρακάτω.

Συστάσεις για ένα επιτυχημένο πρόγραμμα CSC:

1. Εξασφαλίστε το buy-in στο υψηλότερο επίπεδο

Η ανώτερη αγορά στο υψηλότερο οργανωτικό επίπεδο είναι απαραίτητη για την επιτυχία του προγράμματος. Απαιτούνται ανώτερα αριθμητικά στοιχεία που μπορούν να λειτουργήσουν ως πρωταθλητές του προγράμματος και να οδηγήσουν σε

παράδειγμα επηρεάζοντας έτσι τη συμπεριφορά του προσωπικού προς το πρόγραμμα.

2. Ακολουθήστε το πλαίσιο CSC για την υλοποίηση του προγράμματος

Το πλαίσιο CSC που παρουσιάζεται στην παρούσα έκθεση παρέχει μια διαδικασία καθοδήγησης του προγράμματος CSC με τη μορφή μιας βήμα προς βήμα εφαρμογής επικεντρωμένης σε συγκεκριμένες δραστηριότητες, την εφαρμογή τους και τη μέτρηση των επιπτώσεων.

3. Γνωρίστε την οργάνωσή σας για να εξασφαλίσετε επιτυχία

Αυτό το βήμα στο πλαίσιο του CSC είναι το κλειδί για την επιτυχία του προγράμματος, διότι θα ενημερώνει τις διαδικασίες λήψης αποφάσεων που καθορίζουν τους στόχους, τα κριτήρια επιτυχίας και το κοινό-στόχο του προγράμματος CSC.

4. Μετρήστε το τρέχον επίπεδο ασφάλειας του κυβερνοχώρου του κοινού-στόχου

Ο υπολογισμός του τρέχοντος επιπέδου CSC του κοινού-στόχου σας θα σας βοηθήσει να μετρήσετε την επίδραση των δραστηριοτήτων που επιλέξατε να εφαρμόσετε και, συνεπώς, τον αντίκτυπο του προγράμματος CSC.

5. Σχεδιάστε τις καλές πρακτικές που προσδιορίζονται στην παρούσα έκθεση

Έχουν εντοπιστεί ορισμένες καλές πρακτικές από συνεντεύξεις με επαγγελματίες CSC σε οργανισμούς σε ολόκληρη την Ευρώπη και επιτόπια έρευνα που θα βοηθήσει στον σχεδιασμό και την εκτέλεση ενός επιτυχημένου προγράμματος CSC.

Καθώς οι επιχειρήσεις και τα άτομα υιοθετούν τεχνολογίες στις καθημερινές τους δραστηριότητες, το λογισμικό και οι τεχνικές λύσεις που προσπαθούν να μας προστατεύσουν από τις απειλές στον

κυβερνοχώρο έχουν πολλαπλασιαστεί. Ωστόσο, παρά τη συνειδητοποίηση των απειλών στον κυβερνοχώρο, των εξελίξεων στις τεχνολογίες στον κυβερνοχώρο, καθώς και του αυξημένου αριθμού εθνικών και οργανωτικών ομάδων αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT), για να συντονιστούν οι απαντήσεις, συνεχίζουν να αυξάνονται τόσο η συχνότητα όσο και το κόστος των παραβιάσεων δεδομένων. Οι άνθρωποι παραμένουν ο ασθενέστερος κρίκος στην αλυσίδα ασφαλείας και η επένδυση και η ανάπτυξη πολιτισμών στον τομέα της ασφάλειας του κυβερνοχώρου εντός των οργανισμών μπορεί να μειώσει τον κίνδυνο ανθρώπινου παράγοντα, προσδίδοντας θετικό αντίκτυπο στην αποτελεσματικότητα και την ασφάλεια, ενώ ταυτόχρονα μετριάζει τους οικονομικούς κινδύνους.

1.1 Πεδίο εφαρμογής

Αυτή η έκθεση απευθύνεται σε ανώτερα στελέχη για την παροχή καθοδήγησης και εργαλείων για την αλλαγή της αλλαγής του πολιτισμού εντός της οργάνωσής τους, δημιουργώντας και εφαρμόζοντας ένα εσωτερικό πρόγραμμα CSC. Το πλαίσιο βήμα προς βήμα που παρουσιάζεται στην Ενότητα 4 έχει σχεδιαστεί για να εφαρμόζεται και να προσαρμόζεται στις ανάγκες κάθε οργανισμού που επιδιώκει να αναπτύξει ένα πρόγραμμα CSC, ανεξάρτητα από το μέγεθος, τον τομέα ή τη δομή των οργανισμών.

1.2 Ορισμός

Ο πολιτισμός της ασφάλειας στον κυβερνοχώρο (CSC) των οργανώσεων αναφέρεται στις γνώσεις, τις πεποιθήσεις, τις αντιλήψεις, τις νοοτροπίες, τις υποθέσεις, τους κανόνες και τις αξίες των ανθρώπων σχετικά με την ασφάλεια του κυβερνοχώρου και τον τρόπο με τον οποίο εκδηλώνονται στη συμπεριφορά των ανθρώπων με τις τεχνολογίες της πληροφορίας. Το CSC έχει ως στόχο να καταστήσει τις

εκτιμήσεις ασφάλειας πληροφοριών αναπόσπαστο μέρος της δουλειάς, των συνηθειών και της συμπεριφοράς ενός εργαζομένου, ενσωματώνοντάς τις στις καθημερινές τους ενέργειες. Η υιοθέτηση της σωστής προσέγγισης για την ασφάλεια των πληροφοριών επιτρέπει σε μια ανθεκτική CSC να αναπτυχθεί φυσικά από τις συμπεριφορές και τις στάσεις των εργαζομένων προς τα πληροφοριακά περιουσιακά στοιχεία στην εργασία και ως μέρος της ευρύτερης οργανωτικής κουλτούρας της εταιρείας, η CSC μπορεί να διαμορφωθεί, να κατευθυνθεί και να μετατραπεί. Ωστόσο, τα επιχειρηματικά περιβάλλοντα αλλάζουν διαρκώς, επομένως οι οργανώσεις πρέπει να διατηρούν και να προσαρμόζουν ενεργά την CSC τους ως απάντηση στις νέες τεχνολογίες και απειλές, καθώς και στους μεταβαλλόμενους στόχους, διαδικασίες και δομές. Μια επιτυχημένη CSC διαμορφώνει τη σκέψη ασφαλείας του συνόλου του προσωπικού (συμπεριλαμβανομένης της ομάδας ασφάλειας), βελτιώνοντας την ανθεκτικότητα έναντι όλων των απειλών στον κυβερνοχώρο, ιδίως όταν ξεκινάει μέσω της κοινωνικής μηχανικής, αποφεύγοντας την επιβολή επαχθών μέτρων ασφάλειας που εμποδίζουν το προσωπικό να εκτελεί αποτελεσματικά τις βασικές επιχειρηματικές λειτουργίες.

1.3 Η ανάγκη για πολιτισμό στον κυβερνοχώρο

Η πλειονότητα των παραβιάσεων δεδομένων εντός των οργανισμών είναι αποτέλεσμα ανθρώπινων παραγόντων και ενώ οι πολιτικές για την ασφάλεια του κυβερνοχώρου είναι συνήθης μεταξύ των οργανισμών, οι εργαζόμενοι μπορούν να τις θεωρούν ως κατευθυντήριες γραμμές και όχι ως κανόνες. Ομοίως, οι τεχνολογίες δεν μπορούν να προστατεύσουν τους οργανισμούς εάν δεν είναι σωστά ενσωματωμένοι και χρησιμοποιηθούν. Σε αυτό το πλαίσιο, η ανάπτυξη μιας CSC επιτυγχάνει μια αλλαγή στη νοοτροπία, ενθαρρύνει την ευαισθητοποίηση σχετικά με την ασφάλεια και την αντίληψη κινδύνου και διατηρεί στενή οργανωτική κουλτούρα αντί να επιχειρεί να προάγει ασφαλή συμπεριφορά. Στα

επόμενα τμήματα θα εξεταστούν οι διάφορες πτυχές της ανάπτυξης μιας CSC.

2 Δημιουργία επιχειρηματικής υπόθεσης για την εφαρμογή ενός προγράμματος CSC

Αυτή η ενότητα παρουσιάζει στρατηγικές για όσους επιθυμούν να ξεκινήσουν ένα πρόγραμμα CSC στο πλαίσιο του οργανισμού τους και πρέπει να δημιουργήσουν μια επιχειρησιακή υπόθεση για την εξασφάλιση πόρων για αυτό το πρόγραμμα. Με διαφορετικά τμήματα και πρωτοβουλίες στο πλαίσιο ενός οργανισμού που όλοι ανταγωνίζονται για να έχουν πρόσβαση σε ένα περιορισμένο φάσμα οικονομικών και ανθρώπινων πόρων, όσοι επιδιώκουν να εφαρμόσουν ένα πρόγραμμα CSC θα πρέπει συχνά να δημιουργήσουν επιχειρηματική υπόθεση που να δικαιολογεί την κατανομή των πόρων. Για να βοηθήσουμε σε αυτή τη διαδικασία ενισχύοντας μια επιχειρησιακή υπόθεση CSC, εντοπίσαμε και παρουσιάσαμε τρεις πηγές αποδεικτικών στοιχείων που μπορούν να ενσωματωθούν. Αυτά είναι:

1. *Eυρύτερες τομεακές στατιστικές για τις τρέχουσες απειλές στον κυβερνοχώρο*

Διεξάγετε έρευνες για την εγκληματικότητα στον κυβερνοχώρο και την ασφάλεια στον κυβερνοχώρο στον τομέα σας, συγκεντρώνοντας εκθέσεις, δημοσιεύσεις και στατιστικά στοιχεία για να στηρίξετε καλύτερα την περίπτωσή σας. Πηγές για τέτοια στοιχεία περιλαμβάνουν: εθνικές ομάδες CERT, εθνικούς και διεθνικούς αστυνομικούς φορείς, φορείς βιομηχανίας, παρόχους ασφάλειας, ακαδημαϊκούς κύκλους κλπ. Μπορείτε επίσης να αντλήσετε ιστορίες πολυμέσων υψηλής προβολής, καθώς αυτά μπορούν να βοηθήσουν στην παρουσίαση πραγματικών περιπτώσεων. Επικεντρωθείτε στο να δείτε πώς ένας ισχυρός CSC κάνει τη διαφορά σας στον οργανισμό σας όσον αφορά: τη διαχείριση των κινδύνων, προβάλλοντας μια ισχυρή εξωτερική εικόνα, και την προστασία των στοιχείων του ενεργητικού και των δεδομένων του οργανισμού.

2. *Αποδεικτικά στοιχεία που αντλήθηκαν από την ομάδα ασφάλειας του κυβερνοχώρου σας*

Χρησιμοποιήστε αποδεικτικά στοιχεία που συλλέγονται από το τμήμα πληροφορικής σας ή / και την ομάδα ασφάλειας του κυβερνοχώρου (συμπεριλαμβανομένων των εξωτερικών παρόχων κυπριακής ασφάλειας εάν χρησιμοποιούνται). Αυτό περιλαμβάνει αναφορές και στατιστικά στοιχεία από: διακομιστές [cloud], εργαλεία ασφάλειας πληροφορικής και αρχεία καταγραφής. Παρουσιάστε τον αριθμό των επιτυχημένων και ανεπιτυχών επιθέσεων που εντοπίστηκαν στα πάγια

σας, τα οποία εντοπίστηκαν από τα μέτρα ασφαλείας που καλύπτουν τα επίπεδα. Όπου είναι δυνατό, να αναφερθεί το πλήρες κόστος αυτών των επιθέσεων (θυμηθείτε να συμπεριλάβετε τα έξοδα προσωπικού για την αποκατάσταση, τα κόστη, τα έμμεσα κόστη από τη χαμένη παραγωγή κ.λπ.).

- 3. Αυτοπαραληφθέντα αποτελέσματα μιας πρότυπης παρέμβασης CSC**
Εκτελέστε μια εκστρατεία μικρής κλίμακας χρησιμοποιώντας τους ελάχιστους πόρους: (1) επιλέξτε μια ενιαία επιχειρηματική μονάδα ως στόχο σας. (2) επιλέξτε μια ενιαία συμπεριφορά (π.χ. καταγραφή των υπολογιστών όταν δεν βρίσκονται στο γραφείο), καθορίστε τη γραμμή βάσης σας, (3) να εκτελεί μια δραστηριότητα CSC. (4) τότε μετράτε τυχόν αλλαγές για να καθορίσετε την επίπτωση. Χρησιμοποιήστε αυτήν την έξοδο στην επιχειρησιακή σας υπόθεση, κάνοντας το επιχείρημα ότι " με λίγα / καθόλου πόρους είχα την ικανότητα να επιτύχω την αλλαγή X, με περισσότερους πόρους που θα μπορούσα να επιτύχω τον αντίκτυπο Y "

Εάν συμπεριλάβετε μία, περισσότερες ή / και πρόσθετες στρατηγικές στην περίπτωση της επιχείρησής σας, θα εξαρτηθεί από το πλαίσιο του ίδιου του οργανισμού σας. Οι παράγοντες που πρέπει να λάβετε υπόψη εδώ είναι: πώς παρουσιάζονται και υποβάλλονται κανονικά σε αυτές οι περιπτώσεις στον οργανισμό σας? τη συνολική διαθεσιμότητα πόρων στον οργανισμό σας. και τη σημασία που αποδίδεται στην ασφάλεια στον κυβερνοχώρο. Εάν η πρόκληση της απόκτησης πόρων στον οργανισμό σας είναι μεγάλη, ίσως να θέλετε να συμπεριλάβετε όλες τις προσεγγίσεις που αναφέρθηκαν παραπάνω. Εφόσον το CS είναι ήδη στην ημερήσια διάταξη, ίσως αισθάνεστε ότι μια πιο ήπια προσέγγιση θα αρκεί και έτσι μπορείτε να επιλέξετε ποια προσέγγιση θα ακολουθήσετε. Οι αποφάσεις εδώ θα εξαρτώνται επίσης από τους πόρους σας (οικονομικό και χρόνο) και την πρόσβαση στα δεδομένα.

3 Ανάπτυξη και εφαρμογή ενός επιτυχημένου προγράμματος CSC

Η ανάπτυξη και η εφαρμογή ενός επιτυχημένου προγράμματος CSC μέσα στους οργανισμούς είναι ένα καθήκον που απαιτεί μια πολυεπίπεδη και διαφοροποιημένη προσέγγιση, στην οποία συμμετέχουν ανώτερα στελέχη καθώς και άλλοι υπάλληλοι. Η κουλτούρα εκτείνεται πέρα από την ευαισθητοποίηση για να συμπεριλάβει τη διαμόρφωση των πεποιθήσεων, των κανόνων, των αξιών. Απαιτεί την αμοιβαία κατανόηση μεταξύ των ανώτερων στελεχών, των εκτελεστικών φορέων και των εργαζομένων σε σχέση με το ρόλο που αναλαμβάνουν οι ρόλοι, οι ευθύνες και οι πρακτικές τους όσον αφορά την υπεράσπιση του εγκλήματος στον κυβερνοχώρο.

Ο πολιτισμός είναι επίσης μοναδικός σε κάθε οργανισμό και η δημιουργία ενός ισχυρού και βιώσιμου CSC απαιτεί μια σε βάθος γνώση του οργανισμού, του συνολικού πολιτισμού, των στρατηγικών, των πολιτικών, των πρακτικών και των διαδικασιών των εργαζομένων. Για να είναι επιτυχής, μια CSC πρέπει να ενσωματωθεί στην οργανωτική κουλτούρα και να λάβει υπόψη τις ανάγκες και τις πρακτικές των εργαζομένων. Εάν τα προγράμματα και οι δραστηριότητες της CSC καθίστανται υπερβολικά επαχθείς, υπάρχει κίνδυνος οι εργαζόμενοι να αντιστέκονται ή να αγνοούν τα μηνύματα, τις τεχνολογίες και τις πρακτικές της CS που εφαρμόζονται. Η CSC πρέπει να σχηματίζεται με τους υπαλλήλους, αντί να τους επιβάλλεται. Τούτου λεχθέντος, υπάρχει επίσης μια σαφής ανάγκη για ορατό και φωνητικό buy-in από τα ανώτερα στελέχη για να παρέχουν νομιμότητα και ένα σαφές μήνυμα για τη σημασία του προγράμματος CSC ενός οργανισμού.

Αυτή η ενότητα είναι αφιερωμένη στην παροχή πρακτικής καθοδήγησης σε εκείνους που επιδιώκουν να δημιουργήσουν μια ισχυρή CSC μέσα στην οργάνωσή τους. Αυτές οι κατευθυντήριες γραμμές βασίζονται στην υπάρχουσα βιβλιογραφία και καθοδήγηση στον τομέα της ασφάλειας στον κυβερνοχώρο και στη CSC, καθώς και στις γνώσεις και καλές πρακτικές που προκύπτουν από τις διαβουλεύσεις μας με τους εμπειρογνόμονες του CSC και τους υπαλλήλους με ευθύνες CSC σε διαφορετικούς οργανισμούς στην Ευρώπη.

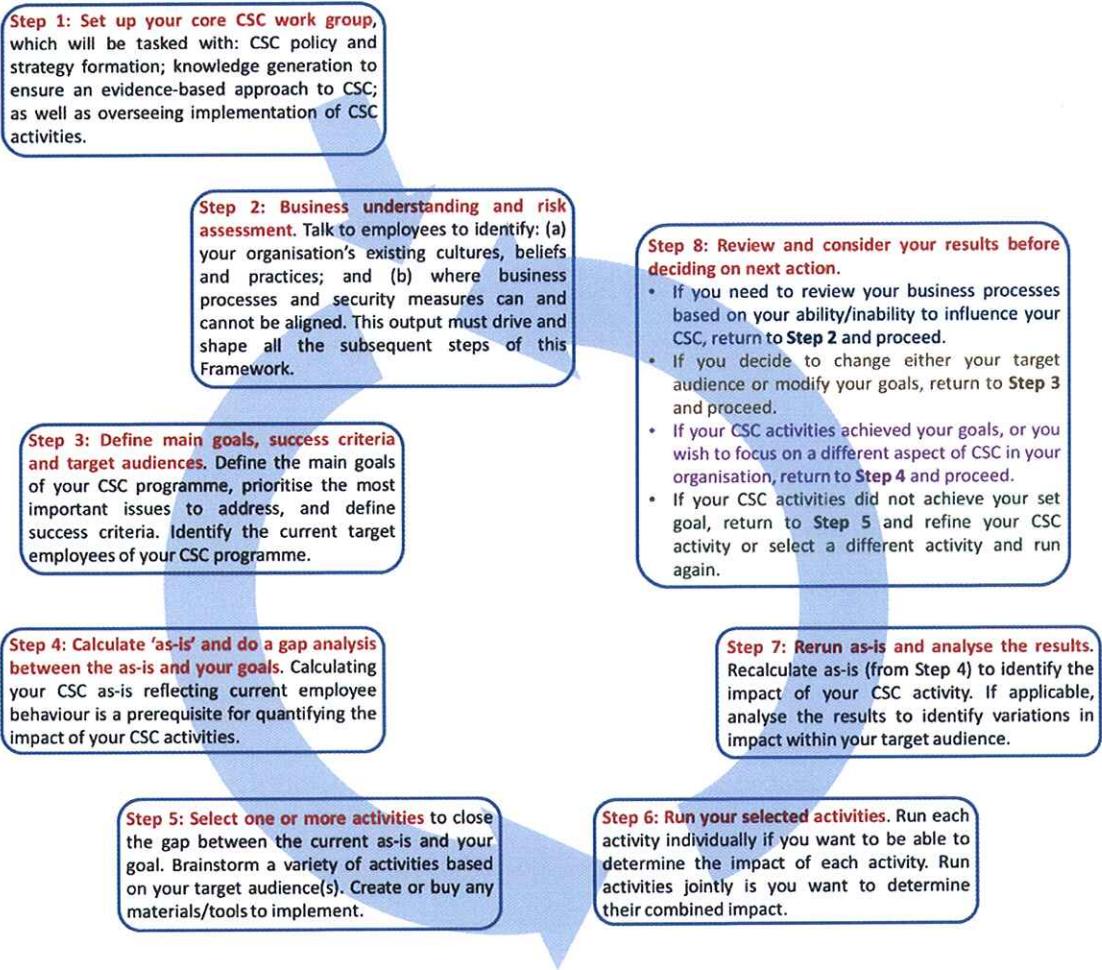
Κατά την ανάπτυξη αυτής της καθοδήγησης, η έρευνα αναγνωρίζει την εγγενή πρόκληση της παροχής μιας ενιαίας δέσμης κανονιστικών κανόνων σχετικής με όλους τους οργανισμούς, ανεξάρτητα από το μέγεθος, τον τομέα, την υπάρχουσα κουλτούρα ή / και την τοποθεσία τους. Δεν υπάρχει προσέγγιση "ενιαίου μεγέθους" όταν πρόκειται για το πιο αποτελεσματικό περιεχόμενο και μεθόδους παράδοσης για την εφαρμογή προγραμμάτων CSC εντός των οργανισμών. Ως αποτέλεσμα, εκτός από το Πλαίσιο Εφαρμογής, όλες οι οδηγίες που παρουσιάζονται παρακάτω σχεδιάζονται ειδικά για να προσαρμόζονται στις μοναδικές συμφραζόμενες ανάγκες κάθε οργανισμού που την απασχολεί. Ως εκ τούτου, παράλληλα με το Πλαίσιο εφαρμογής, παρέχουμε προαιρετικά στοιχεία για τη δημιουργία, την παράδοση και τη μέτρηση της επιτυχίας των προγραμμάτων CSC σας, τα οποία επιλέγονται και συνδυάζονται από την εσωτερική ομάδα υλοποίησης CSC με βάση την άψογη γνώση της δικής τους οργάνωσης.

Παρέχουμε ένα βήμα προς βήμα πλαίσιο / οδηγό για τη δημιουργία του προγράμματος CSC και εξηγείτε πώς να συγκεντρώσετε την ισχυρότερη δυνατή ομάδα εργασίας CSC. Και πάλι, αυτό θα διαφέρει σε κάθε οργανισμό, αλλά η εστίαση που δίνεται είναι στην απαραίτητη ικανότητα για κάθε μέλος, έτσι ώστε αν η ιεραρχία της οργάνωσής σας είναι διαφορετική, είναι σαφές ποια μέλη πρέπει να οδηγήσετε την εφαρμογή προς τα εμπρός.

Παρέχει έναν οδηγό για το πώς μπορείτε να δημιουργήσετε ένα περιβάλλον δεκτικότητας μέσα στον οργανισμό σας, το οποίο είναι επιτακτικό όταν πρόκειται να παραδώσει τα μηνύματα CSC και την εκπαίδευσή σας. Παρέχουμε τον κατάλογο των δραστηριοτήτων CSC και παρέχουμε δύο μεθόδους για την κατασκευή του σημερινού επιπέδου CSC πριν από την έναρξη οποιασδήποτε δραστηριότητας, έτσι ώστε οποιαδήποτε αλλαγή στον πολιτισμό να μπορεί να μετρηθεί με ακρίβεια. Επίσης, προσδιορίζουμε και παρουσιάζουμε μετρήσεις ορθής πρακτικής που θα σας επιτρέψουν να παρακολουθήσετε αυτή τη συμπεριφορική και πολιτισμική αλλαγή. Παρέχουμε καθοδήγηση σχετικά με τον τρόπο δημιουργίας μιας ισχυρής επιχειρησιακής υπόθεσης για την CSC για να εξασφαλιστεί η υποστήριξη από ανώτερα στελέχη και παρουσιάζει εντοπισμένες καλές πρακτικές για την οικοδόμηση μιας ισχυρής CSC εντός των οργανισμών.

4 Ένας οδηγός εφαρμογής για τα προγράμματα CSC

Αυτή η ενότητα παρέχει μια διαδικασία που καλύπτει τη δημιουργία και την υλοποίηση προγραμμάτων CSC με τη μορφή ενός βήμα προς βήμα πλαισίου εφαρμογής που επικεντρώνεται γύρω από συγκεκριμένες δραστηριότητες, την εφαρμογή τους και τη μέτρηση των επιπτώσεων. Η προσέγγιση είναι επαναληπτική κατά το ότι μετά από κάθε δραστηριότητα CS, μετράται ο αντίκτυπος, εξετάζονται τα αποτελέσματα και εξετάζεται η προσέγγιση. Μετά από αυτό, μπορούν να επιλεγούν νέες δραστηριότητες ή να τροποποιηθούν οι μέθοδοι παράδοσης. Αυτό δίνει επίσης την ευκαιρία να εξεταστούν και να τροποποιηθούν οι αρχικοί στόχοι ή / και το κοινό-στόχος.



Σχήμα: Βήμα-προς-βήμα πλαίσιο για τις οργανώσεις να εφαρμόσουν ένα πρόγραμμα CSC

Ενώ κάθε οργανισμός μπορεί να χρειαστεί να τροποποιήσει το Πλαίσιο Εφαρμογής για να καλύψει τις μοναδικές ανάγκες του πλαισίου του, τέτοιες τροποποιήσεις θα πρέπει να γίνονται με

προσοχή. Εάν απαιτούνται αλλαγές, σας συνιστούμε να ακολουθήσετε τις ακόλουθες οδηγίες:

1. Θα ενθαρρυνθεί η εισαγωγή οποιωνδήποτε πρόσθετων βημάτων και / ή διαδικασιών για την κάλυψη των αναγκών του οργανισμού εφαρμογής, εφόσον δεν υπονομεύουν τα υπάρχοντα βήματα.
2. Εκτός από τη μεταβολή της σειράς των Βημάτων 1 και 2, σας συμβουλεύουμε έντονα να μην υποβάλετε άλλες τροποποιήσεις στην τρέχουσα παραγγελία.
3. Μην μπείτε στον πειρασμό να παραλείψετε ή να αφαιρέσετε οποιοδήποτε από τα οκτώ βήματα που υπάρχουν. Κάθε ένα από αυτά τα βήματα εξυπηρετεί έναν συγκεκριμένο σκοπό για την ανάπτυξη ενός ισχυρού προγράμματος CSC.

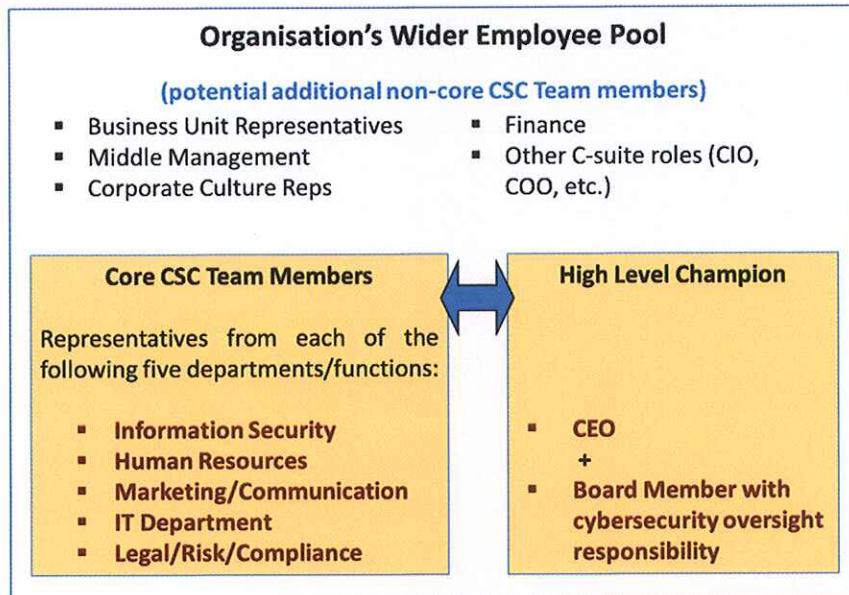
4.1 Σχέδιο βήμα προς βήμα για την εφαρμογή ενός προγράμματος CSC

Παρακάτω παρέχονται αναλυτικές πληροφορίες για κάθε μία από τις οκτώ βαθμίδες που ενσωματώνονται στο σχήμα. Όπως φαίνεται στο σχήμα, αυτή η διαδικασία είναι επαναληπτική / κυκλική, και όχι αυστηρά γραμμική. Μπορείτε κύκλο πίσω σε προηγούμενα βήματα στη διαδικασία όταν: βελτίωση των δραστηριοτήτων CSC? επιλογή νέων δραστηριοτήτων. επιλέγοντας νέα στοιχεία του CSC του οργανισμού σας για την αντιμετώπιση. επιλογή νέων υπαλλήλων στόχων ως εστία για τις δραστηριότητες CSC · και να τροποποιήσετε τους στόχους σας. Αυτές οι δυνατότητες απεικονίζονται στο σχήμα.

4.1.1 Βήμα 1: Ρυθμίστε την κεντρική ομάδα εργασίας CSC

Η ομάδα αυτή θα είναι επιφορτισμένη με τη δημιουργία γνώσεων για να εξασφαλίσει μια προσέγγιση βασισμένη στην τεκμηρίωση για τη ΣΕ, καθώς και τη διαμόρφωση του προγράμματος και της στρατηγικής CSC, την επίβλεψη της εφαρμογής των δραστηριοτήτων CSC και τη διασφάλιση της ευθυγράμμισης με την πολιτική του κυβερνοχώρου για την ασφάλεια στον κυβερνοχώρο. Η συγκέντρωση μιας ομάδας πυρήνων από πέντε συγκεκριμένους τομείς εντός ενός οργανισμού μεγιστοποιεί τη δυνατότητα μελλοντικής επιτυχίας του προγράμματος CSC αυτού του οργανισμού. Αυτή η βασική ομάδα απαιτεί επίσης την υποστήριξη της ανώτερης διοίκησης για την υποστήριξη του προγράμματος CSC. Η συμμετοχή στην κεντρική ομάδα παρουσιάζεται στο Σχήμα παρακάτω. Επιπλέον, μπορούν να

συμπεριληφθούν και άλλοι εκπρόσωποι από την ευρύτερη οργάνωση, ανάλογα με τον σχετικό χαρακτήρα του οργανισμού.



Σχήμα: Βασικά και μη μέλη της ομάδας εργασίας CSC

4.1.2 Βήμα 2: Επιχειρηματική κατανόηση και αξιολόγηση κινδύνου

Αυτό το βήμα περιλαμβάνει την κατανόηση των αξιών, των πολιτισμών, των πεποιθήσεων και των πρακτικών που ήδη υπάρχουν στην οργάνωσή σας και γιατί είναι εκεί. Αυτή η γνώση είναι πιθανόν διαθέσιμη σε κάθε τμήμα και ομάδα. Είναι σημαντικό να εξετάσετε τις διαφορετικές ανάγκες κάθε ομάδας / τμήματος και συγκεκριμένους ρόλους εργασίας, καθώς αυτοί μπορεί να διαφέρουν αρκετά σημαντικά και ίσως να υπάρχουν εμπόδια στην επιτυχία που δεν θα γνωρίζετε αν δεν συμβουλευτείτε τους υπαλλήλους.

Ένα σημαντικό στοιχείο αυτής της διαδικασίας για την *κατανόηση της επιχειρησής σας* είναι η χαρτογράφηση και η αξιολόγηση των τρεχόντων / μελλοντικών μέτρων ασφάλειας που εφαρμόζει η ομάδα ασφάλειας έναντι των διαδικασιών που πρέπει να αναληφθούν σε κάθε επιχειρηματική μονάδα, εάν οι υπάλληλοι αυτοί εκπληρώνουν τις απαιτήσεις των ρόλων τους. Αυτή η χαρτογράφηση και η σύγκριση της επιχειρηματικής διαδικασίας με τα μέτρα ασφάλειας θα επιτρέψουν στην ομάδα CSC να εντοπίσει πού:

1. *συνεργία υπάρχει* μεταξύ των επιχειρήσεων λειτουργίας και τα μέτρα ασφαλείας - σύμφωνα με την οποία τα μέτρα ασφαλείας δεν εμποδίζουν ή να επηρεάσει αρνητικά την εκτέλεση των επιχειρηματικών λειτουργιών;
2. *υπάρχουν συμβιβασμοί*, όπου τα μέτρα ασφαλείας επηρεάζουν αρνητικά την επιχειρηματική λειτουργία, ωστόσο, μέσω κάποιων

τροποποιήσεων σε αμφότερες τις δύο πλευρές μπορεί να επιτευχθεί μια λύση αποδεκτή και από τις δύο πλευρές.

3. *υπάρχουν συγκρούσεις*, όπου τα μέτρα ασφαλείας και οι επιχειρηματικές λειτουργίες δεν μπορούν να συνυπάρχουν καθώς το ένα αποτρέπει το άλλο.

Στην περίπτωση των στοιχείων (α) και (β), η επίτευξη συμμόρφωσης με τις πρακτικές στον τομέα της ασφάλειας στον κυβερνοχώρο με συνεργατικό τρόπο θα είναι εφικτή. Ωστόσο, στην περίπτωση του στοιχείου γ), ο οργανισμός θα πρέπει να αναλάβει την εκτίμηση κινδύνου και την ανάλυση κόστους-οφέλους για να καθορίσει εάν θα εγκαταλείψει το μέτρο ασφαλείας και θα αποδεχθεί ή να αντιμετωπίσει τον κίνδυνο με κάποιο άλλο τρόπο ή να εγκαταλείψει την επιχειρηματική πρακτική εάν ο κίνδυνος ασφαλείας είναι θεωρείται πάρα πολύ υψηλή. Αυτό αντιπροσωπεύει μια επιχειρηματική απόφαση και ίσως χρειαστεί να κλιμακωθεί στην *επιτροπή κινδύνων* των οργανισμών.

Αυτή η διαδικασία χαρτογράφησης για τον προσδιορισμό συνεργειών, συμβίβασμών και συγκρούσεων είναι θεμελιώδους σημασίας για την επιτυχία ή την αποτυχία κάθε μελλοντικού προγράμματος CSC. Εάν οι εργαζόμενοι βρίσκονται σε θέση να μην μπορούν να κάνουν τις δουλειές τους χωρίς να σπάσουν τους κανόνες / πολιτικές για την ασφάλεια στον κυβερνοχώρο, τότε η CSC εντός αυτού του οργανισμού είναι πιθανό να γίνει τοξική και ανθεκτική στην αλλαγή μέσω οποιουδήποτε μεταγενέστερου προγράμματος CSC. Αυτή η διαδικασία χαρτογράφησης ενθαρρύνει επίσης τη δέσμευση των δύο ομάδων μεταξύ της ομάδας ασφάλειας / πληροφορικής και των κέντρων κέρδους / επιχειρηματικών μονάδων, επιτρέποντας και στις δύο πλευρές να κατανοήσουν καλύτερα τις ανάγκες του άλλου, ενώ προσδιορίζει ζητήματα που απαιτούν στρατηγικές αποφάσεις και ιδιοκτησία από ανώτερα διευθυντικά στελέχη. Το CSC σας βοηθάει στην προστασία του οργανισμού σας, συνεπώς, κατά την ανάπτυξη των δραστηριοτήτων CSC, είναι σημαντικό να γνωρίζετε ποια περιουσιακά στοιχεία εγκληματών στον κυβερνοχώρο είναι πιθανό να αναζητήσουν. Για παράδειγμα, εάν διαθέτετε πολύτιμα δεδομένα, θα πρέπει να εστιάσετε σε αυτό συγκεκριμένα, αυτό θα απαιτήσει μια εις βάθος κατανόηση της τρέχουσας συλλογής δεδομένων, των εγκαταστάσεων επεξεργασίας και αποθήκευσης, των διαδικασιών εργασίας γύρω από τα δεδομένα, της φυσικής τοποθεσίας των εξυπηρετητών κ.λπ.

Η CSC πρέπει να ευθυγραμμιστεί με την τρέχουσα οργανωτική σας κουλτούρα και να αποφύγει να ενισχύσει τυχόν αδυναμίες. Επομένως, είναι σημαντικό να εξεταστεί με κριτικό πνεύμα η σημερινή κουλτούρα όσον αφορά τις δυνάμεις και τις αδυναμίες, ώστε να μπορούν να ληφθούν υπόψη. Ο πολιτισμός εξαρτάται από το πλαίσιο και είναι σύνθετος από ανθρώπους,

επικοινωνία, πρακτικές και τοποθεσία. Πρέπει να μιλήσετε με τους υπαλλήλους και να μάθετε για την καθημερινή τους εργασία και για το πώς η CSC μπορεί να ενταχθεί στις δραστηριότητές τους. Εάν η ΣΕ θεωρείται επιβάρυνση ή εμπόδιο, πιθανότατα θα αγνοηθεί από το προσωπικό.

4.1.3 Βήμα 3: Ορίστε τους κύριους στόχους, τα κριτήρια επιτυχίας και το κοινό-στόχο

Για κάθε οργανισμό, είναι σημαντικό να ορίσετε με σαφήνεια τους κύριους στόχους και τα συναφή κριτήρια επιτυχίας για να κρίνετε κατά πόσον πληρούνται αυτοί οι στόχοι σε σχέση με τη μελλοντική CSC του οργανισμού σας. Όταν το κάνετε αυτό, αναγνωρίστε ότι ορισμένοι από αυτούς τους στόχους θα έχουν καθολική εφαρμογή σε ολόκληρο τον οργανισμό, ενώ άλλοι θα απευθύνονται σε συγκεκριμένες ομάδες / ρόλους. Αυτή η διαδικασία ορισμού των στόχων και των συναφών κριτηρίων επιτυχίας θα βοηθήσει στον υπολογισμό της τρέχουσας κατάστασής σας CSC και στον καθορισμό των μετρήσεων στο Βήμα 4. Επίσης, ορίστε τις ομάδες-στόχους σας (π.χ. άλοι ή συγκεκριμένο τμήμα). Για μεγαλύτερους οργανισμούς που ξεκινούν την ανάπτυξη μιας CSC, ίσως είναι ευεργετικό να ξεκινήσετε εστιάζοντας σε ένα συγκεκριμένο κοινό-στόχο, πριν διευρυνθούν ώστε να συμπεριληφθούν όλα τα μέλη του προσωπικού.

4.1.4 Βήμα 4: Υπολογίστε την τρέχουσα κατάσταση και κάντε μια ανάλυση κενού ανάμεσα στην τρέχουσα κατάσταση και τους στόχους σας

Δεν μπορείτε να ποσοτικοποιήσετε τον αντίκτυπο των μελλοντικών σας προγραμμάτων CSC, εάν δεν καθορίσετε πρώτα την τρέχουσα κατάσταση (όπως είναι) που αντιπροσωπεύει το τρέχον επίπεδο CSC του στόχου σας. Ως εκ τούτου, εδώ υπολογίζετε την τρέχουσα κατάσταση και κάνετε μια ανάλυση κενού ανάμεσα στην τρέχουσα κατάσταση και τους στόχους σας. Υπάρχουν τρεις κύριες προσεγγίσεις (κάθε μία από τις οποίες εξετάζεται λεπτομερώς στο τμήμα 13.2, συμπεριλαμβανομένων των πλεονεκτημάτων και μειονεκτημάτων τους για να βοηθήσετε στη διαδικασία επιλογής σας):

- 1) Προσδιορίστε την τρέχουσα κατάστασή σας CSC ανεξάρτητα από τις παρεμβάσεις CSC
- 2) Καθορίστε την τρέχουσα κατάσταση CSC χρησιμοποιώντας τις μετρήσεις παρέμβασης CSC 3) Συνδυάστε τις προσεγγίσεις 1 και 2

Τοποθετώντας αυτό το βήμα στην ευρύτερη διαδικασία στο πλαίσιο αυτό, το σχέδιο είναι να δημιουργήσετε την τρέχουσα κατάσταση σε αυτό το βήμα και στη συνέχεια να επιλέξετε και να εκτελέσετε τις δραστηριότητές σας CSC στα βήματα 5 & 6 πριν επαναλάβετε την τρέχουσα κατάσταση στο βήμα 7. Μετά από αυτή τη διαδικασία θα σας επιτρέψει επίσης να μετρήσετε την επίδραση των δραστηριοτήτων που επιλέγετε να εφαρμόσετε.

4.1.5 Βήμα 5: Επιλέξτε μία ή περισσότερες δραστηριότητες

Οι δραστηριότητες που επιλέγετε πρέπει να συνδέονται με την τρέχουσα κατάσταση και τους στόχους σας και πρέπει να καθορίσετε τη σωστή τακτική που θα υιοθετήσετε κατά την επιλογή και την ανάπτυξη των δραστηριοτήτων σας. Για το σκοπό αυτό, υπάρχουν ερωτήματα που πρέπει να λάβετε υπόψη, συγκεκριμένα: σε ποια θέματα εστιάζετε; ποια είναι τα μηνύματά σας όταν αντιμετωπίζετε αυτά τα θέματα; και τι στοχεύετε (δηλαδή άνθρωποι, διαδικασίες ή τεχνολογίες); Επίσης, πρέπει να επιλέξετε τους διαμεσολαβητές / δραστηριότητες που πρόκειται να χρησιμοποιήσετε, για παράδειγμα: αλλαγές στις πολιτικές / διαδικασίες, αλλαγές λογισμικού, προγράμματα ευαισθητοποίησης (αφίσες, εκστρατείες ηλεκτρονικού ταχυδρομείου κ.λπ.) - συνεδρίες για εξάσκηση; σενάρια και παιχνίδια πολέμου χρησιμοποιώντας κίνητρα, κλπ. Κατά την επιλογή των δραστηριοτήτων, πρέπει να εξετάσετε τους περιορισμούς των πόρων σας - δηλαδή, μπορείτε να αγοράσετε τα απαιτούμενα υλικά / πόρους (off-the-shelf ή παραγγελία), μπορείτε να χρησιμοποιήσετε το εσωτερικό προσωπικό για να αναπτύξετε αυτό που χρειάζεστε να χρησιμοποιούν υπάρχοντα υλικά μέσα στον οργανισμό;

Θυμηθείτε, πάντα να επιλέγετε δραστηριότητες που ταιριάζουν στο οργανωτικό σας πλαίσιο και να αντιμετωπίσετε τα κενά που θέλετε να κλείσετε.

4.1.6 Βήμα 6: Εκτελέστε την επιλεγμένη δραστηριότητα

Εκτελέστε μια δραστηριότητα ξεχωριστά αν θέλετε να μπορείτε να προσδιορίσετε τον συγκεκριμένο αντίκτυπο αυτής της δραστηριότητας. Εκτελέστε δραστηριότητες μαζί ως κοινό σύνολο θέλετε να προσδιορίσετε τον συνδυασμένο αντίκτυπο αυτών των δραστηριοτήτων. Θα πρέπει να παρακολουθείτε στενά αυτές τις δραστηριότητες ενώ εκτελούνται για να διασφαλιστεί ότι εκτελούνται σωστά - θα πρέπει να επιλέξετε την καλύτερη

μέθοδο για την επίτευξη αυτού του στόχου με βάση το πλαίσιο τόσο της δραστηριότητας που τρέχει όσο και των πόρων του οργανισμού σας.

4.1.7 Βήμα 7: Επαναλάβετε τη μέτρηση της τρέχουσας κατάστασης και αναλύστε τα αποτελέσματα

Μετά την ολοκλήρωση της δραστηριότητας (ή των κοινών δραστηριοτήτων), πρέπει να επαναλάβετε τη μέτρηση CSC και να συγκρίνετε με την τρέχουσα κατάσταση και τους στόχους (Βήμα 4) και να αναλύσετε τα αποτελέσματα για να προσδιορίσετε τον αντίκτυπο (δηλαδή επίπεδα επιτυχίας και τυχόν αποτυχίες). Μπορείτε επίσης να χρησιμοποιήσετε αυτά τα αποτελέσματα για να προσδιορίσετε εάν οι θετικές / αρνητικές επιπτώσεις ήταν καθολικές σε ολόκληρο το κοινό-στόχο σας ή αν διέφεραν από διαφορετικά υποσύνολα του κοινού σας: π.χ. συγκεκριμένες ηλικιακές ομάδες, επιχειρηματικές μονάδες, χώρες, ρόλοι κλπ. Τα αποτελέσματα στη συνέχεια τροφοδοτούνται στο Βήμα 8.

Σημειώστε εδώ ότι η τροποποίηση της συμπεριφοράς των εργαζομένων και της συλλογικής KMA σε έναν οργανισμό είναι μια συνεχής διαδικασία. Αυτό πρέπει να λαμβάνεται υπόψη κατά την επιλογή του χρόνου επανεξέτασης της τρέχουσας κατάστασης και της συχνότητας αυτής της επανεξέτασης - δηλαδή, μπορείτε να επιλέξετε να πραγματοποιήσετε πολλαπλές επαναμετρήσεις σε διαφορετικές χρονικές περιόδους (π.χ. 1 μήνα, 3 μήνες, 12 μήνες, etc.) to understand how successful and resilient any behaviour modifications have been.

4.1.8 Βήμα 8: Εξετάστε και εξετάστε τα αποτελέσματά σας πριν αποφασίσετε για την επόμενη ενέργεια

Αυτό το βήμα είναι η ευκαιρία σας να αναθεωρήσετε τη στρατηγική σας, με βάση τα ευρήματά σας και τις εμπειρίες σας, και να καθορίσετε τον τρόπο με τον οποίο η CSC προχωράει προς τα εμπρός. Εάν οι δραστηριότητές σας CSC δεν πέτυχαν τους στόχους σας, επιστρέψτε στο Βήμα 5 και βελτιώστε τις δραστηριότητές σας ή επιλέξτε ένα διαφορετικό σύνολο δραστηριοτήτων και εκτελέστε ξανά. Εάν οι δραστηριότητες CSC σας επιτύχουν τους στόχους σας ή θέλετε να εστιάσετε σε μια διαφορετική πτυχή της CSC στον οργανισμό σας, επιστρέψτε στο Βήμα 4 και προχωρήστε. Εάν αποφασίσετε να αλλάξετε είτε το κοινό-στόχο σας είτε να τροποποιήσετε τους στόχους σας, επιστρέψτε στο Βήμα 3 και προχωρήστε. Εάν, με βάση την ικανότητά σας / την αδυναμία επηρεασμού της CSC του οργανισμού σας, θα πρέπει να

επανεξετάσετε τις επιχειρηματικές σας διαδικασίες ή / και τα μέτρα ασφαλείας, να επιστρέψετε στο Βήμα 2 και να προχωρήσετε.

5 Οργανωτικές απαιτήσεις για μια επιτυχημένη CSC

Η ανάπτυξη μιας ισχυρής CSC δεν είναι μια δραστηριότητα, αλλά είναι μάλλον μια συνεχής διαδικασία που πρέπει να καλλιεργηθεί συνεχώς, προκειμένου να ενσωματωθεί στην κουλτούρα του ευρύτερου οργανισμού. Απαιτεί buyin στο υψηλότερο οργανωτικό επίπεδο, με την δέσμευση του Διευθύνοντος Συμβούλου και άλλων ανώτερων στελεχών με την ευθύνη για την ασφάλεια να είναι επιτακτική. Από την άποψη αυτή, οι ανώτεροι υπάλληλοι πρέπει να δρουν ως πρωταθλητές για την CSC, οδηγώντας σε παράδειγμα, και αυτό θα πρέπει να υποστηριχθεί από την κατανομή των πόρων (ανθρώπινων και οικονομικών) για να ταιριάζει με το συγκεκριμένο έργο.

Ενώ το βασικό buy-in είναι απαραίτητο, η πρωτοβουλία για την ανάπτυξη ενός CSC μπορεί να προέλθει από οπουδήποτε εντός ενός οργανισμού. Οι διαφορετικές προσεγγίσεις έναρξης περιλαμβάνουν τα εξής:

- **Η προσέγγιση "από πάνω προς τα κάτω":** ξεκίνησε από το Δ.Σ., τον Διευθύνοντα Σύμβουλο και / ή το ανώτερο άτομο της C-suite με ευθύνη για την ασφάλεια στον κυβερνοχώρο.
- **Μεσοαστική προσέγγιση:** ξεκίνησε από τα μέσα διαχείρισης με ευθύνη για την ασφάλεια στον κυβερνοχώρο ή την εταιρική κουλτούρα (π.χ. CSO).
- **Προσέγγιση από κάτω προς τα πάνω:** ξεκίνησε από ένα άτομο σε μια επιχειρηματική μονάδα που αναγνωρίζει την ανάγκη.

Ωστόσο, ανεξάρτητα από το ποιος *αρχίζει* ένα πρόγραμμα CSC σε έναν οργανισμό, η *συνεχής επιτυχία* αυτών των προγραμμάτων εξαρτάται από ορισμένες κοινές απαιτήσεις. Πρώτον, ενώ τα προγράμματα CSC που αναπτύσσονται και λειτουργούν από ένα μόνο άτομο μπορεί να έχουν επιτυχία σε πολύ συγκεκριμένους τομείς, η προσέγγιση αυτή σπάνια επιτυγχάνει σε ολόκληρη την ευρύτερη οργάνωση. Πρέπει να συγκεντρώσετε τη σωστή ομάδα πολλαπλών τμημάτων με τις κατάλληλες ευθύνες για την ανάπτυξη και την παράδοση των προγραμμάτων, προκειμένου να είναι επιτυχημένα σε ολόκληρο τον οργανισμό. Δεύτερον, ενώ ο Διευθύνων Σύμβουλος /

Διοικητικός Σύμβουλος δεν χρειάζεται να ξεκινήσει πρόγραμμα CSC, χωρίς το ενεργό, φωνητικό τους στήριγμα, το πρόγραμμα πιθανότατα θα αποτύχει.

5.1 Δημιουργία περιβάλλοντος ευαισθητοποίησης

Μια αποτελεσματική CSC θα πρέπει να ενθαρρύνεται και να καλλιεργείται μέσα στην ευρύτερη οργανωτική κουλτούρα σε συνεργασία με τους εργαζόμενους, αντί να επιβάλλεται, εάν η αξία της ασφάλειας του κυβερνοχώρου πρέπει να γίνει αποδεκτή από όλα τα μέλη. Οι αλλαγές στο περιβάλλον εργασίας στον οργανισμό απαιτούν σαφείς ευθύνες και συμμετοχή όλων στον οργανισμό, συμπεριλαμβανομένου του ανώτερου διοικητικού στελέχους, προωθώντας την κυριότητα του προγράμματος και το κίνητρο για την τήρησή του. Η δέσμευση για την ασφάλεια στον κυβερνοχώρο θα πρέπει να σηματοδοτείται με επαρκή κατανομή του προϋπολογισμού και κίνητρο για μεγαλύτερη ασφάλεια από την απλή συμμόρφωση.

Η CSC μπορεί να είναι αποτελεσματική μόνο αν οι εργαζόμενοι έχουν τα εργαλεία, τις γνώσεις, τις δεξιότητες και την κατανόηση του ρόλου τους μέσα σε αυτό. Πρέπει επίσης να γίνει δεκτή η "κατάσταση με τον τρόπο που κάνουμε τα πράγματα", η οποία θα απαιτήσει ένα συνδυασμό προσεγγίσεων, που όλοι πρέπει να είναι οι άνθρωποι κεντρικοί. Ενώ το μήνυμα CSC πρέπει να προέρχεται από την κορυφή, είναι σημαντικό οι εργαζόμενοι να έχουν τη δυνατότητα να ανατροφοδοτούν το πώς μπορεί να προσαρμοστεί το CS στις τρέχουσες διαδικασίες εργασίας τους. Εάν το CSC εμποδίζει ή καθυστερεί την πρόοδο της εργασίας, τόσο πιο πιθανό είναι να αγνοηθεί. Οι εργαζόμενοι θα πρέπει να είναι σε θέση να γνωστοποιούν κάθε θέμα επάνω στην αλυσίδα έτσι ώστε να γίνουν τροποποιήσεις.

Η αφοσίωση και η συμμετοχή είναι ο βέλτιστος τρόπος για να υιοθετήσουν οι εργαζόμενοι μια πιο προσανατολισμένη προς τον CS συμπεριφορά. Η μάθηση πρέπει να ενθαρρύνεται μέσα σε ένα ασφαλές περιβάλλον για να αποφευχθούν παρεξηγήσεις και αμυντικές συμπεριφορές. Ο εξαναγκασμός θα πρέπει να αποφεύγεται και ο διάλογος θα πρέπει να ενθαρρύνεται - οι εργαζόμενοι θα πρέπει να μπορούν να υποβάλλουν ερωτήσεις και να λαμβάνουν βοήθεια καθώς αντιμετωπίζουν νέες διαδικασίες. Οι ανταμοιβές θα πρέπει να χρησιμοποιούνται για την ενίσχυση και την παρακίνηση της

ασφαλούς συμπεριφοράς και παράλληλα η παρακολούθηση και οι κυρώσεις μπορούν επίσης να λειτουργήσουν ως κίνητρα συμμόρφωσης. Για μια διαρκή αλλαγή πολιτισμού ένας συνδυασμός ανταμοιβής, σαφών ευθυνών και κανόνων ασφάλειας στον κυβερνοχώρο, οι οποίοι είναι και οι δύο ευθυγραμμισμένοι με τις επιχειρηματικές διαδικασίες και δεν έρχονται σε αντίθεση με άλλους κανόνες / διαδικασίες μη-ασφάλειας στον κυβερνοχώρο, είναι πιθανότερο να είναι επιτυχείς.

Όλο και περισσότερο, η εργασία εκτείνεται εκτός του χώρου εργασίας καθώς οι εργαζόμενοι ταξιδεύουν και εργάζονται από το σπίτι. Μία ισχυρή CSC θα πρέπει να κάνει το ίδιο και η CS θα πρέπει να παρουσιαστεί ως ένας «τρόπος ζωής» ως ο βέλτιστος τρόπος ενίσχυσης της προστασίας από επιθέσεις στον κυβερνοχώρο. Ο πολιτισμός υπονοεί επίσης ότι η εστίαση δεν αφορά αποκλειστικά την τεχνολογία και τους τρόπους με τους οποίους οι άνθρωποι συνδέονται με την τεχνολογία, αλλά και με τον τρόπο που σχετίζονται μεταξύ τους και συνεργάζονται και το πλαίσιο μέσα στο οποίο συμβαίνει αυτό. Το να τρέχετε προγράμματα ευαισθητοποίησης ή συμβάντα που αντιμετωπίζουν επίσης το CS στο σπίτι μέσω π.χ. με τη συμμετοχή μελών της οικογένειας μπορεί να είναι ένας καλός τρόπος για να σχηματιστεί μια καλή CSC που να εκτείνεται σε όλη τη δουλειά /

5.2 Συναρμολόγηση ομάδας CSC

Το πρώτο βήμα προεπεξεργασίας στη διαδικασία δημιουργίας μιας CSC μέσα σε έναν οργανισμό είναι η συγκέντρωση μιας ομάδας CSC. Ο συνδυασμός των μελών είναι σημαντικός καθώς θέλετε να διασφαλίσετε:

- Η νομιμότητα της προσέγγισής σας
- Η μακροζωία του προγράμματος
- Ότι φτάνετε σε όλα τα επίπεδα του οργανισμού
- Η τεχνολογική σας υποδομή είναι ενημερωμένη και αντικατοπτρίζει τις επιχειρηματικές ανάγκες των εργαζομένων

- 'Ότι ξέρετε τι είναι τα προτερήματά σας και πώς να τα προστατεύσετε
- 'Ότι δεσμεύετε τους υπαλλήλους και τους παρέχετε κατάλληλα και κατάλληλα εκπαιδευτικά υλικά • 'Ότι η προσέγγισή σας είναι συμβατή και νόμιμη

Ενώ οι διαφορετικές πραγματικότητες κάθε οργανισμού διαφέρουν (ανάλογα με το μέγεθος, την οργανωτική δομή, τις αρμοδιότητες που συνδέονται με τους ρόλους, τη γεωγραφική κατανομή, την υπάρχουσα κουλτούρα, τον επιχειρηματικό τομέα κλπ.), Οι επιτυχημένες ομάδες ανάπτυξης της CSC αποτελούνται συνήθως από ένα βασικό σύνολο ατόμων που ενδεχομένως συνοδεύονται από άλλα από όλη την οργάνωση. Το σχήμα 8 δείχνει τον πυρήνα και τα επιπρόσθετα άτομα. Σημειώστε ότι αυτή η δομή θα πρέπει να προσαρμοστεί ώστε να αντικατοπτρίζει την ειδική κατανομή ρόλων / αρμοδιοτήτων σε κάθε οργανισμό που εφαρμόζει.

5.2.1 Ρόλοι και ευθύνες

Ανώτερη Διοίκηση - Μέλος του διοικητικού συμβουλίου ή υψηλόβαθμο πρόσωπο για την υποστήριξη και τη σηματοδότηση της υποστήριξης του CS στο πλαίσιο του οργανισμού και τη διασφάλιση επαρκών πόρων (ανθρώπινων και οικονομικών) για τη δημιουργία και διατήρηση μιας ισχυρής CSC. Δημιουργία στρατηγικής και διασφάλιση ότι η στρατηγική και οι πολιτικές CSC ενσωματώνονται στη συνολική στρατηγική οργάνωσης. Δεδομένου ότι η διαχείριση της ασφάλειας και του κινδύνου αποτελεί ευθύνη των ανώτερων διοικητικών στελεχών, η παρουσία τους στην ομάδα πρέπει να διασφαλίζει ότι οι στρατηγικές και οι πολιτικές της ΕΣ περιλαμβάνονται στην ευρύτερη στρατηγική ασφάλειας και διαχείρισης κινδύνων. Τα ανώτερα στελέχη της διοίκησης μπορούν επίσης να βοηθήσουν στην ιεράρχηση προτεραιοτήτων για την ευθυγράμμιση με ευρύτερα οργανωτικά ενδιαφέροντα. Τα ανώτερα στελέχη της διοίκησης θα ανακοινώνουν επίσης στο ΣΕ το έργο της CS για να διασφαλίσουν ότι η CSC στα ανώτερα επίπεδα μετασχηματίζεται στην αύξηση της ευαισθητοποίησης σχετικά με την ασφάλεια κινδύνου και στην προετοιμασία για ταχείες αντιδράσεις στα γέλια και στα επεισόδια.

Τμήμα Πληροφορικής - να συνεισφέρουν την τεχνογνωσία τους στο CS και να εξασφαλίζουν ενημερωμένα τεχνικά μέτρα, τα οποία

είναι αποτελεσματικά, απλά και χρήσιμα για την υποστήριξη ασφαλών συμπεριφορών χωρίς να επιβαρύνουν. Η τεχνογνωσία του CS πρέπει να αποτελεί βασική αρμοδιότητα στην υπηρεσία πληροφορικής και πρέπει να χρησιμοποιείται ως συμβολή στη διαχείριση των κινδύνων, προσφέροντας πληροφορίες για τα ανώτερα στελέχη και τη λήψη αποφάσεων.

Ασφάλεια / Ασφάλεια Πληροφοριών (CSO, CISO) - τεχνογνωσία στην ασφάλεια των πληροφοριών, καλή διακυβέρνηση ασφαλείας, άνθρωποι και διαχείριση προόδου. Εάν ο οργανισμός διαθέτει CISO, διαδραματίζει καθοριστικό ρόλο στην ομάδα εργασίας, ευθυγραμμίζει τους στόχους της πληροφορικής και της ασφάλειας, συμμετέχει στην εκπόνηση της στρατηγικής και της πολιτικής της ΕΕ και εκπροσωπεί την ασφάλεια σε εκτελεστικό επίπεδο. Για τη διοίκηση και το διοικητικό συμβούλιο, η CISO θα πρέπει να παρέχει πληροφορίες σχετικά με την εξέλιξη της ασφάλειας, τους κινδύνους και τις πιθανές ενέργειες δράσης σύμφωνα με τις αρχές διαχείρισης κινδύνου. Για τους υπαλλήλους, η CISO παρέχει σαφή, κατανοητή και ανοιχτή επικοινωνία, αποδεικνύοντας ότι η ασφάλεια είναι τώρα μέρος του "τρόπου που κάνουμε πράγματα".

Ανθρώπινο δυναμικό - Παρέχει σύνδεση από τη διοίκηση προς τους υπαλλήλους και εποπτεύει όλες τις πρακτικές που αντιμετωπίζει το προσωπικό, όπως η ευαισθητοποίηση, η κατάρτιση και η επικοινωνία. Ο ΥΕ φέρνει επίσης στο τραπέζι τις γνώσεις σχετικά με τη συμπεριφορά του προσωπικού, τους διαφορετικούς ρόλους τους και ξέρει πώς να ενσωματώνει νέες πρακτικές μέσα στις ήδη καθιερωμένες διαδικασίες. Ο Υπατος Εκπρόσωπος μπορεί να διασφαλίσει ότι όλοι θα περάσουν από την ίδια εκπαίδευση και θα μπορούν να εποπτεύουν τις αξιολογήσεις, τα συστήματα παροχής κινήτρων ή τις πειθαρχικές κυρώσεις.

Νομική - να διασφαλιστεί ότι όλες οι νέες πρακτικές συμβάλλουν στην πλήρη συμμόρφωση της εταιρείας με την εθνική και διεθνή νομοθεσία, συμπεριλαμβανομένης της προστασίας δεδομένων. Η νομική υπηρεσία θα βοηθήσει επίσης να καθορίσει τι μπορεί να ζητηθεί από τους υπαλλήλους στο πλαίσιο των αρμοδιοτήτων των συμβάσεών τους και πώς να τροποποιήσουν τις συμβάσεις εάν χρειαστεί. Εάν κάποια από τις πρακτικές των ΣΕ συνεπάγεται την παρακολούθηση της συμπεριφοράς των εργαζομένων, η νομική υπηρεσία μπορεί να διαπιστώσει ότι οποιαδήποτε παρακολούθηση εμπίπτει στα όρια του νόμου.

Μάρκετινγκ / Επικοινωνίας - Καθώς η CSC αφορά την αλλαγή νοοτροπίας, αντιλήψεων και μεταβίβασης γνώσεων στους ανθρώπους, το Τμήμα Μάρκετινγκ / Επικοινωνιών θα υποστηρίξει την αλλαγή, σχεδιάζοντας και προωθώντας τα προγράμματα ευαισθητοποίησης και εκπαίδευσης του CS, αναπτύσσοντας αποτελεσματική επικοινωνία και διασφαλίζοντας την αποτελεσματική χρήση των μηνυμάτων και των καναλιών επικοινωνία. Μια ισχυρή CSC μπορεί επίσης να είναι μια ισχυρή ευκαιρία μάρκετινγκ για έναν οργανισμό, εμπνέοντας εμπιστοσύνη στους πελάτες και τους επιχειρηματικούς εταίρους, καθώς οι ανησυχίες για την AE αυξάνονται διεθνώς. Το τμήμα μάρκετινγκ μπορεί επίσης να δημιουργήσει ισχυρή CSC ως μέρος της οργανωτικής εικόνας, η οποία επίσης θα την ενισχύσει εσωτερικά.

6 Στοιχεία και πόροι για επιτυχημένα προγράμματα CSC

Αυτή η ενότητα καλύπτει τα στοιχεία και τις δραστηριότητες που απαιτούνται για την κατασκευή ενός επιτυχημένου προγράμματος CSC. Παραθέτουμε τις βασικές δραστηριότητες που απασχολούν σήμερα διάφοροι οργανισμοί και παρέχουν ορισμένες πληροφορίες σχετικά με τη χρήση τους. Όπως και με τα υπόλοιπα στοιχεία της υλοποίησης ενός προγράμματος CSC, η τελική επιλογή μεθόδων για την παράδοση των παρεμβάσεών σας CSC θα αποφασιστεί από την ομάδα υλοποίησης CSC, με βάση τις γνώσεις τους για το τι είναι πιο πιθανό να είναι αποτελεσματικό στον οργανισμό σας. Για παράδειγμα, εάν διαπιστώσετε ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου είναι ένας καλός τρόπος να προσεγγίσετε τους υπαλλήλους σας, χρησιμοποιήστε τα. Εδώ, η γνώση του οργανισμού σας είναι πρωταρχικής σημασίας για την επιλογή των κατάλληλων δραστηριοτήτων για το πρόγραμμά σας CSC. Σε αυτή την ενότητα συμβουλεύουμε επίσης τον υπολογισμό της τρέχουσας κατάστασης και την παραγωγή αποτελεσματικών μετρήσεων για τη μέτρηση του αντίκτυπου των δραστηριοτήτων σας στο CS.

6.1 Βασικά στοιχεία για την κατασκευή προγραμμάτων CSC

6.1.1 Δραστηριότητες υλοποίησης CSC

Οι οργανισμοί χρησιμοποιούν μια ποικιλία μεθόδων για την παροχή μηνυμάτων CS και κατάρτισης στους υπαλλήλους. Οι ηλεκτρονικές μέθοδοι, καθώς και οι μέθοδοι εκτός σύνδεσης και υβριδικών μέσων, μπορούν να χρησιμοποιηθούν για την αύξηση της ευαισθητοποίησης των εργαζομένων μεταξύ των εργαζομένων κατά τη δημιουργία μιας ισχυρής CSC. Η μέθοδος παράδοσης των μηνυμάτων CS θα πρέπει να επιλέγεται ειδικά για κάθε οργανισμό που ταιριάζει με την τρέχουσα κουλτούρα και τις μεθόδους επικοινωνίας. Αν είναι μια μικρότερη εταιρεία που δεν είναι ιδιαίτερα τεχνική στο επίκεντρο, μια προσέγγιση πρόσωπο με πρόσωπο μπορεί να είναι πιο κατάλληλη για τους εργαζόμενους, ενώ οι μεγαλύτερες εταιρείες με τεχνικά έμπειρο προσωπικό μπορεί να προτιμούν προγράμματα ηλεκτρονικής κατάρτισης και ευαισθητοποίησης. Θα πρέπει επίσης να εξετάσετε τους διαθέσιμους πόρους σας, το μέγεθος της οργάνωσης και τα πρότυπα εργασίας του προσωπικού κατά την επιλογή των

δραστηριοτήτων υλοποίησης CSC. Εάν είναι δυνατόν, πρέπει να επιλεγούν διαφορετικές μέθοδοι για να φτάσουμε όσο το δυνατόν ευρύτερα στο κοινό και να επιτραπούν διαφορετικά στυλ μάθησης.

ONLINE	ΥΒΡΙΔΙΟ	OFFLINE
<p>Τα μηνύματα ηλεκτρονικού ταχυδρομείου είναι ένας εύκολος τρόπος προσέγγισης σε όλους σε έναν οργανισμό. Μπορούν να χρησιμοποιηθούν για την παράδοση άμεσων μηνυμάτων CS από την κορυφή (ρύθμιση ατζέντας, προειδοποίησης για νέες απειλές κ.λπ.) ή χρησιμοποιούνται από το HR για την παράδοση νέων εκπαιδευτικών υλικών όπως βίντεο, παιχνίδια, φύλλα συμβουλών, ιστορίες και συχνές ερωτήσεις. Τα μηνύματα ηλεκτρονικού ταχυδρομείου είναι επίσης το εργαλείο παράδοσης για την προσδοκίωση επιθέσεων ηλεκτρονικού "ψαρέματος", οι οποίες θα αυξήσουν την ευαισθητοποίηση των εργαζομένων.</p> <p>Είναι χρήσιμο όλα τα υλικά να είναι επίσης διαθέσιμα στους εργαζόμενους (π.χ. σε ένα εταιρικό intranet) ώστε να μπορούν να ξαναεπισκεφθούν.</p> <p>Τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν εύκολα να παραβλεφθούν και</p>	<p>Εκτελέστε σενάρια, πρόβες, αμμοθίνες και ασκήσεις τυχερού παιχνιδιού .</p> <p>Εκτελέστε σενάρια / ασκήσεις με υπαλλήλους από ένα ή περισσότερα τμήματα για: να αυξήσετε την ετοιμότητα για κυβερνοχώρια. εντοπισμός παλαιότερων μη πραγματοποιημένων αποκλίσεων μεταξύ των διαδικασιών. προσδιορισμός των κινδύνων · αύξηση της εκτίμησης των αναγκών των διαφορετικών μονάδων. δημιουργούν συμπεριφορές / απαντήσεις που παράγονται [και ανήκουν] από το προσωπικό στις επιχειρησιακές μονάδες, αντί να επιβάλλονται από την ομάδα ασφαλείας.</p>	<p>1-2-1 ή ομαδικές εκπαιδευτικές συναντήσεις - όπως και με τα εργαστήρια, οι εκπαιδευτικές συνεδρίες είναι ένας καλός τρόπος για να δημιουργηθεί ένα περιβάλλον διαδραστικής μάθησης, όπου οι εργαζόμενοι μπορούν να μάθουν, να δοκιμάσουν τις δεξιότητές τους, να κάνουν λάθη και να κάνουν ερωτήσεις σε ένα ασφαλές περιβάλλον. Ενώ οι εκπαιδευτικές συναντήσεις ομάδας μπορούν να προσφέρουν εκπαίδευση για όλους τους υπαλλήλους, 1-2-1 συνεδρίες μπορούν να δώσουν ένα στοχοθετημένο μήνυμα για συγκεκριμένα άτομα που μπορεί να έχουν συγκεκριμένες ευθύνες σε σχέση με το CS.</p>

δεν είναι
αποτελεσματικά ως
μόνη μέθοδος για
την
ευαισθητοποίηση
του CS.

Τα βίντεο μπορούν να χρησιμοποιηθούν για σκοπούς κατάρτισης και ευαισθητοποίησης, Μπορούν επίσης να παρουσιάσουν ιστορίες ορθής πρακτικής για να αποδείξουν την αξία μιας σωστής απάντησης σε μια απειλή στον κυβερνοχώρο. Τα βίντεο μπορούν επίσης να περιλαμβάνουν συνομιλίες εσωτερικών ή εξωτερικών εμπειρογνώμονες ή υπάλληλοι με αρμοδιότητες στο ΣΕ	Οι ιστορίες της καλής πρακτικής των εργαζομένων αποτελούν έναν αποτελεσματικό τρόπο παροχής των κατάλληλων συμβουλών και μαθησιακού υλικού με τα οποία μπορούν να ταυτιστούν οι εργαζόμενοι. Οι ιστορίες μπορεί να περιλαμβάνουν μια απάντηση σε μια τρέχουσα απειλή, τα μέτρα που έλαβε ο υπάλληλος και ποιο ήταν το αποτέλεσμα. Οι ιστορίες μπορούν να εκτυπωθούν φυλλάδια ή αφίσες, όπως είπε σε βίντεο ή κατά τη διάρκεια της επιγραμμικής εκπαίδευσης.	Τα φυλλάδια , όπως και οι αφίσες, μπορεί να είναι αποτελεσματικά για την παροχή σύντομων και εύκολα αφομοιώσιμων πληροφοριών και συμβουλών για το CS. Μπορούν επίσης να περιέχουν συμβουλές, συχνές ερωτήσεις, διηγήματα και στοιχεία επικοινωνίας για την ομάδα CS. Τα φυλλάδια είναι ένας καλός τρόπος για να φτάσετε τόσο στο προσωπικό όσο και σε άλλους που επισκέπτονται τις εγκαταστάσεις σας (π.χ. πελάτες και πελάτες) επιχειρηματικοί εταίροι) και να διευρύνετε το κοινό του μηνύματός σας
Τα παιχνίδια χρησιμοποιούνται όλο και περισσότερο για την κατάρτιση και την εκπαίδευση και το CS δεν διαφέρει. Τα παιχνίδια και το παιχνίδι ρόλων διευκολύνουν την εμπλοκή, τη συμμετοχή και το άνοιγμα.	Προσφέρετε κίνητρα για να προωθήσετε την «καλή» συμπεριφορά και να αποθαρρύνετε την «κακή» συμπεριφορά. Αυτές δεν πρέπει να είναι μεγάλες ανταμοιβές (π.χ. εμπορικά προϊόντα, πιστοποιητικά δώρων κ.λπ.). Αυτά μπορεί να συνδέονται με τη συμπεριφορά του ατόμου ή τη συμπεριφορά ολόκληρων επιχειρηματικών μονάδων. Οι	Τα εργαστήρια επιτρέπουν ένα διαδραστικό περιβάλλον για τους υπαλλήλους να παρευρίσκονται, να λαμβάνουν εκπαίδευση / πληροφορίες και είναι επίσης σε θέση να υποβάλουν ερωτήσεις. Παίξτε γύρω με διαφορετικές μορφές και εστίαση - καλέστε εσωτερικούς και εξωτερικούς ομιλητές. Εξασφαλίστε ένα υποστηρικτικό και θετικό περιβάλλον,

	<p>διαγωνισμοί μπορούν να διεξαχθούν σε όλη την επιχείρηση με ανταμοιβές στην ομάδα / μονάδα με τις καλύτερες επιδόσεις.</p>	<p>ώστε οι εργαζόμενοι να αισθάνονται ασφαλείς να κάνουν ερωτήσεις και να κάνουν λάθη.</p>
<p>Τα σεμινάρια με εσωτερικούς ή εξωτερικούς εμπειρογνόμονες είναι ένας διαδραστικός και οικονομικός τρόπος για την αποστολή μηνυμάτων CS στους υπαλλήλους. Τα webinars μπορούν επίσης να αποθηκευτούν και να παρουσιαστούν σε ένα προστό μέρος (π.χ. το intranet της εταιρίας) για εκείνους τους εργαζόμενους που δεν μπορούν να παρακολουθήσουν ή να ξαναεπισκεφθεί πτυχές της ομιλίας.</p>	<p>Τα φύλλα συμβουλών είναι σύντομες λίστες που παρέχουν εύκολη πρόσβαση σε βασικές πληροφορίες σχετικά με το CS. Στόχος τους είναι να παρέχουν συμβουλές σχετικά με την αντιμετώπιση των απειλών στον κυβερνοχώρο με σαφή και συνοπτικό τρόπο. Αυτά μπορούν να εκτυπωθούν σε μορφή φυλλαδιών, ως αφίσες ή τοποθετημένα στο διαδίκτυο στο εταιρικό intranet.</p>	<p>Οι εκδηλώσεις που επικεντρώνονται στο γενικό CS, μια συγκεκριμένη απειλή, τα εργαλεία κατά του εγκλήματος στον κυβερνοχώρο επιτρέπουν μια πιο άτυπη προσέγγιση όπου οι άνθρωποι μπορούν να παρακολουθήσουν συνομιλίες, να πάρουν τυπωμένα υλικά στο σπίτι ή εμπορεύματα CS. Αυτά θα μπορούσαν να επεκταθούν και στις οικογένειες των εργαζομένων, των επιχειρηματικών εταίρων και των πελατών.</p>
<p>Τα σε απευθείας σύνδεση μαθήματα κατάρτισης είναι ένας καλός τρόπος για την κατάρτιση του CS. Τα μαθήματα μπορούν να σχεδιαστούν ως "κουβέρτα" μαθήματα για όλους τους υπαλλήλους και / ή συγκεκριμένες ομάδες-στόχους ανάλογα με τη δομή και την εστίαση της οργάνωσης.</p>	<p>Συχνές ερωτήσεις όπως τα φύλλα άκρων είναι ένας αποτελεσματικός τρόπος για να οργανώσετε τις πληροφορίες σε κείμενο με εύκολη πλοήγηση. Οι Συχνές Ερωτήσεις μπορούν να εκτυπωθούν ως φυλλάδια ή αφίσες ή να αναρτηθούν ηλεκτρονικά για τους υπαλλήλους μαζί με μια λειτουργία αναζήτησης.</p>	<p>Οι διαλέξεις εξωτερικών εμπειρογνωμόνων αποτελούν μια καλή ευκαιρία για μια ευρεία και ενημερωμένη κατανόηση των ζητημάτων και των τάσεων του CS.</p>
<p>Ο οργανισμός Intranet είναι ένα καλό μέρος για να επικοινωνήσετε με τους υπαλλήλους</p>	<p>Διεξάγετε «ψεύτικες επιθέσεις». Αυτά μπορεί να περιλαμβάνουν</p>	<p>Οι αφίσες μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς για να επισημανθούν οι CS</p>

<p>σχετικά με το CS και να επιτρέψετε την πρόσβαση σε CS υλικά (π.χ. βίντεο, συχνές ερωτήσεις</p>	<p>ηλεκτρονικές επιθέσεις με τη μορφή ψεύτικων ηλεκτρονικών μηνυμάτων ηλεκτρονικού "ψαρέματος" που αποστέλλονται στο προσωπικό, μέσω επιθέσεων εκτός σύνδεσης, όπου ελέγχονται οι φυσικοί έλεγχοι πρόσβασης (π.χ. είσοδος στις διαδικασίες κτιρίου, ή ψευδείς τηλεφωνικές κλήσεις απάτης CEO αναλαμβάνονται για να ελέγξουν την τήρηση των σωστών διαδικασιών και διαδικασιών.</p>	<p>μέσα σε έναν οργανισμό. Οι αφίσες μπορούν να περιλαμβάνουν συμβουλές, συμβουλές για καλούς πόρους, επισκόπηση των απειλών, παρουσίαση νέων απειλών, παροχή συμβουλών και στοιχείων επικοινωνίας κλπ.</p>
<p>Τα κοινωνικά μέσα μπορούν να είναι χρήσιμα για την επικοινωνία καλών συνηθειών CS, για ειδοποίηση για συγκεκριμένες απειλές, για καλές πρακτικές και χρήσιμους πόρους. Για να λειτουργήσει καλά, ο οργανισμός πρέπει να διαθέτει ισχυρές πρακτικές κοινωνικών μέσων και οι υπάλληλοι πρέπει να ακολουθούν τους λογαριασμούς του.</p>		

Σχήμα: Επιλογή των δραστηριοτήτων CSC για χρήση για την παροχή προγραμμάτων CSC

6.2 Μέτρηση προγραμμάτων CSC

Δεν μπορείτε να ποσοτικοποιήσετε τον αντίκτυπο των μελλοντικών σας προγραμμάτων CSC, αν δεν καθορίσετε πρώτα μια τρέχουσα κατάσταση που αντιπροσωπεύει το τρέχον επίπεδο CSC του στόχου σας. Αυτό ισχύει αν εστιάζετε σε ολόκληρο τον οργανισμό ή σε συγκεκριμένες επιχειρηματικές μονάδες / δημογραφικά στοιχεία μέσα στον οργανισμό σας.

Ο ευρύς χαρακτήρας της CSC, που αντικατοπτρίζεται στον ορισμό που παρέχεται στο τμήμα 1.1, σημαίνει ότι είναι αδύνατο να διαμορφωθεί μια CSC όπως βασίζεται στη μέτρηση μιας ενιαίας δράσης. Επομένως, για να δημιουργήσετε μια ποσοτικοποιήσιμη τρέχουσα κατάσταση, πρέπει να διαιρέσετε το CSC σε διαστάσεις / μετρήσεις που μπορούν να ποσοτικοποιηθούν και να επιλέξετε τις κατάλληλες μεθόδους συλλογής δεδομένων που πραγματικά μετρούν τις επιλεγμένες μετρήσεις. Η σημασία αυτού του τελευταίου σημείου δεν πρέπει να υποτιμηθεί, καθώς πρέπει να ληφθεί μέριμνα ώστε οι επιλεγμένες μετρήσεις να μετρήσουν πραγματικά τις πτυχές της CSC ενός οργανισμού. Οι προσεγγίσεις για την ανάπτυξη μιας τρέχουσας κατάστασης της CSC και καθοδήγηση για την επιλογή κατάλληλων μετρήσεων παρουσιάζονται παρακάτω.

6.2.1 Διάφορες προσεγγίσεις για την ανάπτυξη της τρέχουσας κατάστασής σας

Υπάρχουν τρεις διαφορετικές προσεγγίσεις που μπορούν να χρησιμοποιηθούν από έναν οργανισμό για την παραγωγή μιας τρέχουσας κατάστασης της CSC προ της θεραπείας πριν εφαρμόσουν τα επιλεγμένα προγράμματα: η μία είναι η μέτρηση της CSC ξεχωριστά από τις θεραπείες που χρησιμοποιείτε. το δεύτερο είναι να χρησιμοποιήσετε τις επιλεγμένες μετρήσεις των θεραπειών ως την τρέχουσα κατάσταση σας. ενώ το τρίτο είναι να ακολουθήσουμε και τις δύο προσεγγίσεις ένα και δύο μαζί. Και οι τρεις προσεγγίσεις χρησιμοποιούνται σε οργανισμούς που έχουν αναπτύξει ενεργά προγράμματα CSC. Έχουμε περιγράψει τα παρακάτω, μαζί με τα εγγενή οφέλη και τους περιορισμούς κάθε προσέγγισης. Πριν από την ανάπτυξη και την ανάπτυξη προγραμμάτων / θεραπειών CSC, η ομάδα εφαρμογής CSC θα πρέπει να αποφασίσει ποια προσέγγιση της τρέχουσας κατάστασης θα υιοθετήσει με βάση το συγκεκριμένο επιχειρησιακό τους πλαίσιο.

6.2.1.1 Προσέγγιση 1: Προσδιορίστε μια τρέχουσα κατάσταση CSC ανεξάρτητα από τις παρεμβάσεις σας CSC

Χρησιμοποιώντας αυτή την προσέγγιση, ο υπολογισμός μιας μέτρησης της τρέχουσας κατάστασης ή της βαθμολογίας CSC για τον οργανισμό σας επιτυγχάνεται με την εννοιοποίηση του CSC ως μία ή περισσότερες διαστάσεις που πρέπει να μετρηθούν μέσω μιας διαδικασίας συλλογής δεδομένων. Αυτή η βαθμολογία CSC

προσδιορίζεται ξεχωριστά στις παρεμβάσεις σας CSC, επομένως δεν είναι ένα βήμα που περιλαμβάνεται στον οδηγό εφαρμογής βήμα προς βήμα για τα προγράμματα CSC στην Ενότητα 2 (θα εμφανιστεί νωρίς στη φάση της προεπεξεργασίας). Αυτή η προσέγγιση χρησιμοποιεί την ακόλουθη διαδικασία:

- Βήμα 1: Συλλέξτε δεδομένα από / στο προσωπικό σας σχετικά με τις συμπεριφορές, τις στάσεις, την ευαισθητοποίηση κλπ. Και υπολογίστε μια τρέχουσα κατάσταση CSC.
- Βήμα 2: Ανάπτυξη και εφαρμογή των παρεμβάσεών σας CSC, χρησιμοποιώντας το Οπτικοποιητικό Πλαίσιο οκτώ σταδίων.
- Βήμα 3: Επαναμετρήστε την τρέχουσα κατάσταση CSC σας σε μελλοντικά διαστήματα για να προσδιορίσετε τις αλλαγές στα επίπεδα CSC του οργανισμού σας.

Ο καθορισμός της τρέχουσας κατάστασης CSC απαιτεί είτε την ανάπτυξη μιας εσωτερικής μεθοδολογίας για την εννοιοποίηση και τον υπολογισμό της CSC είτε τη χρήση εξωτερικών συμβούλων ή / και προϊόντων off-the-shelf για να επιτευχθεί αυτό για εσάς. 'Ενα παράδειγμα εκτός λειτουργίας είναι το κίτ εργαλείων ασφαλείας CLTRe που σπάει το CSC σε επτά διαστάσεις, μετρούμενο με ερωτηματολόγιο προσωπικού. Αυτές οι διαστάσεις αποτελούν μετρήσεις, με την ανάλυση των συλλεγόμενων δεδομένων που παρέχουν το αποτέλεσμα της συλλογής ασφαλείας του οργανισμού σας, τόσο ως συνολικό σύνολο όσο και ως τιμή για κάθε διάσταση που μπορεί να χαρτογραφηθεί σε ένα γράφημα αράχνης. Οι επτά μετρήσεις που χρησιμοποιούνται για τη μέτρηση της CSC στο πλαίσιο του Toolkit Security CLTRe παρουσιάζονται στο Σχήμα.

ΣΕ ΕΠΙΣΚΕΥΕΣ ΔΙΑΣΤΑΣΕΩΝ ΠΟΛΙΤΙΣΜΟΥ ΑΣΦΑΛΕΙΑΣ - ΤΟ ΠΛΑΙΣΙΟ ΑΣΦΑΛΕΙΑΣ

Συμπεριφορές : Πραγματικές ή προβλεπόμενες δραστηριότητες και ενέργειες ανάληψης κινδύνων από εργαζόμενους που έχουν άμεσο ή έμμεσο αντίκτυπο στην κουλτούρα ασφάλειας

Στάσεις: Τα αισθήματα και τα συναισθήματα των εργαζομένων σχετικά με τις διάφορες δραστηριότητες που σχετίζονται με την οργανωτική ασφάλεια

Γνώση: Ενημέρωση των εργαζομένων, επαληθεύσιμες γνώσεις και πεποιθήσεις σχετικά με τις πρακτικές, τις δραστηριότητες και την αυτο-αποτελεσματικότητα που σχετίζονται με την οργανωτική ασφάλεια

Συμμόρφωση: Συμμόρφωση με τις οργανωτικές πολιτικές ασφαλείας, συνειδητοποίηση της ύπαρξης τέτοιων πολιτικών και ικανότητα ανάκλησης της ουσίας τέτοιων πολιτικών

Επικοινωνία: Οι τρόποι επικοινωνίας των υπαλλήλων μεταξύ τους, η αίσθηση του ανήκειν, η υποστήριξη για ζητήματα ασφάλειας και η αναφορά περιστατικών

Πρότυπα: Οι αντιλήψεις για το τι είδους οργανωτική συμπεριφορά και πρακτικές που σχετίζονται με την ασφάλεια θεωρούνται φυσιολογικές από τους υπαλλήλους και τους συνομηλίκους τους και ποιες πρακτικές θεωρούνται ανεπίσημα ως αποκλίνοντες

Ευθύνες: Η συνειδητοποίηση της σπουδαιότητας του κάθε εργαζόμενου ως κρίσιμου παράγοντα για τη διατήρηση ή την καταστροφή της ασφάλειας του οργανισμού

Οφέλη: Αυτή η προσέγγιση παρέχει μια συνολική εικόνα / αξία CSC για τον οργανισμό σας ή / και τις επιχειρησιακές μονάδες που επιτρέπουν την απεικόνιση των μετατοπίσεων της CSC με την πάροδο του χρόνου. Επιπλέον, πολλοί οργανισμοί ή / και επιχειρηματικές μονάδες που χρησιμοποιούν το ίδιο τυποποιημένο μέσο μέτρησης CSC, επιτρέπουν συγκρίσεις τόσο μεταξύ όσο και εντός των οργανισμών και την ταξινόμηση των επιχειρήσεων / μονάδων - επομένως, η ομάδα υλοποίησης CSC θα μπορεί να εντοπίσει ισχυρότερες και πιο αδύναμες περιοχές τη στόχευση πόρων και προγραμμάτων.

Μειονεκτήματα: Αυτή η προσέγγιση δεν αναιρεί την ανάγκη ανάπτυξης πρόσθετων μετρήσεων για μεμονωμένες θεραπείες CSC - δηλαδή, πρέπει ακόμα να πραγματοποιήσετε μετρήσεις πριν και μετά τη θεραπεία με κατάλληλα επιλεγμένες μετρήσεις για κάθε πρόγραμμα CSC που εφαρμόζετε, διαφορετικά δεν μπορείτε να προσδιορίσετε την επίδραση μεμονωμένα προγράμματα. Επιπλέον,

τα εργαλεία μέτρησης που βασίζονται αποκλειστικά σε ερωτηματολόγια αυτοπροσδιορισμού επηρεάζονται από πολυάριθμες προκαταλήψεις (π.χ. εκτροπή επιλεκτικής αναφοράς, παροχή επιθυμητών απαντήσεων στην πραγματικότητα, μοτίβα ερωτήσεων κ.λπ.) · ενώ οι σχεδιαστές / διαχειριστές ερωτηματολογίων μπορούν να χρησιμοποιήσουν τεχνικές για την ελαχιστοποίηση αυτών των επιπτώσεων, δεν μπορούν να ολοκληρωθούν μετριοπαθείς. Τέλος, οι θετικές ή αρνητικές συσχετίσεις μεταξύ των συνολικών αποτελεσμάτων CSC και των επιδράσεων των θεραπειών CSC δεν συνεπάγονται αιτιώδη συνάφεια.

6.2.1.2 Προσέγγιση 2: Προσδιορίστε μια τρέχουσα κατάσταση CSC χρησιμοποιώντας τις μετρήσεις παρέμβασης CSC

Χρησιμοποιώντας αυτήν την προσέγγιση, αναπτύσσετε την τρέχουσα κατάσταση CSC σας ως μέρος του οδηγού εφαρμογής CSC βήμα προς βήμα, λαμβάνοντας τα αποτελέσματα των μετρήσεων πριν τη θεραπεία και χρησιμοποιώντας αυτά ως την τρέχουσα κατάσταση CSC. Αυτή η προσέγγιση χρησιμοποιεί τη φυσική εκδήλωση των σχετικών με την ασφάλεια του κυβερνοχώρου δραστηριοτήτων του προσωπικού ως την τρέχουσα κατάσταση της CSC αυτής της οργάνωσης. Αυτό συνεπάγεται τα ακόλουθα βήματα:

- Βήμα 1: Δημιουργήστε μια λίστα με τις μετρήσεις που σχετίζονται με τις δραστηριότητες στον τομέα της ασφάλειας στον κυβερνοχώρο του οργανισμού σας
- Βήμα 2: Υπολογίστε τις τιμές πριν από τη θεραπεία αυτών των μετρήσεων μέσω των μεθόδων συλλογής δεδομένων που είναι οι πλέον κατάλληλες. Αυτές οι αξίες αποτελούν την τρέχουσα κατάσταση σας CSC
- Βήμα 3: Ανάπτυξη και υλοποίηση των παρεμβάσεών σας CSC, χρησιμοποιώντας το Οπτικοποιητικό Πλαίσιο οκτώ σταδίων που περιγράφεται λεπτομερώς στην ενότητα 11.
- Βήμα 4: Επαναμετρήστε αυτές τις μετρήσεις υπολογίζοντας τις τιμές μεταγενέστερης θεραπείας για να καθορίσετε οποιεδήποτε αλλαγές στα επίπεδα οργανωτικής CSC.

Παράδειγμα εφαρμογής προσέγγισης 2:

Για να παραχθεί η βασική γραμμή CSC, η ομάδα υλοποίησης CSC στην Acme Inc. ξεκινά με την ανταλλαγή ιδεών με μια λίστα σχετικών μετρήσεων. Μερικά παραδείγματα από την ευρύτερη λίστα περιλαμβάνουν τα εξής:

- Τα γραφεία δεν έχουν εμπιστευτικά έγγραφα στο τέλος της ημέρας
- Οι [εικονικοί] υπολογιστές γραφείου του υπαλλήλου καταγράφηκαν όταν δεν βρίσκονταν στο γραφείο
- Δεν κάνετε κλικ σε συνδέσμους από μη αξιόπιστες εξωτερικές πηγές
- Σύμφωνα με τη διαδικασία αναφοράς για ύποπτες δραστηριότητες στον κυβερνοχώρο
- Αφού δημιούργησε τη λίστα μετρήσεων, η ομάδα υλοποίησης CSC προσδιορίζει τις κατάλληλες μεθόδους μέτρησης:
- Γραφεία εκτός από εμπιστευτικά έγγραφα στο τέλος της ημέρας: φυσική επιθεώρηση από το προσωπικό ασφαλείας ή τον επικεφαλής της ομάδας
- Οι [εικονικοί] επιτραπέζιοι υπολογιστές του υπαλλήλου καταγράφηκαν όταν δεν βρίσκονται στο γραφείο: αρχεία καταγραφής
- Κάνοντας κλικ σε συνδέσμους από μη αξιόπιστες εξωτερικές πηγές: χρησιμοποιούν ψεύτικα ηλεκτρονικά μηνύματα ηλεκτρονικού ψαρέματος (phishing)
- Μετά τη διαδικασία υποβολής εκθέσεων για ύποπτες δραστηριότητες στον κυβερνοχώρο: χρησιμοποιήστε ένα τρυπάνι επίθεσης ή διεξάγετε δοκιμή γνώσης σε απευθείας σύνδεση σχετικά με τη διαδικασία αναφοράς

Πριν από την ανάπτυξη και την εφαρμογή προγραμμάτων CSC που στοχεύουν σε αυτές τις μετρήσεις, η ομάδα υλοποίησης CSC διεξάγει μετρήσεις πριν από τη θεραπεία αυτών των μετρήσεων - τα αποτελέσματα της οποίας αποτελούν τη βασική γραμμή CSC της Acme Inc.

Οφέλη: Επιλέγοντας μετρήσεις με βάση συγκεκριμένες συμπεριφορές και στη συνέχεια πραγματοποιώντας μετρήσεις πριν και μετά τη θεραπεία, είναι ευκολότερο για την ομάδα εφαρμογής CSC να αποδείξει την αιτιώδη επίδραση των προγραμμάτων θεραπείας CSC. Κατά συνέπεια, αυτό επιτρέπει την τροποποίηση μελλοντικών προγραμμάτων βάσει των αποτελεσμάτων και οι αποδεδειγμένες επιπτώσεις μπορούν να αξιοποιηθούν για μεγαλύτερη κατανομή πόρων. Ο κατάλογος μετρήσεων που περιλαμβάνει την τρέχουσα κατάσταση της CSC μπορεί να προσαρμοστεί ώστε να αντανακλά το συγκεκριμένο πλαίσιο και τη σύνθεση ενός οργανισμού. Επιπλέον, εφαρμόζοντας τις ίδιες μεθόδους μέτρησης σε έναν οργανισμό, τα αποτελέσματα των διαφορετικών επιχειρηματικών μονάδων ή / και των υποσύνολων των εργαζομένων μπορούν να συγκριθούν από την ομάδα υλοποίησης της CSC για τον εντοπισμό ισχυρότερων και ασθενέστερων ομάδων για την προσαρμογή μελλοντικών θεραπειών.

Μειονεκτήματα: Αυτή η προσέγγιση μειώνει την CSC στις συγκεκριμένες συμπεριφορές που καλύπτονται από τις επιλεγμένες μετρήσεις και λαμβάνοντας υπόψη το ευρύ πεδίο συμπεριφορών, κανόνων, πεποιθήσεων, συμπεριφορών κ.λπ. που περιλαμβάνουν CSC, αυτή η παρούσα κατάσταση της CSC είναι πιθανό να αντιπροσωπεύει μόνο ένα υποσύνολο ευρύτερη CSC σε έναν οργανισμό. Ο εξατομικευμένος χαρακτήρας αυτής της προσέγγισης εμποδίζει τυποποιημένες συγκρίσεις της τρέχουσας κατάστασης CSC μεταξύ διαφορετικών οργανώσεων, καθιστώντας πιο δύσκολο τον προσδιορισμό του τρόπου σύγκρισης ενός οργανισμού με άλλους σε ένα παρόμοιο χώρο.

6.2.1.3 Προσέγγιση 3: συνδυασμός προσεγγίσεων 1 και 2

Δεδομένου ότι α) και οι δύο προηγούμενες προσεγγίσεις έχουν μοναδικά οφέλη και β) πολλά από τα μειονεκτήματα κάθε προσέγγισης αντιμετωπίζονται από το άλλο, η ομάδα υλοποίησης CSC μπορεί να επιλέξει να χρησιμοποιήσει και τις δύο προσεγγίσεις 1 και 2. Αν αυτή η τρίτη, υιοθετηθεί συνδυασμένη προσέγγιση, η ομάδα CSC μπορεί να επιλέξει να μετρήσει τη συνολική βαθμολογία CSC (όπως περιγράφεται στην προσέγγιση 1) σε περιοδική βάση (π.χ. ετησίως, δύο φορές ετησίως, κ.λπ.) για να παρέχει μια εικόνα υψηλότερου επιπέδου για το CSC του οργανισμού σας, ενώ

μετρώνται συγκεκριμένες συμπεριφορές στο πλαίσιο των συνεχιζόμενων δραστηριοτήτων σας CSC (ως περίγραμμα στην προσέγγιση 2).

6.2.2 'Καλές' έναντι 'κακές' μετρήσεις για τη μέτρηση της επιτυχίας

Οι μετρήσεις είναι απαραίτητες τόσο για την καθιέρωση της τρέχουσας κατάστασης της CSC όσο και για τη μέτρηση του αντίκτυπου των προγραμμάτων CSC. Κατά την επιλογή τέτοιων μετρήσεων, οι οργανισμοί αναγνωρίζουν ήδη την ανάγκη χρήσης εκείνων που σχετίζονται τόσο με το πλαίσιο της οργάνωσής τους όσο και με τους στόχους ασφαλείας του οργανισμού τους. Ωστόσο, εκτός από οποιεσδήποτε απαιτήσεις συμφραζομένων, είναι σημαντικό οι ομάδες υλοποίησης CSC να εκτιμήσουν ότι δεν μπορούν να αξιοποιηθούν όλες οι μετρήσεις που μετράνε την ασφάλεια στον κυβερνοχώρο για να μετρήσουν την κουλτούρα της ασφάλειας στον κυβερνοχώρο. Από την άποψη αυτή, για τον συγκεκριμένο σκοπό της μέτρησης της CSC, υπάρχουν τόσο μετρήσεις «καλής» όσο και «κακής» CSC:

- Μια **καλή** μέτρηση CSC είναι αυτή που λέει στον υλοποιητή κάτι πολύτιμο για την κουλτούρα της ασφάλειας στον κυβερνοχώρο μέσα σε έναν οργανισμό.
- Μια **κακή** μέτρηση CSC είναι αυτή που δεν παρέχει στον υλοποιητή πολύτιμες πληροφορίες σχετικά με την κουλτούρα ασφάλειας του οργανισμού στον κυβερνοχώρο, ανεξάρτητα από το αν σχετίζεται με την ασφάλεια στον κυβερνοχώρο.

Καλή και κακή μέτρηση στην πράξη:

Είναι αποδεκτή η ορθή πρακτική ότι οι οργανισμοί πρέπει να διαθέτουν πολιτική για την ασφάλεια στον κυβερνοχώρο, αλλά αυτές οι πολιτικές μπορούν να προσδώσουν αξία μόνο εάν οι εργαζόμενοι είναι εξοικειωμένοι με το περιεχόμενό τους. Ως αποτέλεσμα, το ISO στο Acme Inc. διεξάγει ένα ηλεκτρονικό εκπαιδευτικό πρόγραμμα για την εξοικείωση των εργαζομένων με την πολιτική. Επιθυμεί να μετρήσει τις επιπτώσεις επίγνωσης αυτού του προγράμματος που απαιτεί την επιλογή κατάλληλης μετρικής.

- Μια κακή μέτρηση εδώ είναι η μέτρηση του αριθμού των εργαζομένων που ανέλαβαν την κατάρτιση. Ενώ αυτό είναι μετρήσιμο, δεν παρέχει πληροφορίες σχετικά με το πόσο ευαισθητοποιημένοι είναι οι υπάλληλοι του πραγματικού περιεχομένου της πολιτικής για την ασφάλεια του κυβερνοχώρου της Acme.
- Μια καλή μέτρηση θα ήταν να δοκιμαστούν οι γνώσεις των εργαζομένων σχετικά με το περιεχόμενο αυτής της πολιτικής με τη διεξαγωγή προ- και μετα-δοκιμών σε κάθε πλευρά του ηλεκτρονικού εκπαιδευτικού προγράμματος, καθώς τα δεδομένα που συλλέγονται αφορούν άμεσα στην CSC της Acme Inc.

Εκτός από την απαίτηση ότι οι επιλεγμένες μετρήσεις παρέχουν πολύτιμες πληροφορίες για το CSC ενός οργανισμού, υπάρχει η πρακτική απαίτηση ότι η ομάδα υλοποίησης CSC πρέπει να είναι σε θέση να συλλέγει δεδομένα σχετικά με τις επιλεγμένες μετρήσεις, προκειμένου να πραγματοποιήσει τις απαραίτητες μετρήσεις πριν και μετά. Αυτή η πρακτική απαίτηση θα καθοριστεί με βάση την οργάνωση ανά οργανισμό, ανάλογα με τις δυνατότητες κάθε οργανισμού. Για να βοηθηθούν οι ομάδες υλοποίησης CSC εδώ, υπάρχει μια σειρά μεθόδων και φορέων που μπορούν να επιφορτιστούν με τη συλλογή δεδομένων μέτρησης. Αυτά περιλαμβάνουν τα ακόλουθα:

- Αξιοποίηση υπάρχουσας αναφοράς τεχνολογίας λογισμικού και υλικού: Αναφορές από διακομιστές, εργαλεία ασφάλειας IT και αρχεία καταγραφής. π.χ. τον αριθμό των επιθέσεων και τον αριθμό των παντελονιών που συλλέγονται από την ασφάλεια πληροφορικής και το λογισμικό προστασίας από ιούς.
- Αποστέλλει έρευνες με ερωτήσεις στους υπαλλήλους σχετικά με την ευαισθητοποίησή τους στον κυβερνοχώρο.

Αυτά αποτελούνται είτε από ποιοτικά ή ποσοτικά ερωτηματολόγια, είτε από ένα μείγμα και των δύο

- Αναφορά ασφαλείας: π.χ. αριθμός χαμένων / κλεμμένων συσκευών

- Αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου ηλεκτρονικού "ψαρέματος" (phishing) και εκστρατείες κακόβουλου λογισμικού (malware) για τη μέτρηση της απόκρισης των εργαζομένων, π.χ.
- Παρακολουθεί τις δραστηριότητες πληροφορικής των εργαζομένων εν γένει, ενώ ταυτόχρονα αναγνωρίζει τα όρια της ιδιωτικής ζωής. Εστίαση εδώ μπορεί να είναι περισσότερο σε επίπεδο ομάδας ή τμήματος για να αποφευχθεί η εστίαση της επιτήρησης σε συγκεκριμένα άτομα.

6.2.3 Παραδείγματα «καλών» μετρήσεων που χρησιμοποιούν οι οργανισμοί

Το σχήμα 11 κατωτέρω παρουσιάζει μια σειρά μετρήσεων που προέρχονται από υπάρχοντες πόρους / βιβλιογραφία και χρησιμοποιούνται επί του παρόντος από διάφορους οργανισμούς στο πλαίσιο των προγραμμάτων CSC τους που πληρούν τα «καλά κριτήρια» που προσδιορίζονται. Λάβετε υπόψη ότι δεν πρόκειται για εξαντλητική λίστα, ούτε προτείνουμε ότι θα πρέπει (ή μάλιστα θα πρέπει) να χρησιμοποιήσετε αυτές τις συγκεκριμένες μετρήσεις στα δικά σας προγράμματα CSC. Όπως συμβαίνει με όλες τις οδηγίες που παρουσιάζονται, πρέπει να κάνετε contextualisation της επιλογής των μετρήσεων με τον δικό σας οργανισμό και τις απαιτήσεις του CSC: δηλαδή οι μετρήσεις που σχετίζονται με τη μεταφορά των δικών σας συσκευών ή τη συντήρηση ενός καθαρού γραφείου έχουν νόημα μόνο αν οι συσκευές αυτές είναι ενεργοποιήσετε και διατηρείτε ένα γραφείο. Ομοίως, αν ο οργανισμός σας δεν έχει τη δυνατότητα να μετρήσει μια συγκεκριμένη συμπεριφορά που συνδέεται με μια μέτρηση (είτε λόγω τεχνικής, νομικούς ή οικονομικούς περιορισμούς), τότε η εν λόγω μέτρηση θα χρειαστεί να απορριφθεί.

ΠΙΘΑΝΕΣ ΜΕΤΡΙΚΕΣ ΓΙΑ ΤΗΝ ΚΑΘΟΡΙΣΜΟΣ ΤΗΣ ΤΡΕΧΟΥΣΑΣ ΚΑΤΑΣΤΑΣΗΣ ΚΑΙ ΤΗ ΜΕΤΡΗΣΗ ΤΗΣ ΕΠΙΤΥΧΙΑΣ ΤΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΤΗΣ CSC

Αριθμός / τοις εκατό των εργαζομένων που πέφτουν θύματα μιας ψεύτικης επίθεσης phishing.

Αριθμός / τοις εκατό των υπαλλήλων που ακολουθούν τις

διαδικασίες αναφοράς μετά την ανίχνευση μιας [ψευδούς] επίθεσης ηλεκτρονικού ψαρέματος.

1. Αριθμός / τοις εκατό των εργαζομένων που εμφανίζουν την κατανόηση των πολιτικών ασφαλείας, των διαδικασιών και των προτύπων

(που μπορεί να μετρηθεί μέσω δοκιμών)

2. Αριθμός / τοις εκατό των υπαλλήλων που εμφανίζουν ότι ενεργούν σύμφωνα με τις πολιτικές ασφαλείας, τη διαδικασία και το

(η ομάδα CSC μπορεί να επιλέξει να επιλέξει συγκεκριμένα στοιχεία από την πολιτική και να αναπτύξει κατάλληλα τα μέτρα δοκιμών)

Αριθμός / ποσοστό συσκευών που ενημερώνονται και είναι τρέχουσες σύμφωνα με την πολιτική

Αριθμός / τοις εκατό των συσκευών που είναι κρυπτογραφημένες σύμφωνα με την πολιτική του οργανισμού (μπορεί να επιλέξει να εστιάσει σε συγκεκριμένες συσκευές που χρησιμοποιούνται για τη φυσική μεταφορά δεδομένων - δηλαδή, μνήμες μνήμης, σκληρούς δίσκους κ.λπ.)

Αριθμός / τοις εκατό των εργαζομένων που εξασφαλίζουν το περιβάλλον γραφείου πριν από την αναχώρησή τους, ακολουθώντας έτσι την πολιτική των οργανισμών

Αριθμός / τοις εκατό των εργαζομένων των οποίων η δομή του κωδικού πρόσβασης ανταποκρίνεται στις απαιτήσεις του οργανισμού

Αριθμός / τοις εκατό των εργαζομένων που μπορούν να εντοπίσουν, να σταματήσουν και να αναφέρουν μια επίθεση κοινωνικής μηχανικής

Αριθμός / τοις εκατό των εργαζομένων που δημοσιεύουν ευαίσθητες οργανωτικές πληροφορίες σε ιστότοπους κοινωνικής δικτύωσης

Αριθμός / τοις εκατό των εργαζομένων που ακολουθούν

σωστά τις διαδικασίες καταστροφής δεδομένων

Αριθμός / τοις εκατό των υπαλλήλων που ακολουθούν την πολιτική φυσικής ασφάλειας για τον περιορισμό της πρόσβασης σε άτομα που δεν μεταφέρουν και εμφανίζουν έγκυρο δελτίο

Παράδειγμα μετρήσεων για χρήση στη ρύθμιση Τρέχουσα κατάσταση και μέτρηση των επιπτώσεων των δραστηριοτήτων CSC

7 Καλές πρακτικές από τις αναπτυγμένες πρωτοβουλίες CSC

Με βάση ένα συνδυασμό επιτόπιων αναλύσεων και συνεντεύξεων με επαγγελματίες CSC σε οργανισμούς σε ολόκληρη την Ευρώπη, εντοπίστηκαν ορισμένες καλές πρακτικές. Αυτά παρουσιάστηκαν παρακάτω, διαιρούμενα με δύο τρόπους με βάση το συγκεκριμένο κοινό-οτόχο.

7.1 Καλές πρακτικές που στοχεύουν διαφορετικά επίπεδα αρχαιότητας σε έναν οργανισμό

Το διάγραμμα παρουσιάζει τις αναγνωρισμένες ορθές πρακτικές, που οργανώνονται σύμφωνα με το επίπεδο αρχαιότητας των εργαζομένων στο πλαίσιο ενός οργανισμού, καλύπτοντας το φάσμα από το επίπεδο του διοικητικού συμβουλίου έως το μη διαχειριστικό επίπεδο.

ΣΤΟΧΕΥΜΕΝΟ ΚΟΙΝΟ	ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ
	Ορίστε την ασφάλεια στον κυβερνοχώρο ως σταθερό θέμα της ημερήσιας διάταξης στις συνεδριάσεις του διοικητικού συμβουλίου - υποδεικνύοντας έτσι την υποστήριξή σας προς την CSC στον ευρύτερο οργανισμό.
Επίπεδο Διοικητικού Συμβουλίου	Απαιτείται η απόλυτη υπευθυνότητα στον κυβερνοχώρο που έχει ανατεθεί σε έναν επαρκώς ανώτερο διευθυντή της C-suite που βρίσκεται είτε στο διοικητικό συμβούλιο είτε αναφέρεται απευθείας στο συμβούλιο.
	Να απαιτούν περιοδικές πληροφορίες τόσο για την κατάσταση της κουλτούρας στον τομέα της ασφάλειας στον κυβερνοχώρο εντός του οργανισμού όσο και για τα μέτρα και τους πόρους που διατίθενται για την προώθηση της διαμόρφωσης και διατήρησης αυτής της κουλτούρας.
Ανώτερα διοικητικά στελέχη	Να είστε μέλος της ομάδας εργασίας CSC για να μπορέσετε να προσφέρετε οδηγίες, να υποστηρίξετε σήματα, να βοηθήσετε στη στρατηγική και τη χάραξη πολιτικής και να εξασφαλίσετε επαρκείς πόρους
	Παρέχετε αναφορές κατάστασης μέχρι το διοικητικό συμβούλιο και κατευθύνετε οποιαδήποτε μηνύματα
	Να είναι ορατό στην υποστήριξή σας για το CS και να προωθήσετε το θέμα στις πρακτικές και την ομιλία σας. Αυτό συνεπάγεται επίσης τη διασφάλιση της ανώτερης

	<p>διοίκησης: αναλαμβάνει τουλάχιστον την ίδια εκπαίδευση ως προς το σύνολο του προσωπικού, είναι ένας πλήρης στόχος των δραστηριοτήτων της CSC και δεν αποδίδει ιδιαίτερες απολύσεις για να μην ακολουθήσει και να δεσμεύεται από τους ίδιους κανόνες με τους άλλους υπαλλήλους.</p>
	<p>Επικοινωνήστε και προωθήστε το CS στους υπαλλήλους σας, Βοηθήστε με τυχόν ερωτήματα.</p>
	<p>Εξασφαλίστε ότι οι εργαζόμενοι συμβουλεύονται και ακούνε στις ανησυχίες τους, μεταδίδοντας τα μηνύματά τους στην αλυσίδα στην ομάδα CSC. Με αυτόν τον τρόπο, μπορούν να γίνουν λύσεις για να συμπληρωθούν οι πρακτικές εργασίας τους.</p>
Μέση Διοίκηση	<p>Ελέγχετε τη συμπεριφορά CS και ελέγχετε τη συμμόρφωση.</p>
	<p>Να είστε φωνητικοί και προληπτικοί στο να προσδιορίσετε πού οι πολιτικές / πρακτικές της CS και άλλες επιχειρηματικές πολιτικές / πρακτικές διαφωνούν στην καθημερινή τους λειτουργία. Διατηρήστε αυτή τη στάση μέχρι να αλλάξει ή να αφαιρεθεί η πρακτική του CS ή / και η επιχειρηματική πρακτική - μια συνειδητή απόφαση που πρέπει να βασίζεται στην όρεξη του οργανισμού για κίνδυνο.</p>
	<p>Επικοινωνήστε με τα μηνύματα CS στον οργανισμό σας. Παρακολουθήστε εκδηλώσεις εκπαίδευσης και ευαισθητοποίησης και ακολουθήστε τις διαδικασίες του CS.</p>
Υπαλλήλους	<p>Εάν αισθάνεστε ότι οι λύσεις ή οι πρακτικές της CS παρεμποδίζουν την εργασία σας, μην τις αγνοείτε. Προσελκύστε τις ανησυχίες σας στον διαχειριστή της γραμμής σας.</p>
	<p>Προκαλέστε όσους δεν ακολουθούν ορθές διαδικασίες ασφαλείας.</p>

Ορθές πρακτικές που στοχεύουν σε διαφορετικούς ρόλους λειτουργικούς ρόλους μέσα σε έναν οργανισμό

Το Σχήμα παρουσιάζει αναγνωρισμένες ορθές πρακτικές, που στοχεύουν συγκεκριμένα τμήματα και ρόλους εντός ενός οργανισμού.

ΣΤΟΧΕΥΜΕΝΟ KOINO	ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ
Ασφάλεια	<p>Παρέχετε την εστίαση στην ασφάλεια και την εμπειρία στην ομάδα εργασίας CSC</p> <p>Εξασφαλίστε σαφή επικοινωνία ασφαλείας στους υπαλλήλους και σιγουρευτείτε ότι καταλαβαίνουν γιατί θα πρέπει να προσέχουν την ασφάλεια και το CS και τι ακριβώς αναμένεται από αυτούς.</p>

	<p>Βεβαιωθείτε ότι υπάρχει ένα σαφές σημείο επαφής στο εσωτερικό της επιχείρησής σας.</p>
	<p>Αναπτύξουν μια κατανόηση της οργάνωσης, δηλαδή, μιλήστε <i>με το</i> (όχι <i>σε</i>) οι διαφορετικές επιχειρηματικές μονάδες για να καταλάβει τι ακριβώς διαδικασία που πρέπει να αναλάβουν να κάνουν τη δουλειά τους, έτσι ώστε να συμφωνήσουν συλλογικά: (i) το οποίο διαδικασίες ασφάλειας <i>συμπληρώνουν</i> αυτές τις επιχειρηματικές διαδικασίες? (ii) όπου μπορούν να γίνουν <i>συμβίβασμοί</i> για την εξασφάλιση αποδεκτής εργασιακής αρμονίας μεταξύ της CS και των επιχειρηματικών διαδικασιών · και σε περίπτωση που υπάρχουν <i>συγκρούσεις</i> που δεν μπορούν να επιλυθούν, σε αυτήν την περίπτωση κλιμακώνεται αυτή η σύγκρουση στην κατάλληλη επιτροπή [κινδύνου], έτσι ώστε η επιχείρηση να αποφασίσει εάν θα εγκαταλείψει την επιχειρηματική πρακτική ή θα δεχτεί τον κίνδυνο να απομακρύνει το μέτρο του CS.</p>
Το τμήμα πληροφορικής	<p>Συμβάλλετε στην τεχνογνωσία σας στον τομέα πληροφορικής και τεχνολογίας των πληροφοριών στην ομάδα εργασίας της CSC.</p>
	<p>Δημιουργήστε ή εφαρμόστε υποστηρικτική υποδομή και τεχνολογία πληροφορικής που βοηθά τους εργαζομένους στην προστασία από την εγκληματικότητα στον κυβερνοχώρο.</p>
	<p>Βεβαιωθείτε ότι εφαρμόζονται τεχνολογίες που μπορούν να παρέχουν χρήσιμες γνώσεις σχετικά με τη συμπεριφορά και τις επιθέσεις CS, έτσι ώστε τα δεδομένα να μπορούν εύκολα να συγκεντρωθούν για ανάλυση και να ενσωματωθούν στο πρόγραμμα CSC.</p>
Ομάδα υλοποίησης CSC	<p>Βεβαιωθείτε ότι οι μετρήσεις και οι ρυθμίσεις της τρέχουσας κατάστασης έχουν οριστεί με ακρίβεια πριν ξεκινήσει οποιαδήποτε δραστηριότητα.</p>
	<p>Εξασφαλίστε σαφή επικοινωνία μέσα στην ομάδα CSC και μεταξύ της ομάδας και του υπόλοιπου οργανισμού.</p>
	<p>Αναλύστε τα συμπεράσματα μετά από κάθε κύκλο εφαρμογής, προκειμένου να τροποποιήσετε την προσέγγισή σας.</p>

8 Η περίπτωση για την εφαρμογή μιας κουλτούρας στον κυβερνοχώρο

8.1 Οικονομικό κόστος επιθέσεων και απειλών

Το οικονομικό κόστος των παραβιάσεων μπορεί να περιλαμβάνει τόσο το άμεσο κόστος (π.χ. απώλεια πνευματικής ιδιοκτησίας ή δεδομένα) όσο και το έμμεσο κόστος (π.χ. απώλεια φήμης ή / και ισχύος στην αγορά). Οι απώλειες μπορούν να λάβουν πολλαπλές μορφές, συμπεριλαμβανομένου του χρόνου διακοπής των υπηρεσιών, συμβιβασμό εμπιστευτικών πληροφοριών, πρόστιμα για παραβιάσεις προσωπικών δεδομένων (βλέπε παρακάτω) και μειωμένα κέρδη μέσω ζημιών στη φήμη. Το 2016, οι απώλειες πληροφοριών και εσόδων, μαζί με το κόστος των επιχειρηματικών διαταραχών, αντιπροσώπευαν το 95% των δαπανών παραβίασης.¹⁰

Αν και τα ακριβή αριθμητικά στοιχεία είναι δύσκολο να ποσοτικοποιηθούν, ιδίως οι απώλειες που οφείλονται στην άρνηση παροχής υπηρεσιών σε πελάτες, οι κυρώσεις στον κυβερνοχώρο μπορούν να οδηγήσουν σε μεγάλο κόστος και απώλειες. Μια αναφορά McAfee και Intel για το 2014 εκτιμά ότι το παγκόσμιο έγκλημα στον κυβερνοχώρο προκάλεσε απώλειες μεταξύ 325 και 500 δισ. Ευρώ. Ενώ το κόστος παραβίασης των δεδομένων ποικίλλει ανάλογα με τη χώρα και τη βιομηχανία, το 2017 το μέσο κόστος μιας παραβίασης δεδομένων ήταν € 3,14 εκατομμύρια, με κάθε χαμένο ή κλεμμένο αρχείο με ευαίσθητες ή εμπιστευτικές πληροφορίες που κοστίζουν € 122. Το κόστος μειώθηκε σε σύγκριση με το 2016, ωστόσο, το μέσο μέγεθος των παραβιάσεων δεδομένων αυξήθηκε κατά 1,8%, με κατά μέσο όρο 24,089 αρχεία που παραβιάστηκαν ανά χώρα ή περιοχή σε παγκόσμιο επίπεδο.

Οι αριθμοί των επιθέσεων έχουν αυξηθεί σημαντικά τα τελευταία χρόνια. Μεταξύ 2015 και 2016 εντοπίστηκε τετραπλασιασμός του όγκου των ανεπιθύμητων μηνυμάτων και των κακόβουλων συνημμένων¹² με 229.000 επιθέσεις να μπλοκάρονται καθημερινά το 2016. Καμία εταιρεία δεν είναι ασφαλής, ανεξάρτητα από το μέγεθός της, με το οικονομικό όφελος να είναι το μεγαλύτερο κίνητρο για cyberattacks το 2016. Οι απειλές στον κυβερνοχώρο είναι πλέον μια επιχειρηματική επιχείρηση, με αξιοσημείωτες εξελίξεις στον τομέα των ransomware μεταξύ 2015 και 2016 που χαρακτηρίζονται από την αύξηση της ποικιλομορφίας, τον αριθμό των ανιχνεύσεων και την

τετραπλάσια αύξηση του μέσου ποσού λύτρας που απαιτείται. Επιπλέον, η παγκόσμια έκθεση κινδύνου σε κυβερνοεπιθέσεις έχει αυξηθεί χάρη στις παγκόσμιες αλυσίδες αξίας με τις εταιρείες να εξαρτώνται όλοι και περισσότερο από το ένα το άλλο.

Θετικά, η γενικότερη ευαισθητοποίηση σχετικά με την ασφάλεια στον κυβερνοχώρο και τις επενδύσεις σε σύγχρονη τεχνολογία και πρακτικές μεταξύ όλων των διαδικτυακών φορέων μπορεί να αυξήσει την ασυλία όλων και να επιβραδύνει σημαντικά την εξάπλωση των απειλών στον κυβερνοχώρο. Αυτό υποδηλώνει ότι οι επενδύσεις στην CSC μπορούν να οδηγήσουν σε οικονομίες κλίμακας μεταξύ των χρηστών του Διαδικτύου και θα μπορούσαν ακόμη να θεωρηθούν ως μέρος της εταιρικής κοινωνικής ευθύνης μιας εταιρείας. Η ασφάλεια είναι σημαντική τόσο για τους πελάτες, όσο και για τις μεγαλύτερες οικονομικές συνέπειες των κυβερνοεπιχειρήσεων για τις επιχειρήσεις που χάνονται από τις επιχειρήσεις λόγω της πτώσης της εμπιστοσύνης των καταναλωτών, ιδίως στις ρυθμιζόμενες βιομηχανίες. Μια ισχυρή CSC μπορεί να χρησιμοποιηθεί για τη βελτίωση της εμπιστοσύνης, όχι μόνο εντός μιας επιχείρησης, αλλά και με πελάτες και επιχειρηματικούς εταίρους.

Τέλος, οι επενδύσεις σε τεχνολογίες και πρακτικές στον κυβερνοχώρο μπορούν να στηρίξουν την επιχειρηματική καινοτομία και να μειώσουν σημαντικά τόσο το κόστος όσο και τις απώλειες. Η επιχειρηματική καινοτομία μέσω της επέκτασης, της εξειδίκευσης ή της υιοθέτησης νέων τεχνολογιών είναι απαραίτητη για τη διατήρηση της ανταγωνιστικότητας και μια ισχυρή CSC που υιοθετεί ένα πρόγραμμα ευαισθητοποίησης είναι ο πιο αποδοτικός έλεγχος ασφάλειας για τη διαχείριση των κινδύνων ασφάλειας των νέων τεχνολογιών.

8.2 Καθοδήγηση και αντίκτυπος πολιτικής

Οι οργανισμοί δεν χρειάζεται να ενεργούν μόνοι τους όταν προωθούν την CSC τους. Ο δημόσιος τομέας μπορεί να βοηθήσει μέσω εκπαιδευτικών εκστρατειών, πρωτοβουλιών τυποποίησης και πιστοποίησης που μπορούν να επηρεάσουν τις δεξιότητες, τις γνώσεις και τα κίνητρα των ανθρώπων και των εταιρειών, διευκολύνοντας την ανάπτυξη της CSC.

Η εκπαίδευση είναι ένας τομέας στον οποίο η δημόσια πολιτική μπορεί να έχει ιδιαίτερη επίδραση. Πρόσφατες μελέτες έχουν επισημάνει μια παγκόσμια έλλειψη επαγγελματιών του κυβερνοχώρου, παρά τις υψηλές αμοιβές που προσφέρονται. Αυτό οδηγεί σε ανεπαρκή πόρους στον κυβερνοχώρο που οδηγεί σε αυξημένο άγχος και μακρές ώρες για επαγγελματίες πληροφορικής και μπορεί να προκαλέσει ανθρώπινα λάθη. Δεδομένου ότι οι ομάδες πληροφορικής και ασφάλειας σε έναν οργανισμό συμβάλλουν αποφασιστικά στο περιεχόμενο του μετασχηματισμού των πολιτικών, οι επενδύσεις στην εκπαίδευσή τους βρίσκονται στη βάση μιας καλής CSC.

Οι πρωτοβουλίες δημόσιας εκπαίδευσης μπορούν να υποστηρίξουν την ασφάλεια στον κυβερνοχώρο ως βασική πτυχή οποιασδήποτε εκπαίδευσης πληροφορικής και μπορούν να εξασφαλίσουν ότι οι νέες τεχνολογίες και πρακτικές αποτελούν μέρος αυτής και οι ειδικοί της πληροφορικής πρέπει να προσαρμοστούν στο νέο περιβάλλον του cloud computing, την αντιμετώπιση των επιπτώσεων και τη διαχείριση του κινδύνου πληροφόρησης. Ένα παράδειγμα δημόσιας υποστήριξης για την εκπαίδευση στον κυβερνοχώρο είναι η εθνική πρωτοβουλία για την εκπαίδευση στον κυβερνοχώρο του 2010 (NICE), με επικεφαλής το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) στις ΗΠΑ. Το πρόγραμμα NICE επικεντρώνεται στην ευαισθητοποίηση, την επίσημη εκπαίδευση, τη δομή του εργατικού δυναμικού, την κατάρτιση και την επαγγελματική ανάπτυξη για όλους και έχει δώσει προτεραιότητα: επιτάχυνση της μάθησης και ανάπτυξη δεξιοτήτων, διαφοροποίηση του εργατικού δυναμικού στον κυβερνοχώρο και την ανάπτυξη της σταδιοδρομίας και των προγραμματισμό του εργατικού δυναμικού των επαγγελματιών του κυβερνοχώρου.

Οι αντιλήψεις και οι γνώσεις του γενικού πληθυσμού μπορούν επίσης να επηρεαστούν μέσω εκπαιδευτικών πολιτικών και γενικών δηλώσεων αξίας, με σαφή πολιτική βούληση για ασφάλεια στον κυβερνοχώρο ικανό να αλλάξει τις εθνικές συμπεριφορές. Η ιεράρχηση της CSC στις εθνικές στρατηγικές στον τομέα της ασφάλειας στον κυβερνοχώρο και η προσφορά μη δεσμευτικών κατευθυντήριων γραμμών, έρευνας και ενημέρωσης στις επιχειρήσεις μπορούν να διευκολύνουν περαιτέρω την CSC, με τέτοιες εθνικές εκστρατείες που αποδεικνύονται ιδιαίτερα επωφελείς για τις ΜΜΕ.

Τα πρότυπα μπορούν επίσης να υποστηρίζουν την ανάπτυξη μιας CSC, καθώς μπορούν να παρουσιάσουν χρήσιμα πλαίσια για την ενσωμάτωσή τους στην CSC, επηρεάζοντας συγχρόνως τα κίνητρα της εταιρείας για την υλοποίηση ενός προγράμματος CSC. Τα πρότυπα μπορούν να καλύπτουν τόσο τεχνικές όσο και επιχειρησιακές πτυχές και μπορούν να καθοδηγήσουν διαχειριστές ασφάλειας και προσωπικό πληροφορικής σχετικά με σχέδια και στρατηγικές στον τομέα της ασφάλειας στον κυβερνοχώρο, καθώς και συγκεκριμένους ρόλους και ευθύνες. Τα υπάρχοντα δημοφιλή πρότυπα διαχείρισης της ασφάλειας καλύπτουν ήδη ευρείς τομείς, όπως: πολιτική ασφάλειας των πληροφοριών, επικοινωνιών και διαχείρισης λειτουργιών · οργάνωση της ασφάλειας των πληροφοριών · διαχείριση περιουσιακών στοιχείων; διαχείριση συμβάντων επιχειρηματική συνέχεια · την ασφάλεια των ανθρώπινων πόρων και τη συμμόρφωση.

Οι διεθνείς και εθνικές αρχές μπορούν να βοηθήσουν στην ανάπτυξη της CSC υιοθετώντας, προωθώντας και υποστηρίζοντας τα τρέχοντα βιομηχανικά πρότυπα, με βάση την ορθή και διεξοδική έρευνα των βέλτιστων πρακτικών. Παρόλο που τα πρότυπα είναι γενικά και καθολικά, οι οργανισμοί ενθαρρύνονται να προσαρμόζουν τις χρήσιμες πρακτικές ασφαλείας και τα πλαίσια στο δικό τους προφίλ κινδύνου και στις βιομηχανίες τους. Μια μελέτη του 2016 μεταξύ επαγγελματιών πληροφορικής και ασφάλειας στις ΗΠΑ διαπίστωσε ότι το 84% των οργανισμών είχε ήδη υιοθετήσει κάποιο πλαίσιο ασφάλειας για καθοδήγηση, με τα πιο δημοφιλή να είναι το πρότυπο του Συμβουλίου Ασφαλείας Δεδομένων (PCI), ISO / IEC 27001/27002 , Οι κρίσιμοι έλεγχοι ασφαλείας της KAK και το πλαίσιο NIST για τη βελτίωση της ασφάλειας στον κυβερνοχώρο. Επιπλέον, το 44% χρησιμοποίησε περισσότερα από ένα πλαίσια, καθώς οι οργανώσεις επωφελούνται από τα πλαίσια και προσαρμόζονται στις ανάγκες των οργανώσεων, των επιχειρηματικών μοντέλων και των επιχειρηματικών εταίρων.

Τέλος, η συμμόρφωση με αυστηρά πρότυπα μπορεί να χρησιμοποιηθεί για την επίτευξη πιστοποιήσεων. Τα πιστοποιητικά μπορούν να αποδείξουν την ασφάλεια και την αξιοπιστία σε πιθανούς επιχειρηματικούς εταίρους και πελάτες και μπορούν να ενθαρρύνουν την τήρηση των προτύπων, προωθώντας έτσι μια CSC. Οι εθνικές και διεθνείς αρχές μπορούν έτσι να χρησιμοποιήσουν πρότυπα για να υποστηρίξουν την ανάπτυξη της CSC εντός των οργανισμών.

8.3 Νομικές πτυχές: υποχρεώσεις / ή κανονιστικές και νομικές πτυχές

Οι κανονιστικές πτυχές μπορούν να επηρεάσουν τον τρόπο με τον οποίο μια εταιρεία αναπτύσσει την CSC και, λαμβάνοντας υπόψη τις αυξανόμενες επιθέσεις στον κυβερνοχώρο και την προστασία της ιδιωτικής ζωής, πρέπει να προετοιμαστεί ο ρυθμιστικός κίνδυνος αλλαγών στη νομοθεσία, καθώς ενδέχεται να προκύψουν νέα διοικητικά βάρη. Ο κανονισμός μπορεί να επιβάλει πρόσθετες δαπάνες στις επιχειρήσεις και ο επακόλουθος σχεδιασμός, η εκτέλεση, η τεκμηρίωση και η ενημέρωση των πολιτικών ασφαλείας πρέπει να αντιστοιχούν στις ρυθμιστικές ευθύνες των εταιρειών έναντι των πελατών τους, των εργαζομένων και των επιχειρηματικών εταίρων.

Η νομοθεσία μπορεί επίσης να υποχρεώσει την τυποποίηση των προγραμμάτων ασφαλείας από συγκεκριμένους οργανισμούς. Για παράδειγμα, η οδηγία του 2016 για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών (οδηγία για τα NAK) καθιερώνει απαιτήσεις ασφάλειας και κοινοποίησης για φορείς εκμετάλλευσης / παρόχους ψηφιακών ή / και βασικών υπηρεσιών και προβλέπει κυρώσεις και διαδικασίες επιβολής κατά εταιριών οι οποίες δεν συμμορφώνονται πλήρως ασφάλειας. Κατά συνέπεια, πρέπει να ληφθούν μέτρα για την πρόληψη και την ελαχιστοποίηση των επιπτώσεων οποιασδήποτε παραβίασης και η υιοθέτηση μιας νοοτροπίας διαχείρισης κινδύνων περιλαμβάνεται μεταξύ των ευθυνών αυτών των φορέων εκμετάλλευσης.

Οι νομικές ευθύνες και υποχρεώσεις μπορούν επίσης να επηρεάσουν τους οργανισμούς. Λόγω του μεγέθους και του κόστους των παραβιάσεων της ασφάλειας των πληροφοριών, η εμπλοκή στην ασφάλεια του κυβερνοχώρου της οργάνωσής τους από αξιωματικούς και διευθυντές πρέπει να θεωρείται μέρος των εμπιστευτικών ευθυνών τους. Ενώ πρέπει να λαμβάνεται μέριμνα για τη λήψη αποφάσεων, το πρότυπο του εύλογου δεν είναι στατικό, αντανακλώντας τα διαφορετικά προφίλ κινδύνου της οργάνωσης, καθώς και την εξέλιξη των τεχνολογιών και πρακτικών τελευταίας τεχνολογίας. Η νομοθεσία, όπως ο νόμος Sarbanes-Oxley στις ΗΠΑ, δημιουργεί νομικές υποχρεώσεις για τα ανώτερα στελέχη και το διοικητικό συμβούλιο να εξετάζει συνεχώς, να διασφαλίζει και να

υποβάλλει έκθεση σχετικά με την ασφάλεια των πληροφοριών. Αυτό ενισχύει τη σημασία της επικαιροποίησης των πολιτικών και της διατήρησης της συμμετοχής των ανώτερων στελεχών.

Τέλος, οι εταιρείες ενδέχεται να αντιμετωπίσουν πρόστιμα για παραβιάσεις δεδομένων, οι οποίες επηρεάζουν τα προσωπικά δεδομένα των χρηστών. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR), ο οποίος τίθεται σε ισχύ το 2018, επιβάλλει αυστηρότερες εγγυήσεις και τυποποιημένες υποχρεώσεις τόσο για τις εταιρείες όσο και για τους υπεργολάβους τους. Επιπροσθέτως, επιβάλλει ταχείες ειδοποίησεις για παραβιάσεις δεδομένων από τις εταιρείες προς τις αρχές και τους χρήστες, αυξάνοντας τις πιθανότητες για ζημιές στη φήμη. Τέλος, μπορεί να επιβληθούν υψηλά διοικητικά πρόστιμα ύψους έως 20 εκατ. Ευρώ ή 4% ή ετήσιος συνολικός κύκλος εργασιών (όποιο είναι υψηλότερο) για παραβιάσεις των απαιτήσεων προστασίας και προστασίας δεδομένων. Τα πρόστιμα αυτά αποτελούν αναπόσπαστα επιχειρήματα για την ενσωμάτωση της προστασίας του κυβερνοχώρου μέσω ενός CSC.

8.4 Η σημασία των ανθρώπινων παραγόντων στην ασφάλεια του κυβερνοχώρου

Παρά το γεγονός ότι η πλειοψηφία των cyberattacks το 2016 είναι hacking και malware-related, τρεις από τις κορυφαίες πέντε απειλές cyberattack σχετίζονται με τους ανθρώπινους παράγοντες, κοινωνική μηχανική μέσω μηνυμάτων ηλεκτρονικού "ψαρέματος", ανθρώπινα λάθη και σκόπιμη κακή χρήση. Το 2015, 21,8% και το 2016, το 15,8% όλων των παραβιάσεων δεδομένων οφείλεται σε phishing, spoofing ή κοινωνική μηχανική, ενώ το 2017, τα ανθρώπινα λάθη αντιστοιχούσαν στο 19 έως 36% όλων των παραβιάσεων δεδομένων, ανάλογα με τη χώρα ή την περιοχή.²⁶ Εκτός από τις απειλές που βασίζονται στον κυβερνοχώρο, υπάρχει η πρόσθετη πρόκληση να διασφαλιστεί η φυσική ασφάλεια κατά τη συζήτηση των ανθρωπίνων φορέων, ιδίως όταν αντιμετωπίζονται απειλές εμπιστευτικών πληροφοριών, καθώς η ασφάλεια του κυβερνοχώρου περιλαμβάνει εγγενή ανθρώπινα / φυσικά στοιχεία. Οι πολιτικές που καλύπτουν τη διατήρηση ενός καθαρού γραφείου χωρίς διαβαθμισμένο έγγραφο, οθόνες κλεισίματος και συστήματα όταν βρίσκονται μακριά από έναν υπολογιστή, άτομα με δυσκολίες στο προσωπικό που δεν εμφανίζουν αναγνωριστικά σήματα σε επιχειρηματικούς ορόφους και επιβολή

ελέγχων πρόσβασης σε κτίρια είναι όλα τα μέτρα φυσικής προστασίας που πρέπει να ενσωματωθούν σε οργανισμούς CSC.

Η ανθρώπινη συμβολή στον κυβερνοχώρο είναι σαφής. Ωστόσο, η διάδοση της γνώσης, η αύξηση της ευαισθητοποίησης και η επιρροή στη συμπεριφορά των εργαζομένων για τον μετριασμό αυτών των κινδύνων είναι δύσκολα καθήκοντα και αγνοώντας τους ανθρώπινους παράγοντες στην ανάπτυξη και την ανάπτυξη πολιτικών και διαδικασιών στον τομέα του κυβερνοχώρου, προδικάζει αυτές τις δραστηριότητες σε αποτυχία. Το προσωπικό θα επιδιώξει ενεργά την καταστρατήγηση των πολιτικών ασφάλειας που: εμποδίζουν τους να ολοκληρώσουν τις καθορισμένες επιχειρηματικές τους λειτουργίες, να επιβάλουν αυτό που θεωρούν ως αδικαιολόγητο βάρος, και / ή αντιπροσωπεύουν έλλειψη κατανόησης ως προς το τι πρέπει να δοθεί προτεραιότητα. Αυτό συνήθως δεν οφείλεται σε κακόβουλη ασάφεια ή αμφιθυμία, αλλά από την επιθυμία να «επιτελέσουν επιτυχώς τη δουλειά τους». Για παράδειγμα, οι αυστηρές εταιρικές πολιτικές σχετικά με τη χρήση ιδιωτικών συσκευών για εργασία μπορεί να θεωρηθούν ως άσκοπα επιβαρυντικές για τους εργαζομένους. Επιβάλλοντας πολλαπλούς, πολύπλοκους κωδικούς πρόσβασης που πρέπει να αλλάζουν τακτικά χωρίς να επιτρέπονται τα μπρελόκ με κωδικό πρόσβασης, υποχρεώνει το προσωπικό να γράφει τους κωδικούς πρόσβασης για να τις απομνημονεύει, ενδεχομένως χρησιμοποιώντας ηλεκτρονικά μέσα. Οι υπολογιστές στα τμήματα έκτακτης ανάγκης του νοσοκομείου παραμένουν συνδεδεμένοι με το προσωπικό (κατά πολιτικές ασφάλειας) που δίνουν προτεραιότητα στην άμεση θεραπεία ασθενών για να σώσουν τη ζωή τους πέρα από την προστασία των δεδομένων των ασθενών.²⁷

Επιπλέον, οι άνθρωποι διαθέτουν μια πεπερασμένη χωρητικότητα για να συμμορφώνονται με τα αιτήματα ασφάλειας στο χώρο εργασίας. Πέρα από ένα συγκεκριμένο όριο, οι προσπάθειες επιβολής πρόσθετων διαδικασιών και απαιτήσεων ασφαλείας θα αντιμετωπιστούν από την αντίσταση και από προσπάθειες παρακάμψεως. Έχει σημειωθεί ότι σε πολλούς εργασιακούς χώρους, αυτό το όριο συμμόρφωσης έχει υπερβεί από καιρό τους περισσότεροι χρήστες.²⁸

Η ανάπτυξη μιας CSC είναι σημαντική για τη διαχείριση του κινδύνου του ανθρώπινου παράγοντα, επιτρέποντας παράλληλα την υιοθέτηση και τη χρήση νέων τεχνολογιών από τις εταιρείες. Πρέπει να επιδιωχθεί η αποτελεσματικότητα, η ευελιξία και η

προσαρμοστικότητα, που υποστηρίζονται από μια ισχυρή κουλτούρα της ασφάλειας στον κυβερνοχώρο. Οι καινοτομίες, όπως η υιοθέτηση μιας πολιτικής που βασίζεται στη δική σας συσκευή ή η απόκτηση ενός νέου επιχειρηματικού εταίρου, μπορούν να καταστήσουν τους οργανισμούς εκτεθειμένους, αλλά είναι απαραίτητοι για τη διατήρηση της ανταγωνιστικότητας και της ανάπτυξης. Μια καλή CSC θα ενσταλάξει μια νοοτροπία ασφάλειας στους ανθρώπους σε όλες τις πτυχές της δουλειάς τους και μπορεί να μετατραπεί ακόμη και στην ιδιωτική ζωή τους.

9 Οργανωτικοί παράγοντες που επηρεάζουν τους πολιτισμούς στον κυβερνοχώρο

Οι οργανώσεις μπορούν να λάβουν μέτρα για να διαμορφώσουν τόσο την CSC όσο και η ευρύτερη οργανωτική τους κουλτούρα μπορούν να επηρεάσουν σε μεγάλο βαθμό την CSC. Εδώ, οι συνεργασίες εντός του οργανισμού είναι ουσιαστικές, καθώς η ανοιχτή επικοινωνία θα διευκολύνει την ανάπτυξη μιας CSC. Ενώ όλοι μέσα σε μια εταιρεία πρέπει να συμμετέχουν, συμβάλλοντας στα πεδία της εμπειρογνωμοσύνης τους, προσδιορίζοντας τους τομείς όπου οι κίνδυνοι στον κυβερνοχώρο και άλλες επιχειρηματικές λειτουργίες τέμνουν και πιθανές λύσεις σύγκρουσης και προβληματισμού, ορισμένες εκτελεστικές θέσεις και τμήματα έχουν να διαδραματίσουν βασικό ρόλο στην ανάπτυξη της CSC. Αυτοί οι παράγοντες εξετάζονται παρακάτω.

9.1 Οργανωτική κουλτούρα

Η οργανωτική κουλτούρα είναι ένα πολύπλοκο σύστημα κοινών πεποιθήσεων και αξιών μεταξύ των εργαζομένων, που καθοδηγεί τη συμπεριφορά τους ή απλά είναι ο τρόπος που γίνονται τα πράγματα. Οι απόψεις, οι στάσεις και οι συμπεριφορές των εργαζομένων στην ασφάλεια των πληροφοριών θα επηρεαστούν με τη σειρά τους από τις αλλαγές στην κουλτούρα της ασφάλειας του οργανισμού. Η οργανωτική κουλτούρα μπορεί να ενισχύσει τη δέσμευση για την οργάνωση και να ενισχύσει τη σταθερότητα προσφέροντας καθοδήγηση και αποδεκτά πρότυπα για τη συμπεριφορά των εργαζομένων. Τόσο η αποδεκτή όσο και η απαράδεκτη συμπεριφορά πρέπει να καθοριστούν σύμφωνα με τις επιθυμίες της οργάνωσης και να ενθαρρύνονται ή να καταγγέλλονται αντίστοιχα. Εάν επιβληθούν κυρώσεις, απαιτείται συνεκτικότητα στην εφαρμογή τους για να εξασφαλιστεί η συμμόρφωση και να επηρεαστούν οι αλλαγές στη νοοτροπία των εργαζομένων.

Σε αυτό το πλαίσιο, μια αποτελεσματική CSC πρέπει να ενσωματωθεί πλήρως στην οργανωτική κουλτούρα, εάν η αξία της ασφάλειας του κυβερνοχώρου πρέπει να γίνει αποδεκτή από όλα τα μέλη. Οι αλλαγές στο εργασιακό περιβάλλον πρέπει να υποστηριχθούν εμφανώς από τα ανώτερα διοικητικά στελέχη και να υλοποιηθούν μέσω σαφών ευθυνών και συμμετοχής από όλους στον οργανισμό,

προωθώντας την κυριότητα οποιουδήποτε προγράμματος και κίνητρο να τηρηθεί. Η δέσμευση για την ασφάλεια στον κυβερνοχώρο θα πρέπει επίσης να σηματοδοτείται μέσω επαρκούς κατανομής του προϋπολογισμού και κίνητρο για την επίτευξη μεγαλύτερης ασφάλειας, παρά απλής συμμόρφωσης με τα τετραγωνίδια. Πράγματι, η δέσμευση για την ποιότητα και την ασφάλεια στον κυβερνοχώρο υποδηλώνει μια ευρύτερη οργανωτική κουλτούρα αριστείας στις επιχειρήσεις.

9.2 Η ευρύτερη στρατηγική στον τομέα της ασφάλειας στον κυβερνοχώρο

Προϋπόθεση για μια CSC είναι η ανάπτυξη και η επικοινωνία των πολιτικών και διαδικασιών, οι οποίες καθορίζουν σαφείς ευθύνες και χρησιμεύουν ως οδηγός για τη συμπεριφορά και τις συμπεριφορές στον τομέα της ασφάλειας. Με βάση μια αρχική εκτίμηση της τρέχουσας κατάστασης της κουλτούρας ασφάλειας, η διοίκηση θα πρέπει να καταρτίσει μια στρατηγική για την ασφάλεια στον κυβερνοχώρο, ενσωματώνοντας μια πολιτική καθοδήγησης της πολιτιστικής αλλαγής και καθορισμού των στόχων ασφάλειας και του οράματος του οργανισμού. Με τον τρόπο αυτό, συγκεκριμένους στόχους και τη χρηστικότητα του τελικού χρήστη θα πρέπει να είναι τα θεμελιώδη ζητήματα, όπως είναι δυνατές μόνιμες αλλαγές στη συμπεριφορά μόνο όταν εξισώνουν την επιτυχία και την ικανοποίηση μεταξύ των εργαζομένων.

Για να διευκολυνθεί η ιδιοκτησία, η αποδοχή και η υποστήριξη των εργαζομένων, όλοι σε μια εταιρεία θα πρέπει να ενθαρρύνονται να συμμετέχουν κατά την ανάπτυξη και την ενσωμάτωση μιας πολιτικής ασφάλειας πληροφοριών. Αυτό διασφαλίζει ότι τα μέτρα ασφαλείας προσαρμόζονται στις λειτουργικές και ιεραρχικές διαφορές εντός της εταιρείας και ότι αποφεύγονται γίνονται υπερβολικά επαχθείς ή περίπλοκες.

Μια επιτυχημένη στρατηγική θα πρέπει: (1) να ενισχύσει τις ισχυρές νοοτροπίες και δράσεις διακυβέρνησης, (2) να σχεδιάζονται παρόμοια με άλλες επιχειρηματικές λειτουργίες για να διευκολύνουν την αποδοχή, (3) να οικοδομηθεί γύρω από ένα προσαρμόσιμο πλαίσιο για τη διευκόλυνση της μακράς χρήσης και (4) η αποτελεσματικότητά του πρέπει να είναι μετρήσιμη για να αποδειχθεί επιτυχία. Η χρήση μετρήσεων εδώ μπορεί να βοηθήσει τη διοίκηση

στην αναθεώρηση και την ενημέρωση της πολιτικής μέσω της τακτικής παρακολούθησης και της εκτίμησης των επιπτώσεων.

9.3 Διασυνοριακή οργάνωση - οι ρόλοι που πρέπει να διαδραματίσουν οι διαφορετικές ομάδες

9.3.1 Ο ρόλος της ανώτερης διοίκησης

Η ασφάλεια στον κυβερνοχώρο έχει ανατεθεί στην ανώτατη διοίκηση, η οποία οφείλεται στους κινδύνους των παραβιάσεων της οικονομίας και της φήμης, στις κανονιστικές απαιτήσεις και στις πιέσεις που ασκούν οι μέτοχοι. Η εκκίνηση, η μετάδοση και η ενσωμάτωση των πολιτιστικών αλλαγών απαιτεί ηγεσία και εξαγορά από τα ανώτερα διοικητικά στελέχη και για να εξασφαλιστεί η διαρκή αυτή αλλαγή, θα πρέπει να επισημάνει σαφώς τη δέσμευσή της και τη συμμετοχή της στην CSC διαθέτοντας επαρκείς πόρους για ολοκληρωμένα προγράμματα, ενώ εκχωρεί σαφείς ευθύνες και εξουσία.

Η ανώτατη διοίκηση και το διοικητικό συμβούλιο θα πρέπει να αντιμετωπίζουν την ασφάλεια του κυβερνοχώρου ως έναν κίνδυνο που πρέπει να ληφθεί υπόψη και να λάβουν στρατηγικές αποφάσεις σχετικά με τις απαιτήσεις ασφαλείας της οργάνωσής τους εξετάζοντας την εφαρμογή πιθανών πολιτικών και τεχνικών μέτρων. Από την άποψη αυτή, η ασφάλεια πρέπει να θεωρείται όχι μόνο ως κόστος, αλλά ως μείωση του κινδύνου. Επιπλέον, πρέπει να καθιερωθούν σαφείς προτεραιότητες και να κοινοποιηθούν στην CISO, που να του επιτρέπουν να εκτελεί τα καθήκοντά του σε ευθυγράμμιση με την όρεξη, τα συμφέροντα και τις απαιτήσεις για την ανάληψη κινδύνου.

Τέλος, για να αλλάξει τον πολιτισμό, τα ανώτερα στελέχη πρέπει να χρησιμοποιούν μια σειρά μέσων, συμπεριλαμβανομένων των δηλώσεων αξίας, της εσωτερικής επικοινωνίας, της εκπαίδευσης και πρέπει να οδηγούν με παραδείγματα μέσω των συμπεριφορών τους, υποστηρίζοντας τις οραματικές τους δηλώσεις. Η ισχυρή CSC εντός της διοίκησης αποδεικνύεται με την αύξηση της ευαισθητοποίησης σχετικά με την ασφάλεια κινδύνου, τη διεξαγωγή ασκήσεων αντίδρασης στην παραβίαση της ασφάλειας και τα ασκήματα συνέχειας και τη βελτίωση της επικοινωνίας με την CISO.

9.3.2 Ο ρόλος των CISOs

Η CISO διαδραματίζει καθοριστικό ρόλο στην ανάπτυξη μιας CSC. Πρέπει να κατανοεί τις ανάγκες και τις λειτουργίες της επιχείρησής του, χρησιμοποιώντας τις τεχνικές και τις επικοινωνιακές τους δεξιότητες για να ευθυγραμμίζει τους στόχους της πληροφορικής και της ασφάλειας με τους επιχειρηματικούς. Οι CISOs συμμετέχουν στη σύνταξη της στρατηγικής για την ασφάλεια στον κυβερνοχώρο και αντιπροσωπεύουν την ασφάλεια σε εκτελεστικό επίπεδο διατηρώντας παράλληλα καλά κανάλια επικοινωνίας τόσο με ανώτερα στελέχη όσο και με υπαλλήλους για να μοιραστούν αποτελεσματικά το όραμά τους.

Για τη διοίκηση και το διοικητικό συμβούλιο, η CISO θα πρέπει να καταστήσει σαφή την αξία της ασφάλειας στον κυβερνοχώρο, προσφέροντας ταυτόχρονα πληροφορίες σχετικά με την εξέλιξη της ασφάλειας, τους κινδύνους και τις επιλογές σύμφωνα με τη διαχείριση κινδύνου. Για τους υπαλλήλους, η CISO πρέπει να συμμετέχει σε σαφείς και κατανοητές δραστηριότητες επικοινωνίας, συμμετοχής και υποστήριξης, αποδεικνύοντας ότι η ασφάλεια αποτελεί μέρος της "συνήθους επιχειρηματικής δραστηριότητας" και όχι εμπόδιο στις επιχειρηματικές δραστηριότητες. Οι CISOs είναι υπεύθυνες για την καλή διακυβέρνηση της ασφάλειας, τους ανθρώπους και τη διαχείριση της διαδικασίας. Η συμμετοχή στις διαδικασίες λήψης αποφάσεων και η κοινή κατανόηση μεταξύ των ενδιαφερομένων είναι σημαντική και μπορεί να διευκολυνθεί μέσω επιτροπών, ρόλων διασύνδεσης, ανοικτής επικοινωνίας και κοινωνικής συμμετοχής σε όλη τη διαδικασία μετασχηματισμού.

9.3.3 Ο ρόλος της μεσαίας διοίκησης

Ως διαμεσολαβητής μεταξύ των εργαζομένων και της ανώτερης διοίκησης, η μεσαία διοίκηση έχει να διαδραματίσει βασικό ρόλο στον καθορισμό του τόνου της ασφάλειας στον κυβερνοχώρο σε έναν οργανισμό. Πρέπει να είναι πεπεισμένοι για τα οφέλη της και πρέπει να συμμετέχουν αποτελεσματικά στην εφαρμογή της ασφάλειας στον κυβερνοχώρο σε ολόκληρο τον οργανισμό. Για να αποφευχθεί η αντιμετώπιση της ασφάλειας του κυβερνοχώρου ως εμπόδιο και επιβάρυνση από τις ομάδες που οδηγούν τη μεσαία διοίκηση, θα πρέπει να επιμείνουν και να ενθαρρύνουν την ασφαλή συμπεριφορά, προσφέροντας ανατροφοδότηση και κίνητρα στους υπαλλήλους,

τόσο όσον αφορά την επιχειρηματική τους δραστηριότητα όσο και την απόδοση της πληροφορικής.

9.3.4 Ο ρόλος της πληροφορικής

Ο ρόλος της ομάδας IT στην CSC είναι πολύπλευρος. Η ομάδα θα πρέπει να διασφαλίσει ότι υιοθετούνται σύγχρονα τεχνικά μέτρα, τα οποία είναι αποτελεσματικά, απλά, χρήσιμα και υποστηρίζουν ασφαλή συμπεριφορά, καθόσον δεν είναι υπερβολικά επαχθείς. Για να επιτευχθούν αποτελεσματικά αυτοί οι στόχοι με την προσαρμογή των λύσεων, όσοι διατηρούν την τεχνική υποδομή πρέπει να κατανοούν την επιχειρηματική διάρθρωση της οργάνωσης και των δραστηριοτήτων τους, ενώ η ανοικτή επικοινωνία των στόχων, των ορόσημων και των διαδικασιών πληροφορικής μπορεί να καθοδηγήσει περαιτέρω το πρόγραμμα CSC.

Η εξειδίκευση στην ασφάλεια στον κυβερνοχώρο πρέπει να αποτελεί βασική αρμοδιότητα του τμήματος πληροφορικής, η οποία υλοποιείται είτε μέσω εξειδίκευμένης ομάδας είτε μέσω συνεργασίας με εξωτερικούς παρόχους υπηρεσιών. Αυτή η εμπειρογνωμοσύνη στον τομέα του κυβερνοχώρου θα πρέπει να ενημερώνει τη διαχείριση των κινδύνων, να υποστηρίζει τη λήψη αποφάσεων των CISO και να παρέχει πληροφορίες για τα ανώτερα στελέχη. Μπορεί επίσης να αποτελέσει μοχλό για την ανάπτυξη της εκπαίδευσης για την ασφάλεια και την υιοθέτηση προληπτικών τεχνολογιών σε ολόκληρο τον οργανισμό.

Πρέπει να διασφαλιστεί η συλλογή δεδομένων σχετικά με τους κινδύνους του κυβερνοχώρου και τις επιθέσεις κατά των δικτύων του οργανισμού. Τα δεδομένα σχετικά με την απόδοση στον κυβερνοχώρο του οργανισμού μπορούν να χρησιμοποιηθούν για να επανεκτιμηθούν και να επικαιροποιηθούν τα προγράμματα απόκρισης επίπτωσης της εταιρείας, να κατανοηθεί σε βάθος το προφίλ κινδύνου της εταιρείας και να μετρηθεί ο αντίκτυπος κάθε εφαρμοσμένου προγράμματος CSC.

9.3.5 Ο ρόλος της νομιμότητας / συμμόρφωσης

Η υπηρεσία νομικής συμμόρφωσης έχει ένα ρόλο να διαδραματίσει παρέχοντας εξειδίκευμένες νομικές συμβουλές για να εξασφαλίσει ότι

όλες οι πρακτικές CSC και cyber-security ενσωματωμένες στον οργανισμό συμμορφώνονται με την εθνική και διεθνή νομοθεσία, συμπεριλαμβανομένων των κανόνων προστασίας δεδομένων. Η υπηρεσία θα πρέπει επίσης να παρέχει στήριξη κατά την εφαρμογή τεχνικών μέτρων που αποσκοπούν στην παρακολούθηση της συμπεριφοράς των εργαζομένων, προκειμένου να διαπιστωθεί ότι το τι παρακολουθείται και πώς χρησιμοποιούνται οι πληροφορίες συμμορφώνεται πλήρως με τις εθνικές και διεθνικές νομικές απαιτήσεις.

9.3.6 Ο ρόλος του ανθρώπινου δυναμικού

Το ανθρώπινο δυναμικό (HR) διαδραματίζει σημαντικό ρόλο ως σύνδεσμος μεταξύ διοίκησης και εργαζομένων. Χάρη στη θέση τους σε μια οργανωτική, η HR μπορεί να προσφέρει πληροφορίες σχετικά με τη συμπεριφορά και την ψυχή των εργαζομένων, οι οποίες με τη σειρά τους μπορούν να χρησιμοποιηθούν για την αντιμετώπιση πιθανών απειλών εσωτερικών παραγόντων ή για το σχεδιασμό και την παροχή αποτελεσματικών προγραμμάτων εκπαίδευσης για την ασφάλεια. Το τμήμα μπορεί επίσης να διασφαλίσει ότι όλοι οι συμμετέχοντες στον οργανισμό υποβάλλονται στην απαραίτητη εκπαίδευση ασφάλειας, επιβάλλοντας τη συμμόρφωση, κατά τη διεξαγωγή αξιολογήσεων πρακτικής ασφαλείας των εργαζομένων και, ενδεχομένως, επιβάλλοντας πειθαρχικές κυρώσεις.

9.3.7 Ο ρόλος του μάρκετινγκ / των εσωτερικών επικοινωνιών

Το CSC αφορά στην αλλαγή νοοτροπίας, αντιλήψεων και μεταβίβασης γνώσεων στους ανθρώπους, με ασφάλεια που παρουσιάζεται στους υπαλλήλους ως "συνήθης εργασία". Το τμήμα μάρκετινγκ μπορεί να βοηθήσει την ανάπτυξη της CSC, σχεδιάζοντας και πρωθώντας προγράμματα ενημέρωσης και εκπαίδευσης σχετικά με την ασφάλεια και δημιουργώντας μηνύματα που μεγιστοποιούν τις επιπτώσεις και τονίζουν τα οφέλη της CSC. Μπορούν επίσης να μεγιστοποιήσουν τη σχέση κόστους-αποτελεσματικότητας, αξιοποιώντας εξατομικευμένες προσεγγίσεις και πολλαπλά κανάλια.

Η Cybersecurity μπορεί επίσης να χρησιμοποιηθεί ως ένα ισχυρό εργαλείο μάρκετινγκ για την προσέλκυση πελατών και επιχειρηματικών συνεργατών, ειδικά καθώς οι ανησυχίες για την

προστασία της ιδιωτικής ζωής και του κυβερνοχώρου αυξάνονται παγκοσμίως. Οι δραστηριότητες των εταιρικών κοινωνικών μέσων, που διαχειρίζεται το τμήμα μάρκετινγκ, μπορούν να παρουσιάσουν την ασφάλεια του κυβερνοχώρου ως βασική πτυχή της εικόνας μιας εταιρείας, φωτίζοντας και ενισχύοντας την εσωτερική CSC αυτής της εταιρείας.

9.4 Εγκρίθηκαν επιχειρηματικά μοντέλα και μοντέλα απασχόλησης

Τα σημερινά ευέλικτα επιχειρηματικά μοντέλα μπορούν να επηρεάσουν την CSC ενός οργανισμού. Οι νέοι και οι έκτακτοι υπάλληλοι (όπως οι σύμβουλοι ή οι συμβασιούχοι υπάλληλοι) που είναι λιγότερο ενσωματωμένοι σε έναν οργανισμό δεν θα επηρεάζονται τόσο από την οργανωτική κουλτούρα. Για να αναπτυχθεί μια CSC, πρέπει να δοθεί ιδιαίτερη προσοχή στις επικοινωνίες και την κατάρτιση για όλες τις κατηγορίες εργαζομένων και αυτή η εκπαίδευση πρέπει να επανεξετάζεται συνεχώς ώστε να καλύπτει τις αλλαγές στις τεχνολογίες και τις πρακτικές εργασίας.

Η επιχειρηματική εξάρτηση από την πρόσβαση στο Διαδίκτυο συνεχίζει να αυξάνεται, ενώ τα περιβάλλοντα εργασίας επιτρέπουν όλο και περισσότερο τις πολιτικές "bring-your-own-device" που ανοίγουν νέες εκθέσεις κινδύνου. Ταυτόχρονα, η αποδυνάμωση των ξεχωριστών ορίων ευθύνης για τις εταιρείες που ενσωματώνονται στα ευρύτερα δίκτυα άλλων και η αύξηση των παγκόσμιων αλυσίδων αξίας και των εταιρικών σχέσεων συνεπάγονται όλο και περισσότερες εκθέσεις κινδύνου. Μια ισχυρή CSC, σε συνδυασμό με τις συμβατικές ρήτρες ασφαλείας ⁴⁰ και τις αξιολογήσεις κινδύνου από νέους επιχειρηματικούς εταίρους, μπορεί να συμβάλει στην επίτευξη ενισχυμένης ασφάλειας πληροφοριών.

10 Μη οργανωτικοί παράγοντες που επηρεάζουν τους πολιτισμούς στον κυβερνοχώρο

Η CSC είναι ο τρόπος με τον οποίο ενεργούν οι εργαζόμενοι όσον αφορά την ασφάλεια του κυβερνοχώρου, την προστασία των πληροφοριακών στοιχείων του οργανισμού ή την επίτευξη του επιθυμητού επιπέδου ασφάλειας του κυβερνοχώρου, καθώς και τις υποκείμενες γνώσεις, πεποιθήσεις, αντιλήψεις, στάσεις, υποθέσεις, κανόνες και αξίες. Η ανάπτυξη μιας αποτελεσματικής CSC απαιτεί την αναγνώριση και τη χρησιμοποίηση παραγόντων εκτός της επιστήμης της διοίκησης και της διαχείρισης. Η κατανόηση των επιπτώσεων της ανθρώπινης ψυχολογίας, των κοινωνιολογικών παραγόντων και των πολιτισμικών επιπτώσεων είναι απαραίτητη για την ανάπτυξη μιας επιτυχημένης CSC. Εξάλλου, οι εργαζόμενοι είναι πρωτίστως ανθρώπινοι όντες που κινούνται τόσο στο περιβάλλον εργασίας τους (οργανωτικό) όσο και σε ευρύτερες κοινωνικές πιέσεις.

Αυτή η έννοια του πολιτισμού μπορεί να περιλαμβάνει επαναλαμβανόμενες συμπεριφορές, ομαδικές προδιαγραφές, ενσωματωμένες δεξιότητες, κοινές έννοιες και επίσημες τελετές και εορτασμούς. Μέσα από τις αόρατες δομές που προσφέρουν, αυτές οι ιδέες, συμπεριφορές και κοινωνικά έθιμα διευκολύνουν και καθοδηγούν τις πεποιθήσεις και τις αλληλεπιδράσεις των μελών της οργάνωσης. Είναι η κοινωνική πτυχή του πολιτισμού που οδηγεί στη φυσική ανάπτυξη κοινών συνόλων πεποιθήσεων μεταξύ των ανθρώπων και καθώς η ασφάλεια είναι και μια ψυχική συμπεριφορά, πρέπει να ενσωματωθεί στο σύστημα αξιών του οργανισμού μέσω της μεταμόρφωσης του πολιτισμού, πριν μια οργάνωση μιλήσει για την πολιτισμός στον κυβερνοχώρο. Αυτό που είναι απαραίτητο για την προώθηση, ανάπτυξη και ενσωμάτωση της CSC, είναι ότι οι υφιστάμενες οργανωτικές κουλτούρες μπορούν να μετασχηματιστούν.

Για να βοηθήσει στην κατανόηση αυτής της διαδικασίας, ο πολιτισμός μπορεί να χωριστεί σε τρία επίπεδα που αλληλεπιδρούν μεταξύ τους: (1) πρωθιόμενες αξίες, (2) ορατές συμπεριφορές και (3) τις υποκείμενες υποθέσεις που διατηρούμε. Ο μετασχηματισμός του πολιτισμού ενός οργανισμού θα πρέπει να αρχίσει με μια αλλαγή στις αξίες, οδηγώντας στην υιοθέτηση νέας συμπεριφοράς. Εάν η συμπεριφορά αυτή είναι επιτυχής στην επίλυση ενός προβλήματος,

πιθανότατα θα υιοθετηθεί μόνιμα και η αξία θα μετατραπεί σε υποκείμενη υπόθεση.

10.1 Ανθρώπινοι παράγοντες που επηρεάζουν τις καλλιέργειες ασφάλειας στον κυβερνοχώρο

Οι τεχνολογίες ασφάλειας μπορούν να είναι αποτελεσματικές μόνο εάν οι εργαζόμενοι έχουν τις απαραίτητες γνώσεις, δεξιότητες, κατανόηση και αποδοχή για τη χρήση τους.⁴⁹ Η επίτευξη αυτής της «ανθρώπινης ασφάλειας» μπορεί να απαιτήσει αλλαγή τόσο στη γνώση όσο και στη συμπεριφορά των εργαζομένων, όπου η εκπαίδευση και η κατάρτιση μπορούν να χρησιμοποιηθούν για την προώθηση της γνώσης, ενώ η συμπεριφορά μπορεί να μεταβληθεί μέσω πολιτιστικών και οργανωτικών κινήτρων και κυρώσεων.

10.1.1 Ψυχολογικοί παράγοντες

Για να πεισθούν οι άνθρωποι να αλλάξουν, πρέπει να γίνουν τρεις παράλληλες διαδικασίες: (1) πρέπει να υπάρξει δυσαρέσκεια με την παρούσα κατάσταση. (2) αυτή η δυσαρέσκεια πρέπει να προκαλέσει άγχος ή / και ενοχή. και (3) οι εργαζόμενοι πρέπει να υιοθετούν νέα συμπεριφορά σε ένα ασφαλές περιβάλλον χωρίς να διακυβεύουν την ταυτότητα ή την ακεραιότητά τους. Για να «ξεσηκώσει» την υπάρχουσα κουλτούρα, οι αδυναμίες της πρέπει να εντοπιστούν και να κοινοποιηθούν, μετά την οποία η νέα κουλτούρα μπορεί να ενσταλάξει μεταβάλλοντας τη γνώση και τη συμπεριφορά. Αυτό πρέπει να διεξαχθεί σε ένα ασφαλές περιβάλλον μάθησης για να αποφευχθεί το άγχος και οι αμυντικές στάσεις εναντίον του νέου πολιτισμού. ο εξαναγκασμός πρέπει να αποφευχθεί, καθώς θα αυξήσει την άμυνα και θα μειώσει την αποδοχή της αλλαγής.⁵⁰ Αντίθετα, οι άνθρωποι πρέπει να ασχολούνται με τον πολιτισμό έτσι ώστε να συμμετέχουν, να συμβάλλουν σε αυτό και να αισθάνονται υπεύθυνοι γι 'αυτό. Αυτό μπορεί να επιτευχθεί μέσω της υπευθυνότητας, της εμπιστοσύνης, της επικοινωνίας και της συνεργασίας εντός του οργανισμού.

Τα ατομικά χαρακτηριστικά γνωρίσματα μπορούν επίσης να επηρεάσουν τη συμπεριφορά και τις στάσεις των ανθρώπων όσον αφορά την ασφάλεια, ενώ το προσωπικό ευσυνείδητου και επιμελούς προσώπου τείνει να γνωρίζει και να τηρεί την ασφάλεια, όπως και το πιο μακροπρόθεσμο προσωπικό.⁵¹ Διαφάνεια και η εμπειρία μπορούν

να ενθαρρύνουν την εμπιστοσύνη στην ασφάλεια, ενώ ο νευρωτισμός και η συναισθηματική αστάθεια έχουν το αντίθετο αποτέλεσμα. Ωστόσο, δεδομένου ότι οι κατάλληλες συνθήκες είναι ανοιχτές, το νευρικό και το εξωστρεφόμενο προσωπικό είναι πιο πιθανό να παραβιάζουν τις πολιτικές για την ασφάλεια στον κυβερνοχώρο. Τέλος, το επίπεδο αντίληψης και αποστροφής του ατόμου μπορεί να οδηγήσει σε διαφορές στη συμπεριφορά. Όλες αυτές οι σκέψεις πρέπει να λαμβάνονται υπόψη κατά το σχεδιασμό ενός μετασχηματισμού της ασφάλειας.

Το φύλο μπορεί επίσης να επηρεάσει τη συμπεριφορά και τις στάσεις των εργαζομένων, καθώς οι άνδρες τείνουν να είναι πιο σίγουροι για τη συμπεριφορά τους όσον αφορά την ασφάλεια και την ιδιωτική ζωή σε σχέση με τις γυναίκες, αν και οι γυναίκες γενικά αντιλαμβάνονται την ευπάθεια περισσότερο και είναι πιο πιθανό να συμπεριφέρονται με ασφάλεια. Οι άνδρες φαίνεται να επηρεάζονται από τη στάση απέναντι στην τεχνολογία, ενώ οι γυναίκες από κοινωνικούς ρόλους, ελέγχους συμπεριφοράς και κανόνες. Για την ενθάρρυνση της CSC, απαιτείται ένας ισορροπημένος εργασιακός χώρος μεταξύ των φύλων και η κατάλληλη διαμόρφωση του νέου πολιτισμού.

10.1.2 Συμμόρφωση και προσωπικότητα

Καθώς τα προγράμματα ασφαλείας απαιτούν πρόσθετη προσπάθεια, η συμπεριφορά των εργαζομένων μπορεί να επηρεάζεται από το αντιληπτό κόστος και τα οφέλη της συμμόρφωσης με την ασφάλεια, έτσι ώστε να πεισθεί το προσωπικό να ενεργεί με ασφάλεια. Για την επίτευξη μόνιμης αλλαγής, οι άνθρωποι πρέπει να κατανοήσουν: (1) τις απειλές που αντιμετωπίζουν, (2) την πολιτική ασφαλείας που πρέπει να τηρούν και (3) την ευθύνη που φέρουν.

Τα άτομα είναι γενικά κακά στην αξιολόγηση των κινδύνων από απειλές στον κυβερνοχώρο, υπερεκτιμώντας τη σπανιότητά τους καθώς και τη γνώση και τον έλεγχό τους. Διάφορες προκαταλήψεις συμβάλλουν σε αυτό, συμπεριλαμβανομένης μιας ψευδούς αίσθησης εξοικείωσης με τις απειλές στον κυβερνοχώρο, και την παρατήρηση των παραλείψεων ως αποδεκτής συμπεριφοράς υπό αβέβαιες συνθήκες. Τα προγράμματα ευαισθητοποίησης και εκπαίδευσης μπορούν να χρησιμοποιηθούν για να αλλάξουν τις αντίληψεις

κινδύνου και να διδάξουν στους εργαζόμενους πώς να διεξάγουν εύκολα τα καθήκοντα ασφαλείας με απόλυτη σιγουριά.

Τέλος, ένα θετικό πρόγραμμα ασφάλειας που βασίζεται στο ανοιχτό πνεύμα, στην εμπιστοσύνη και στην ενδυνάμωση είναι πιθανότερο να έχει διαρκή αντίκτυπο και να διασφαλίζει τη συμμόρφωση, παρά να εξαρτάται αποκλειστικά από το φόβο και την ευθύνη. Για μια διαρκή αλλαγή πολιτισμού, ένας συνδυασμός τόσο των ανταμοιβών όσο και ενός βαθμού εξαναγκασμού είναι πιθανότερο να είναι επιτυχής. Οι ανταμοιβές θα πρέπει να χρησιμοποιούνται για την ενίσχυση και την παροχή κινήτρων για ασφαλή συμπεριφορά, ενώ παράλληλη παρακολούθηση και κυρώσεις μπορούν να χρησιμοποιηθούν για την αύξηση του αντιληπτού προσωπικού κόστους της ανασφαλούς συμπεριφοράς. Παράγοντες όπως η αίσθηση της βεβαιότητας ανίχνευσης και η σοβαρότητα των τιμωριών μπορούν να λειτουργήσουν ως κίνητρα συμμόρφωσης ²¹ ενώ η ενσωμάτωση της συμμόρφωσης στη φυσική ροή εργασίας μπορεί να συμβάλει σε μια ισχυρή CSC.

10.1.3 Το κοινωνικό περιβάλλον

Οι άνθρωποι είναι κοινωνικά όντα που ακολουθούν τους ομαδικούς κανόνες και είναι γνωστό εδώ και καιρό ότι η πίεση των συμμαθητών μπορεί να επηρεάσει τη συμπεριφορά ενός ατόμου. Το ίδιο ισχύει για τη συμπεριφορά στον κυβερνοχώρο. Καθώς οι άνθρωποι επιθυμούν να αποκτήσουν την έγκριση άλλων, η συμπεριφορά τους μπορεί να επηρεαστεί σοβαρά από τις αντιλαμβανόμενες προσδοκίες των στελεχών και των συνομηλίκων. Οι σαφείς οδηγίες από τη διοίκηση σχετικά με τον τόπο ασφάλειας στον οργανισμό και οι συλλογικές συμπεριφορές των συναδέλφων μπορούν να έχουν μεγάλο αντίκτυπο στην ανάπτυξη ασφαλούς συμπεριφοράς. Μια κουλτούρα ασφάλειας, σε συνδυασμό με ικανοποίηση από την εργασία και οργανωτική υποστήριξη, οδηγούν σε αυξημένη συμμόρφωση με την ασφάλεια.

Οι εργαζόμενοι είναι επίσης πιο ενθαρρυνμένοι να συμμορφώνονται με τη στρατηγική ασφαλείας του οργανισμού τους, όταν πιστεύουν ότι και άλλοι γύρω τους κάνουν επίσης. Πράγματι, η τάση μας να ακολουθούμε το παράδειγμα άλλων σε αβέβαιες ή νέες συνθήκες είναι ένας ισχυρός κοινωνικός οδηγός αλλαγής συμπεριφοράς, κάτι που ισχύει ιδιαίτερα όταν οι άνθρωποι μπορούν να παρατηρούν ανοιχτά και να συζητούν συμπεριφορές ασφάλειας με άλλους που

χρησιμοποιούν τα ίδια εργαλεία ασφάλειας. Ως εκ τούτου, ένα πρόγραμμα ασφαλείας που έχει σχεδιαστεί για να ενσωματώνει ανακοινώσεις κοινής χρήσης, αλληλεπιδρασης και ασφάλειας μπορεί να είναι αποτελεσματικό για να εξασφαλίσει ότι όλοι οι εργαζόμενοι αναλαμβάνουν ατομική και συλλογική ευθύνη για τις συμπεριφορές τους ως προς την ασφάλεια.

Τέλος, οι άνθρωποι φυσικά επιδιώκουν καλύτερα αποτελέσματα για την κοινότητά τους ως σύνολο. Η πεποίθηση ότι οι ασφαλείς ενέργειες ενός ατόμου επηρεάζουν τη συνολική ασφάλεια του οργανισμού είναι πιο πιθανό να ενθαρρύνει μια τέτοια συμπεριφορά. Αυτό σημαίνει ότι θα πρέπει να διαβιβάζονται σαφή μηνύματα στους εργαζομένους σχετικά με τη σημασία της ασφάλειας των πληροφοριών και τον αντίκτυπο των δικών τους ενεργειών στο θέμα αυτό.

10.2 Εξωτερικοί παράγοντες

10.2.1 Εθνικοί πολιτισμοί

Οι εθνικοί πολιτισμοί μπορούν να καθορίσουν και να επηρεάσουν τις αξίες και τις υποθέσεις του ατόμου και έτσι να διαμορφώσουν τη χρήση της CSC και της πληροφορικής γενικά. Οι συγκεκριμένες αξίες που υπαγορεύονται από την εθνική κουλτούρα περιλαμβάνουν το σεβασμό στην εξουσία, τον ατομικισμό έναντι του κολεκτιβισμού, την αποφυγή αβεβαιότητας και τις αντιλήψεις ελέγχου, οι οποίες μπορούν να επηρεάσουν την ανάπτυξη της CSC. Η εθνικότητα μπορεί επίσης να επηρεάσει την οργανωτική κουλτούρα. για παράδειγμα, η ασφάλεια των πληροφοριών και η συμμόρφωση είναι στενά συνδεδεμένες στις ΗΠΑ.

Οι εθνικοί πολιτισμοί μπορούν επίσης να επηρεάσουν την υιοθέτηση, ανάπτυξη, διανομή και διαθεσιμότητα τεχνολογιών που φυσικά οδηγούν σε διαφορές. Οι εθνικές διαφορές στον τρόπο με τον οποίο οι άνθρωποι χρησιμοποιούν συγκεκριμένες τεχνολογίες συνδέονται επίσης με τη στάση τους έναντι της ιδιωτικής ζωής. Για παράδειγμα, οι άνθρωποι από τις Ηνωμένες Πολιτείες ήταν πιο πρόθυμοι να μοιραστούν πληροφορίες online από ότι οι άνθρωποι από την Ινδία και τα Ηνωμένα Αραβικά Εμιράτα⁸² που θα μπορούσαν να διαμορφώσουν την αποδοχή τους από τις πρακτικές της CSC. Τέτοιες διαφορές όσον αφορά την πρόσβαση και τη χρήση τεχνολογιών, την

κατανόηση της ιδιωτικής ζωής ή των δεδομένων προσωπικού χαρακτήρα, καθώς και την άποψη της εξουσίας, μπορούν να οδηγήσουν σε διαφορές στο CSC.

11 Υπάρχουσες πρακτικές και πόροι

11.1 Ευαισθητοποίηση, εκπαίδευση και επικοινωνία

Η γνώση, μαζί με τις στάσεις, τις αξίες και την αντίληψη κινδύνου, μπορούν να καθορίσουν όλους τους τρόπους συμπεριφοράς των ανθρώπων. Αυτό είναι σημαντικό καθώς τα προγράμματα ευαισθητοποίησης σχετικά με την ασφάλεια, η εκπαίδευση και η κατάρτιση μπορούν να αξιοποιηθούν για να επηρεάσουν τις γνώσεις τους, οι οποίες, σε συνδυασμό με την αλλαγή οργανωτικής κουλτούρας, μπορούν να επιφέρουν μια διαρκή CSC.

Η εκπαίδευση μπορεί να χρησιμοποιηθεί για να αλλάξει την ευαισθητοποίηση της ασφάλειας διδασκαλώντας τους εργαζόμενους τι, πώς και γιατί να κάνει τα πράγματα [διαφορετικά], και αυτή η συνειδητοποίηση της ασφάλειας θα ενισχύσει τότε την CSC καθώς ωριμάζει από τη γνώση στην πεποίθηση, την αποδοχή και τη συμπεριφορά. Η κατανόηση των απειλών και των διαθέσιμων εργαλείων, η αποδεκτή και απαράδεκτη συμπεριφορά, οι εφαρμοστέες κυρώσεις και τα αντίμετρα, καθώς και οι λόγοι που δικαιολογούν τις νέες πρακτικές ασφαλείας, λειτουργούν όλοι για να προωθήσουν την κυριότητα και τη συμμόρφωση των ανθρώπων. Η κατανόηση αυτή μπορεί να επιτευχθεί μέσω ανοικτής, έγκαιρης επικοινωνίας και σχετικής και καλοσχεδιασμένης εκπαιδευτικής παιδείας.

Για να επηρεάσουν αποτελεσματικά την ευαισθητοποίηση σε θέματα ασφάλειας σε ένα οργανισμό, τα προγράμματα κατάρτισης θα πρέπει να σχεδιάζονται με δύο πράγματα στο μυαλό: (1) κατανόηση των ευθυνών που συνδέονται με διαφορετικές λειτουργίες, και (2) την επίτευξη ενός ελάχιστου επιπέδου ευαισθητοποίησης σε επίπεδο εταιρείας.⁸⁰ Ο καθένας στην οργάνωση θα πρέπει να λάβει κάποιο βασικό επίπεδο εκπαίδευσης και οι εργαζόμενοι θα πρέπει να είναι εφοδιασμένοι με ευαισθητοποίηση σε κινδύνους, δεξιότητες και ελέγχους που σχετίζονται ειδικά με το ρόλο τους.⁸¹ Για την επίτευξη ασφαλούς συμπεριφοράς προσφέρουν στους εργαζόμενους μια εξατομικευμένη και ουσιαστική εκπαίδευση για να τους βοηθήσουν να εκπληρώσουν τις ευθύνες τους χρησιμοποιώντας μια ποικιλία διαδραστικής εκπαίδευσης για να ενσταλάξουν αυτή τη νέα γνώση, όπως τα παιχνίδια και ο ρόλος, για να διευκολύνουν την εμπλοκή, τη συμμετοχή και το άνοιγμα.

Ο σχεδιασμός ενός προγράμματος ευαισθητοποίησης θα αναγνωρίσει και θα αντικατοπτρίζει την ανθρώπινη ψυχολογία, τις γνωστικές ικανότητες, τις κοινωνικές συμπεριφορές και τα σύγχρονα εργασιακά περιβάλλοντα. Τα προγράμματα θα πρέπει να παρέχουν στους εργαζόμενους αυτονομία, συμμετοχή και ιδιοκτησία, με τους στόχους ασφαλείας να ευθυγραμμίζονται με τα κίνητρα των επιχειρήσεων και τις οργανωτικές δομές. Τέλος, η διοίκηση πρέπει να αποτελέσει παράδειγμα για την οργάνωση διαθέτοντας επαρκείς πόρους και προσφέροντας συνεχή καθοδήγηση και υποστήριξη. Για το σκοπό αυτό, ειδικοί, ρεαλιστικοί και μετρήσιμοι στόχοι, καθώς και η κατάλληλη επικοινωνία με τους εργαζόμενους είναι καθοριστικής σημασίας για την επιτυχία οποιουδήποτε προγράμματος ενημέρωσης. Οι παράγοντες επιτυχίας για ένα καλό πρόγραμμα ευαισθητοποίησης σχετικά με την ασφάλεια μπορεί να συστηματοποιηθούν με τον ακόλουθο τρόπο:

- **Παραμείνετε συναφείς** - τόσο όσον αφορά τις νέες απειλές, όσο και τις αλλαγές των εργαζομένων και της οργάνωσης. Θα πρέπει να περιληφθούν όλες οι απαραίτητες γνώσεις για διαφορετικό προσωπικό, μαζί με το όραμα της διοίκησης για ρόλους και ευθύνες.
- **Σχέδιο φυσικής μάθησης** - πρέπει να αφιερωθεί επαρκής χρόνος για την κατάρτιση. Το πρόγραμμα θα πρέπει να επηρεάζει θετικά τη γνώση, τη στάση και τη συμπεριφορά των συμμετεχόντων.
- **Συμπεριλάβετε ολόκληρο τον οργανισμό** - η ανοικτή επικοινωνία και η ευαισθητοποίηση σε ολόκληρο τον οργανισμό επιτρέπει την εσωτερική συνοχή και την ανατροφοδότηση για βελτιώσεις.
- **Μοιραστείτε τον ενθουσιασμό** - ένα δημιουργικό, ποικίλο και προσαρμοσμένο εκπαιδευτικό πρόγραμμα μπορεί να επιτύχει περισσότερα. Οι μέθοδοι εξαρτώνται από τις επιθυμίες και τον προϋπολογισμό του οργανισμού, αλλά μπορούν να περιλαμβάνουν ένα ή περισσότερα παιχνίδια, ιστορίες, ταινίες και μελέτες περιπτώσεων, εργαστήρια και ασκήσεις κρίσης.

11.1.1 Η σχέση μεταξύ του πολιτισμού της ασφάλειας στον κυβερνοχώρο και της ευαισθητοποίησης της ασφάλειας πληροφοριών

Τα πλαίσια και οι εκπαιδευτικές δραστηριότητες για την ευαισθητοποίηση σχετικά με την Cyber / Information Security είναι καλά καθιερωμένες στρατηγικές για την αύξηση της ανθεκτικότητας του προσωπικού στον κυβερνοχώρο. Η ευαισθητοποίηση σχετικά με την ασφάλεια μπορεί να οριστεί ως "μια συνεχής διαδικασία μάθησης που έχει νόημα στους αποδέκτες και προσφέρει μετρήσιμα οφέλη στον οργανισμό από τη διαρκή αλλαγή συμπεριφοράς". Η διαφορά μεταξύ της ευαισθητοποίησης CSC και Cyber Security είναι ότι η ευαισθητοποίηση για την Cyber Security είναι ένα μόνο στοιχείο ή υποσύνολο CSC. Η ευαισθητοποίηση των εργαζομένων είναι ένα από τα στοιχεία της CSC, ωστόσο, η CSC παίρνει μια ευρύτερη και βαθύτερη άποψη της στάσης του κυβερνοχώρου για την ασφάλεια ενός υπαλλήλου, συμπεριλαμβάνοντας συμπεριφορές, στάσεις, κανόνες, πεποιθήσεις, αλληλεπιδράσεις κλπ., Καθώς και ευαισθητοποίηση.

11.2 Εργαλεία, πλαίσια και μεθοδολογίες

Ο μετασχηματισμός της κουλτούρας ασφάλειας είναι σύνθετος και απαιτεί μεταβαλλόμενες αξίες και πεποιθήσεις, αλλάζοντας τη συμπεριφορά και τελικά διαμορφώνοντας τις υποκείμενες υποθέσεις σχετικά με την ασφάλεια στον κυβερνοχώρο. Υπάρχουν διαφορετικές προσεγγίσεις σχετικά με το πώς ακριβώς θα αναπτυχθεί και θα προωθηθεί μια CSC. Έχει προταθεί το ακόλουθο συνολικό πλαίσιο που προσφέρει έναν βήμα-βήμα οδηγό για τη συστηματοποίηση των παραπάνω συμβουλών:

- **Δέσμευση κορυφαίας διαχείρισης** - ως πρώτο βήμα, η ανώτερη διοίκηση πρέπει να θέσει τη νέα κατεύθυνση της κουλτούρας ασφάλειας μέσω δηλώσεων, συνθημάτων, εκστρατειών ευαισθητοποίησης, παραδειγμάτων, ανταμοιβών και κυρώσεων. Η οργανωτική νοοτροπία θα αλλάξει, θα διαμορφωθεί από τη δέσμευση αυτή και θα ενισχυθεί μέσω μιας πολιτικής εταιρικής ασφάλειας πληροφοριών.
- **Καθορίστε το πρόβλημα στο επιχειρηματικό πλαίσιο** - δεύτερον, οι στάσεις και οι συμπεριφορές των εργαζομένων

πρέπει να αξιολογούνται στο πλαίσιο της συγκεκριμένης οργάνωσης.

- **Αξιολόγηση της τρέχουσας κατάστασης** - Πριν ληφθούν οποιαδήποτε περαιτέρω βήματα, θα πρέπει να αξιολογηθεί η τρέχουσα κατάσταση της κουλτούρας ασφάλειας στον οργανισμό με βάση τις υπάρχουσες (1) αξίες, πολιτικές και διαδικασίες, (2) πρακτικές, (3) υποθέσεις / πεποιθήσεις, 4) εξετάζεται η γνώση.
- **Καθορίστε την ιδανική κατάσταση** - πρέπει να οραματιστεί μια ιδανική κατάσταση για την επιχειρηματική διαδικασία, οριζόμενο κατά μήκος των ίδιων 4 γραμμών. Όλες αυτές οι πτυχές πρέπει να προσεγγίζονται με συγκεκριμένο και μετρήσιμο στόχο.
- **Καθορίστε τα απαραίτητα βήματα** - πρέπει να οριστούν σαφώς τα βήματα για να μετακινηθείτε από την τρέχουσα κατάσταση σε μια ιδανική κατάσταση. Θα πρέπει να γίνει μια στροφή από τις αφηρημένες τιμές σε συγκεκριμένους στόχους με σαφή προτεραιότητα SMART.⁹⁹ Η πολιτική ασφάλειας μπορεί να χρησιμοποιηθεί εδώ για να διαμορφώσει τους μελλοντικούς στόχους, τις διαδικασίες και την εκπαίδευση των εργαζομένων.
- **Εκπαιδεύστε τους υπαλλήλους** - η εκπαίδευση αποτελεί βασικό στοιχείο για να πείσει το προσωπικό για την ανάγκη αλλαγής της υπάρχουσας κουλτούρας ασφάλειας, για να μάθει τι πρέπει να κάνει, πώς να το κάνει και γιατί πρέπει να γίνει. Θα πρέπει να σχεδιαστεί το εκπαιδευτικό πρόγραμμα με αυτούς τους στόχους. Θυμηθείτε ότι οι αλλαγές πολιτισμού απαιτούν χρόνο και επιμονή. Οι εργαζόμενοι πρέπει να γνωρίζουν ότι η σημερινή κουλτούρα δεν είναι πλέον κατάλληλη.
- **Καθορίστε τις μετρήσεις αλλαγής πολιτισμού** - οι μετρήσεις θα πρέπει να χρησιμοποιούνται για τη μέτρηση της ανάπτυξης της CSC και να παρέχουν συνεχή ανατροφοδότηση στους υπαλλήλους και τη διοίκηση.
- **Ανατροφοδότηση, ανταμοιβές και τιμωρίες** - Θα παρέχεται συνεχής ανατροφοδότηση στους υπαλλήλους από τη διοίκηση μέσω ανταμοιβών και κυρώσεων με βάση μετρήσεις απόδοσης.

- **Επανεξέταση και βελτίωση** - οι αρχικά ορισμένοι στόχοι ενδέχεται να απαιτούν αναθεώρηση εάν είναι αδύνατο να επιτευχθούν ή απαράδεκτοι για τους εργαζομένους. Σε ορισμένες περιπτώσεις, η τελική κουλτούρα που επιδιώκεται μπορεί να ενισχυθεί μέσω της επαναδιαπραγμάτευσης.

Άλλα πλαίσια για την ανάπτυξη και τη μετατροπή της CSC στους οργανισμούς περιλαμβάνονται στα παραρτήματα της παρούσας έκθεσης.

11.3 Μέτρηση επιτυχημένης απόδοσης

Οι μετρήσεις έχουν ζωτικό ρόλο να διαδραματίσουν στην αλλαγή του πολιτισμού και την ασφάλεια των πληροφοριών, καθώς βοηθούν στην αξιολόγηση της τρέχουσας και επιθυμητής CSC, καθώς και στην πρόοδο που σημειώνεται. Προσφέρουν χρήσιμες πληροφορίες για τους υπαλλήλους και τη διοίκηση και μπορούν να επιβεβαιώσουν την αποτελεσματικότητα των μέτρων ασφαλείας που εφαρμόζονται στο πλαίσιο της νέας κουλτούρας στον κυβερνοχώρο, υποδεικνύοντας πόσο επιτυχημένα είναι.

Οι καλές μετρήσεις πρέπει να είναι μετρήσιμες, επαναλαμβανόμενες και συγκρίσιμες ώστε να επιτρέπουν ακριβείς γνώσεις. Πρέπει επίσης να είναι εύκολα προσβάσιμα, συναφή και να προσφέρουν χρήσιμη ανατροφοδότηση για βελτίωση.¹⁰³ Πρέπει να δοθεί ιδιαίτερη προσοχή για να εξασφαλίσει όλες τις επιλεγμένες μετρήσεις είναι σχετικές για την CSC. Για παράδειγμα, οι μετρήσεις όπως ο αριθμός των εργαζομένων που συμμετέχουν στην εκπαίδευση στον κυβερνοχώρο ή τα αποτελέσματα των ερωτηματολογίων σχετικά με τις γνώσεις και τις τεχνικές δεξιότητες στον κυβερνοχώρο είναι ποσοτικοποιήσιμα και συγκρίσιμα και σχετίζονται με τον καθορισμό του επιπέδου γνώσης και ευαισθητοποίησης των εργαζομένων. Ωστόσο, δεν επαρκούν για την κατανόηση της CSC, καθώς δεν σχετίζονται με τη συμπεριφορά των εργαζομένων στην πράξη, ούτε με τις στάσεις και τις πεποιθήσεις τους.

Η συμπεριφορά των εργαζομένων μπορεί να εξεταστεί με τη μέτρηση της επίδρασης της CSC στην πράξη. Από την άποψη αυτή, ορισμένα εργαλεία λογισμικού στον κυβερνοχώρο συλλέγουν χρήσιμα δεδομένα σχετικά με τον αριθμό των επιθέσεων στο δίκτυο του οργανισμού, τον αριθμό των παρεμποδισμένων επιθέσεων και τον

χρόνο που χρειάστηκε για να τους αναγνωρίσουν. Επιπλέον, οι ψεύτικες επιθέσεις ηλεκτρονικού "ψαρέματος" (phishing) και κακόβουλου λογισμικού που αποστέλλονται στους ίδιους τους υπαλλήλους της εταιρείας μπορούν επίσης να δώσουν μια εικόνα για τη συμπεριφορά του προσωπικού στον κυβερνοχώρο. Η συμμόρφωση μπορεί επίσης να μετρηθεί με τεχνικά εργαλεία που παρακολουθούν τις δραστηριότητες των εργαζομένων.

Τέλος, η μέτρηση της στάσης και των πεποιθήσεων σχετικά με την ασφάλεια του κυβερνοχώρου εντός του οργανισμού είναι επίσης απαραίτητη, ωστόσο, είναι πιο δύσκολο να προσδιοριστεί ποσοτικά και να συγκριθεί. Τα ερωτηματολόγια και / ή οι δίαυλοι επικοινωνίας μπορούν να χρησιμοποιηθούν για να μελετήσουν τις αντιλήψεις και τις αντιλήψεις των εργαζομένων σχετικά με ορισμένες βασικές πτυχές της CSC, συμπεριλαμβανομένων των απειλών στον κυβερνοχώρο, τη δέσμευση διαχείρισης, τη διαθεσιμότητα των απαραίτητων πόρων, τα τρέχοντα, αποτελεσματικά και εύχρηστα τεχνικά εργαλεία και πολιτικές, την εμπλοκή και τις ευθύνες όσον αφορά την ασφάλεια του κυβερνοχώρου, καθώς και την αποτελεσματικότητα και το άνοιγμα της επικοινωνίας στο θέμα εντός του οργανισμού. Οι πτυχές που σχετίζονται στενότερα με τις πεποιθήσεις και τις υποθέσεις των εργαζομένων μπορούν επίσης να εξεταστούν εξετάζοντας τις επιδιωκόμενες δραστηριότητες των εργαζομένων, τα γενικά αισθήματα και τα συναισθήματα σχετικά με την οργανωτική ασφάλεια και πρακτικές, την αίσθηση του ανήκειν, την κοινωνική επικοινωνία και την αναφορά συμβάντων. κανόνες της οργανωτικής συμπεριφοράς και των πρακτικών μέσα στην εταιρεία τους.

12 Συστάσεις

Αυτή η αναφορά περιγράφει καλές πρακτικές, μεθοδολογικά εργαλεία και καθοδήγηση βήμα προς βήμα για όσους επιθυμούν να ξεκινήσουν ή να ενισχύσουν το δικό τους πρόγραμμα στον τομέα της πολιτιστικής ασφάλειας στον κυβερνοχώρο, περιλαμβανομένων πόρων για την παραγωγή επιχειρηματικής υπόθεσης για την εξασφάλιση χρηματοδότησης για ένα τέτοιο πρόγραμμα. Η επιτυχία ενός προγράμματος CSC βασίζεται σε ορισμένα βασικά στοιχεία, τα οποία προσδιορίζονται και περιγράφονται παρακάτω.

Συστάσεις για ένα επιτυχημένο πρόγραμμα CSC:

- Ασφαλής αγορά στο υψηλότερο επίπεδο**

Η ανώτερη αγορά στο υψηλότερο οργανωτικό επίπεδο είναι απαραίτητη για την επιτυχία του προγράμματος. Απαιτούνται ανώτερα ποσά που μπορούν να λειτουργήσουν ως πρωταθλητές του προγράμματος και να οδηγήσουν σε παράδειγμα, επηρεάζοντας έτσι τη συμπεριφορά του προσωπικού προς το πρόγραμμα.

- Ακολουθήστε το πλαίσιο CSC για την υλοποίηση του προγράμματος**

Το πλαίσιο CSC που παρουσιάζεται στην παρούσα έκθεση παρέχει μια διαδικασία καθοδήγησης του προγράμματος CSC με τη μορφή μιας βήμα προς βήμα εφαρμογής επικεντρωμένης σε συγκεκριμένες δραστηριότητες, την εφαρμογή τους και τη μέτρηση των επιπτώσεων.

- Γνωρίστε την οργάνωσή σας για να εξασφαλίσετε επιτυχία**

Αυτό το βήμα στο πλαίσιο του CSC είναι το κλειδί για την επιτυχία του προγράμματος, διότι θα ενημερώνει τις διαδικασίες λήψης αποφάσεων που καθορίζουν τους στόχους, τα κριτήρια επιτυχίας και το κοινό-στόχο του προγράμματος CSC.

- Μετρήστε το τρέχον επίπεδο ασφάλειας του κυβερνοχώρου του κοινού-στόχου**

Ο υπολογισμός του τρέχοντος επιπέδου CSC του κοινού-στόχου σας θα σας βοηθήσει να μετρήσετε την επίδραση των δραστηριοτήτων που επιλέξατε να εφαρμόσετε και, συνεπώς, τον αντίκτυπο του προγράμματος CSC.

- **Σχεδιάστε τις καλές πρακτικές που προσδιορίζονται στην παρούσα έκθεση**

Έχουν εντοπιστεί ορισμένες καλές πρακτικές από συνεντεύξεις με επαγγελματίες CSC σε οργανισμούς σε ολόκληρη την Ευρώπη και επιτόπια έρευνα που θα βοηθήσει στον σχεδιασμό και την εκτέλεση ενός επιτυχημένου προγράμματος CSC.

13 Βιβλιογραφία

1. Abawajy, J., 'User preference of cyber security awareness delivery methods, Behaviour and information technology', Vol. 33, No 3, 2014, pp. 237-248.
2. Albrechtsen, E., & Hovden, J., 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An Intervention Study', Computer and Security, Vol. 29, No 4, pp. 432– 445.
3. Alfawaz, S., Nelson, K., Mohannak, K., 'Information security culture: A Behaviour Compliance Conceptual Framework', 8th Australasian Information Security Conference, Brisbane, Australia, 2010.
4. Alnatheer, M., 'A Conceptual Model to Understand Information Security Culture', Int. J. Soc. Sci. Humanit., Vol. 4, No 2, 2014, pp. 104–107.
5. Alnatheer, M., Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia, 2012.
6. Anwar, M., He, W., Ash, I., Yuan, X., Li, L. & Xu, L., 'Gender difference and employees' cybersecurity behaviors', Computers in Human Behavior, 2017.
7. Ardichvili, A., Page, V., & Wentling, T., 'Motivation and barriers to participation in virtual knowledge-sharing communities of practice', Journal of Knowledge Management, Vol. 7, No 1, 2003.
8. Argyris, C., & Schön, D., Organizational learning, Addison-Wesley, Reading, 1978.
9. Asch, S., 'Studies of independence and conformity: A minority of one against a unanimous majority', Psychological monographs: General and applied, Vol. 70, No 9, 1956, pp. 1-70.
10. Ashenden, D., 'Information Security management: A human challenge?' Information Security Technology Report, Vol. 13, No 4, 2008, pp. 195-201.
11. Ashenden, D., & Sasse, A., 'CISOs and Organisational Change: Their Own Worst Enemy?', Computers & Security, Elsevier, 2013.
12. Atoum, I., Otoom, A., & Ali, A., 'A holistic cyber security implementation framework', Information Management & Computer Security, Vol. 22, No 3, 2014, pp. 251-264.
13. Australian Department of Defence, Human Factors and Information Security, no date.
14. Beaument, A., Sasse, A., & Wonham, M., The Compliance Budget: Managing Security Behaviour in Organisations, 2008.
15. Business Software Alliance, Information Security Governance, 2013.
16. Cheng, Y., Li, W., Holm, E., & Zhai, Q., 'Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory', Computer Security, Vol. 39, 2013, pp. 447– 459.
17. Chipperfield, C., & Furnell, S., 'From security policy to practice: Sending the right messages', Computer Fraud Security, Vol. 2010, No 3, 2010, pp. 13–19.
18. CISCO, Cybersecurity Management Program, 2017.
19. Cook, S., & Yanow, D., 'Culture and organizational learning'. Journal of Management Inquiry, Vol. 2, No 4, 1993, pp. 373–390.
20. D'Arcy, J., Hovav, A., & Galletta, D., 'User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A

- Deterrence Approach', *Information Systems Research*, Vol. 20, No 1, 2009, pp. 79-98.
21. Das, S., Kim, T., Dabbish, L., & Hong, J., The Effect of Social Influence on Security Sensitivity, *Symposium on Usable Privacy and Security (SOUPS)*, Menlo Park 2014.
 22. Da Veiga, *Information Security Culture Assessments*, 2014.
 23. Deal, T., & Kennedy, A., *Corporate cultures*, Addison-Wesley, Reading, 1982.
 24. Deal, T., & Kennedy, A., *The new corporate cultures*, Perseus, New York, 1999.
 25. Denison, D., *Corporate Culture and Organizational Effectiveness*, Wiley, New York, 1990.
 26. Deloitte, *Risk Intelligent governance in the age of cyber threats*, 2012.
 27. Detert, J., Schroeder, R., & Mauriel, J., 'A Framework for Linking Culture and Improvement Initiatives in Organisations'. *Academy of Management Review*, Vol. 25, No 4, 2000, pp. 850-863.
 28. Dimensional Research, *Trends in Security Framework Adoption*, 2016.
 29. Dodge, R., Carver, C., & Ferguson, A.J., 'Phishing for User Security Awareness', *Computers and Security*, Vol. 26, 2007, pp. 73-80.
 30. Dojkovski, S., Lichtenstein, S., & Warren, M., Fostering information security culture in small and medium size enterprises: an interpretive study in Australia, in *Proceedings of the 15th European Conference on Information Systems*, University of St. Gallen, St. Gallen, 2007, pp. 1560-1571.
 31. Ernst & Young, *Cyber Program Management*, 2014.
 32. Eminagaoglu, M., Ucar, E., & Eren, S., 'The positive outcomes of information security awareness training in companies – a case study'. *Information Security Technical Report*, Vol. 4, 2010, pp. 1–7.
 33. ENISA, *Measurement Framework and Metrics for Resilient Networks and Services: Challenges and recommendations*, 2011.
 34. ENISA, *Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures*, 2016.
 35. Fagerström, A., *Creating, Maintaining and Managing an Information Security Culture*, 2013.
 36. Fitzgerald, T., Building Management Commitment through Security Councils, or Security Council Critical Success Factors, In H. F. Tipton (Ed.), *Information Security Management Handbook*, Auerbach Publications, Hoboken, 2007, pp. 105-121.
 37. Foley & Lardner LLP, *Taking Control of Cybersecurity*, 2015.
 38. Furnell, S., *A Conceptual Model for Cultivating an Information Security Culture*, 2015.
 39. Furnell, S., & Clarke, N., *Organisational Security Culture: Embedding Security Awareness, Education and Training*, 2005.
 40. Furnell, S., & Thomson, K., 'From culture to disobedience: Recognising the varying user acceptance of IT security', *Computer Fraud Security*, Vol. 2009, No 2, 1999, pp. 5–10.
 41. Geertz, C., *The interpretation of cultures*, Basic Books, New York, 1973.
 42. Goffman, E., *The presentation of self in everyday life*, Doubleday, New York, 1959.

43. Goffman, E., *Interaction ritual*, Hawthorne, Aldine, 1967.
44. Greene, G., & Arcy, J., 'Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance', 2010, pp. 1–8.
45. Halevi, T., et al., 'Cultural and Psychological Factors in Cyber-Security', iiWAS '16, November, 2016.
46. Hearth, T., & Rao., 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness', *Decision Support Systems*, Vol. 47, No 2, 2009a, pp. 154-165.
47. Hearth, T., & Rao, H., 'Protection motivation and deterrence: a framework for security policy compliance in organizations', *European Journal of Information Systems*, Vol. 18, No 2, 2009b, pp. 106-125.
48. Henderson, R., & Clark, K., 'Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms'. *Administrative Science Quarterly*, Vol. 35, 1990, pp. 9–30.
49. Herley, C., 'More is not the answer', *IEEE Security & Privacy*, Vol. 12, No 1, 2014, pp. 14-19.
50. Hewlett Packard, Awareness is only the first step, 2015.
51. Homans, G., *The human group*, Harcourt Brace Jovanovich, New York, 1950.
52. Hong, J., Das, S., Kim, T., Dabbish, L., *Social Cybersecurity: Applying Social Psychology to Cybersecurity*, Human Computer Interaction Institute, Carnegie Mellon University, 2015.
53. IBM, X-Force Threat Intelligence Index, 2017.
54. ISC, Global Information Security Workforce Study, 2015.
55. Ifinedo, P. 'Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory'. *Computers & Security*, Vol. 31, No 1, 2012, pp. 8395.
56. Jones, M., Moore, M., & Snyder, R., (Eds.) *Inside organizations*, Sage, Thousand Oaks, 1988.
57. Karahanna, E., Straub, D., Chervany, N., 'Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs', *MIS Quarterly*, Vol. 23, No 2, 1999.
58. Kilmann, R., & Saxton, M., *The Kilmann-Saxton culture gap survey*. Organizational Design Consultants, Pittsburgh, 1983.
59. Koh, K., Ruighaver, A., Maynard, S., & Ahrnad, A, *Security Governance: Its impact on Security Culture*, 3rd Australian Information Security Management Conference, Perth, 2005.
60. Kruger, H., & Kearney, W., 'A prototype for assessing information security awareness'. *Computers & Security*, Vol. 25, No 4, 2006, pp. 289 – 296.
61. Lacey, D., *Managing the Human Factor in Information Security: How to win over staff and influence business managers*, Wiley, 2009a.
62. Lacey, D., 'Understanding and Transforming Organisational Culture', *Proceedings of the Third International Symposium on Human Aspects of Information Security & Assurance*, 2009b.
63. Leidner, D., & Kayworth, T., 'A review of culture in information systems research: towards a theory of information technology culture conflict', *MIS Quarterly*, Vol. 30, No 2, 2006, pp. 357-399.

64. Lim, J., Chang, S., Maynard, S., & Ahmad, A, Exploring the Relationship between Organizational Culture and Information Systems Security Culture, in Proceedings of the 7th Australian Information Security Management Conference, Edith Cowan University, 2009, pp. 87–97.
65. Malandrin, L., & Carvalho, T., 'Maintaining Information Security in the New Technological Scenario', Vol. 5, No 3, 2013.
66. Martins, A., & Elof, J., Information Security Culture, 2002, p. 204-206.
67. Maynard, S., Exploring Organisational Security Culture – Research Model, 2002.
68. Maynard, S., & Ruighaver, A, Evaluating IS Security Policy Development, 2002.
69. McBride, M., Carter, L., & Warkentin, M., The Role of Situational Factors and Personality on Cybersecurity Policy Violation, Institute for Homeland Security Solutions, 2012.
70. McKinsey, Meeting the Cybersecurity Challenge, 2011.
71. Ministry of Finance of Finland, Effective Information Security, 2009.
72. Morris, M., Venkatesh, V., & Ackerman, P., 'Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior'. IEEE Transactions on Engineering Management, Vol. 52, No 1, 2005, pp. 69-84.
73. Ngo, L., IT Security Culture Transition Process, 2008.
74. Niekerk, J. Van., & Solms, R. Von., An holistic framework for the fostering of an information security subculture in organizations. Information Security South Africa (ISSA), 2005.
75. Nosworthy, J., Implementing information security in the 21st century - do you have the balancing factors?, 2000.
76. OECD, Digital Security Risk Management for Economic and Social prosperity, 2015.
77. O'Neill, B., Developing a Risk Communication Model to Encourage Community Safety from Natural Hazards, Fourth NSW Safe Communities Symposium, Sydney, 2004
78. Pahnila, S., Siponen, M., & Mahmood, A., Employees' behavior towards IS security policy compliance, Hawaii, 2007.
79. PCI Security Standards Council, Best Practices for Implementing a Security Awareness Program, 2014.
80. Peters, T., & Waterman, R., In search of excellence, HarperCollins, New York, 1982.
81. Ponemon Institute, The human factor in data protection [online], 2012.
82. Ponemon Institute, Cost of Cyber Crime Study and the Risk of Business Innovation, 2016.
83. Ponemon Institute, Cost of Data Breach Study, 2016.
84. Ponemon Institute, Cost of Data Breach Study, 2017.
85. Post, G., & Kagan, A., 'Evaluating information security trade-offs: restricting access can interfere with user tasks', Computers & Security, Vol. 26, No 3, 2007.

86. Ramachandran, S., Srinivasan, V., & Goles, T, 'Information Security Cultures of Four Professions: A Comparative Study'. Paper presented at the 41st Hawaii International Conference on System, Hawaii, 2004.
87. RAND, Cybersecurity economic issues, 2008.
88. Reid, R., & Van Niekerk, J., 'A Cyber Security Culture Fostering Campaign through the Lens of Active Audience Theory', HAISA, 2015, pp. 34-44.
89. Robbins, S., Organizational Behavior: Concepts, Controversies, and Applications (Fourth Edition ed.), Prentice Hall, New Jersey, 1989.
90. Roer, K., How to build and maintain security culture, 2014.
91. Roer, K., & Petrič, G., CLTRe Indepth insights into the human factor: The 2017 Security Culture Report, 2017.
92. Ross, S., & Masters, R., Creating a Culture of Security, 2011.
93. Rowe, D., Lunt, B., & Ekstron, J., The Role of Cyber-Security in Information Technology Education, 2011.
94. RSA, Translating Security Leadership into Board Value, 2017.
95. Sasse, A., 'Scaring and bullying people into security won't work', IEEE Security & Privacy, Vol. 3, 2015, pp. 80–83.
96. Sasse, A., & Smith, M., 'The Security-Usability Tradeoff Myth', IEEE Security & Privacy, Vol. 14, No 5, 2016, pp. 11-13.
97. Schein, E., Coming to a New Awareness of Organizational Culture, 1984, pp. 2-3.
98. Schein, E., Organizational Culture and Leadership, Jossey-Bass, San Francisco, 1992.
99. Schein, E., 'Empowerment, coercive persuasion and organizational learning: do they connect?', The Learning Organization, Vol. 6, No 4, 1999, pp. 163–172.
100. Schein, E., Organizational Culture and Leadership, 2004, p. 334.
101. Schlienger, T., Tool Supported Management of Information Security Culture, 2005.
102. Schlienger, T., & Teufel, S., Information Security Culture - the Social-Cultural Dimension in Information Security Management, 2002.
103. Siponen, M., & Willison, R., 'Information security management standards: Problems and solutions', Information & Management, Vol. 46, No 5, 2009, pp. 267-270.
104. Smircich, L., 'Concepts of culture and organizational analysis'. Administrative Science Quarterly, Vol. 28, 1983, pp. 339-358.
105. Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J., 'Analysis of end user security behaviors', Computers & Security, Vol. 24, No 2, 2005.
106. Susanto, H., Almunawar, M., & Tuan, Y., 'Information security management system standards: A comparative study of the big five', International Journal of Electrical Computer Sciences, Vol. 11, No 5, 2011, pp. 23-29.
107. Symantec, Internet Security Threat Report, 2017.
108. Tarimo, C., ICT Security Readiness Checklist for Developing Countries: A Social-Technical Approach, 2006.
109. Thomson, K., & von Solms, R., 'Information security obedience: a definition', Computer Security, Vol. 24, No 1, 2005, pp. 69–75.

110. Thomson, K., von Solms, R., & Louw, L., 'Cultivating an organizational information security culture', *Computer Fraud Security*, October, 2006, pp. 49–50.
111. Thompson, R., Higgins, C., Howell, J., 'Influence of experience on personal computer utilization', *Journal of Management Information Systems*, Vol. 11, No 1, 1994.
112. Trice, H., & Beyer, J., *Using six organizational rites to change culture*, Jossey-Bass, San Francisco, 1985, pp. 370–399.
113. Trice, H., & Beyer, J., *The cultures of work organizations*, Prentice Hall, Englewood Cliffs, 1993.
114. Van den Steen, E., *On the Origin of Shared Beliefs (and Corporate Culture)*, MIT School of Management, 2005.
115. Van Niekerk, J., 'Establishing an information security culture in organizations: an outcomes based education approach', PhD diss., Nelson Mandela Metropolitan University, 2005.
116. Van Niekerk, J., *A Holistic Framework for Fostering IS sub-culture in organizations: an outcomes based education approach*, 2005.
117. Van Niekerk, J., & von Solms, R., *An Holistic Framework for the Fostering of an Information Security SubCulture in Organizations*, Centre for Information Security Studies, Nelson Mandela Metropolitan University, 2005.
118. Venkatesh, V., Morris, M., Davis, G., & Davis, F., 'User acceptance of information technology: toward a unified view', *MIS Quarterly*, Vol. 27, No 3, 2003.
119. Verizon, *Data Breach Investigations Report*, 2016.
120. Von Solms, B., 'Information Security -- the Third Wave?', *Computers & Security*, Vol. 19, No 7, 2000, pp. 615620.
121. Von Solms, R., 'Information security management: why standards are important', *Information Management & Computer Security*, Vol. 7, No 1, 1999, pp. 50-58.
122. Vroom, R., & von Solms, R., 'Towards information security behavioural compliance', *Computer Security*, vol. 23, no. 3, 2004, pp. 191–198.
123. Wasko, M., Faraj, S., 'It is what one does: why people participate and help others in electronic communities of practice', *Journal of Strategic Information Systems*, Vol. 9, 2000.
124. Weick, K., *Sensemaking in organizations*, Sage, Thousand Oaks, 1995.
125. World Economic Forum, *A Framework for Assessing Cybersecurity Resilience*, 2016.
126. Yanus, S., & Shin, R., *Critical Success Factors for Managing an Information Security Awareness Programme*, 2007.