ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
Τμήμα Ναυτιλίας και Επιχειρηματικών Υπηρεσιών

&

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
Τμήμα Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής

ΔΙΙΔΡΥΜΑΤΙΚΟ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΣΤΗ ΝΑΥΤΙΛΙΑ ΚΑΙ ΤΙΣ ΜΕΤΑΦΟΡΕΣ»

ΤΙΤΛΟΣ

Ασφάλεια Κυβερνοχώρου στη Ναυτιλία

ΤΙΤΛΟΣ ΑΓΓΛΙΚΑ

Cyber Security in Maritime Industry.

Ονοματεπώνυμο Σπουδαστή:

Αναστασία Δημακοπούλου

Ονοματεπώνυμο Υπεύθυνου Καθηγητή:

Δρ. Νικήτας Νικητάκος

Δρ. Δημήτρης Παπαχρήστος

ΔΙΑΤΡΙΒΗ

Οκτώβριος 2019

Μεταπτυχιακή Διατριβή που υποβάλλεται στο καθηγητικό σώμα για την μερική εκπλήρωση των υποχρεώσεων απόκτησης του μεταπτυχιακού τίτλου του Διϊδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών «Νέες Τεχνολογίες στη Ναυτιλία και τις Μεταφορές» του Τμήματος Ναυτιλίας και Επιχειρηματικών Υπηρεσιών του Πανεπιστημίου Αιγαίου και του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής του Πανεπιστημίου Δυτικής Αττικής.

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

Η κάτωθι υπογεγραμμένη Αναστασία Δημακοπούλου του Θωμά με αριθμό μητρώου 78 φοιτήτρια του Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών Τμήματος «Νέες Τεχνολογίες στη Ναυτιλία και τις Μεταφορές» του Τμήματος Ναυτιλίας και Επιχειρηματικών Υπηρεσιών του Πανεπιστημίου Αιγαίου και του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής του Πανεπιστημίου Δυτικής Αττικής πριν αναλάβω την εκπόνηση της Διπλωματικής Διατριβής μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

- Η Διπλωματική Διατριβή (Δ.Δ.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και των Ιδρυμάτων και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.
- Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Δ.Δ.., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.
- Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που του έχει απονείμει ο μεταπτυχιακός τίτλος , αυτός ανακαλείται με απόφαση της Ε.Δ.Ε. του ΠΜΣ. Η Ε.Δ.Ε. με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Δ.Δ. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Δ.Δ. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στον Κανονισμό Λειτουργίας του Π.Μ.Σ..

Η Δηλούσα

Αναστασία Δημακοπούλου

Ημερομηνία

Πίνακας περιεχομένων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
Τμήμα Ναυτιλίας και Επιχειρηματικών Υπηρεσιών
&
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
Τμήμα Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής

Περίληψη

Στον κόσμο της πληροφορίας και της ηλεκτρονικής ανταλλαγής δεδομένων, η ανάγκη για ασφάλεια ολοένα και αυξάνεται. Ο επιχειρησιακός κόσμος δείχνει ολοένα και περισσότερο ενδιαφέρον αναφορικά με την ασφάλεια στον κυβερνοχώρο. Είναι δεδομένο ότι η τεχνολογία εξελίσσεται με πολύ γρήγορους ρυθμούς και αυτό καθιστά πιο δύσκολη την προσαρμογή των ανθρώπων με αυτή. Ο κλάδος της ναυτιλίας είναι ένα μέρος του επιχειρησιακού κόσμου το οποίο εκτίθεται καθημερινά σε κινδύνους και αποτελεί παγκόσμιο προβληματισμό. Ο IMO θεσπίζοντας κανονισμούς, έχει ως στόχο να παρέχει υψηλή ασφάλεια στον θαλάσσιο κυβερνοχώρο. Οι ναυτιλιακές εταιρείες ακολουθούν επίσης τις κατευθυντήριες γραμμές της BIMCO οι οποίες έχουν εγκριθεί από τον IMO και με αυτές καλύπτονται σε ότι αναφορά το κομμάτι του ISM και ασφαλιστικά. Οι νηογνώμονες από την άλλη, βοηθούν τις εταιρείες να εφαρμόζουν σωστά τις διαδικασίες και να κάνουν δοκιμές διείσδυσης στα συστήματα τους. Παίζουν δηλαδή ρόλο συμβουλευτικό. Τέλος, στη παρούσα εργασία έχει ως στόχο να απαντήσει σε συγκεκριμένα ερωτήματα τα οποία επικεντρώνονται στην ελληνική ναυτιλία. Τα ερωτήματα αφορούν τις διαδικασίες και τους κανονισμούς που εφαρμόζουν οι εταιρείες, ποιους παράγοντες χρησιμοποιούν ώστε να ενδυναμώνουν τα συστήματά τους και τέλος πως επιτυγχάνουν ασφαλιστική κάλυψη σε περίπτωση επίθεσης.

Λέξεις κλειδιά: Κυβερνοασφάλεια, προστασία δεδομένων, ασφάλεια δεδομένων, ασφάλεια πληροφοριών, διαχείριση κινδύνου, αξιολόγηση κινδύνου, εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, συστήματα ασφαλείας, σύστημα διαχείρισης της ασφάλειας, απειλές, δοκιμή διείσδυσης, ασφάλειες, νηογνώμονες, κανονισμοί, διαδικασίες, κυβερνοασφάλεια στη ναυτιλία, πρότυπα διαχείρισης της ασφάλειας.

Abstract

In the world of information and electronic data sharing, the need for security is increasing. The business world is increasingly interested in cybersecurity. It is a given that technology is evolving at a very fast pace and this makes it harder for people to adapt to it. The shipping industry is a part of the business world that is at risk every day and is a global concern. IMO, by adopting regulations, aims to provide high security in the maritime cyberspace. The shipping companies also follow the guidelines of BIMCO that have been approved by the

IMO and are covered by the ISM code and insurance. On the other hand, classification societies help companies to properly apply procedures and perform penetration tests on their systems. That is, they play an advisory role. Finally, the purpose of the present work is to answer specific questions that focus on Greek shipping. The questions relate to the procedures and regulations applied by companies, what factors they use to strengthen their systems, and finally how to obtain insurance in the event of an attack.

Keywords: Cyber security, data protection, data security, information security, risk management, risk assessment, confidentiality, integrity, availability, security systems, security management system, threats, penetration test, security, classification societies, regulations, procedures, cyber security, safety management standards.

1. Εισαγωγή

Η είσοδος στην ψηφιακή εποχή είναι γεγονός και η ανάγκη για ασφάλεια στον κυβερνοχώρο μεγαλώνει με την πάροδο του χρόνου. Καθημερινά περιστατικά παραβίασης προσωπικών δεδομένων και πληροφοριών οδηγούν στην ανεύρεση λύσεων και πρακτικών μεθόδων που σχετίζονται με αυτό το θέμα. Υπηρεσίες, οργανισμοί καθώς και ο καθένας προσωπικά, είναι πλέον πιο καχύποπτοι σε σχέση με τις επιθέσεις στο διαδίκτυο και την ασφάλεια των προσωπικών δεδομένων. Αυτή η παγκόσμια τάση που τείνει να γίνει συνήθεια στην καθημερινότητα των ανθρώπων θα εξεταστεί παρακάτω στο πεδίο την ναυτιλίας.

Η ναυτιλία αποτελεί παγκόσμια υπερδύναμη και δεν είναι καθόλου τυχαίο που το Cyber Security έχει μπει για τα καλά στο χώρο αυτόν. Εκτός από κοινούς κανονισμούς οι οποίοι εφαρμόζονται σε άλλους οργανισμούς, στη ναυτιλία εφαρμόζονται επιπλέον κανονισμοί οι οποίοι έχουν θεσπιστεί για τη διασφάλιση των πληροφοριών κατά την επικοινωνία των πλοίων με το γραφείο. Ένας λόγος που εφαρμόζονται πλέον υποχρεωτικά κανονισμοί και διαδικασίες σχετικά με την κυβερνοασφάλεια στη ναυτιλία είναι το σκάνδαλο με τη Maersk μια εταιρεία η οποία είναι η μεγαλύτερη εταιρεία μεταφοράς εμπορευματοκιβωτίων παγκοσμίως. Η Maersk είχε δηλώσει ότι περίμενε απώλειες μεταξύ 200- 300 εκατομμύρια δολάρια και αυτό οφειλόταν σε μια σημαντική διακοπή λειτουργίας του συστήματος η οποία ήταν απλά αποτέλεσμα ενός ιού που κατάφερε να εισχωρήσει στο σύστημα με αποτέλεσμα η εταιρεία να κλείσει προσωρινά όλα τα κρίσιμα συστήματα τα οποία είχαν μολυνθεί. Είναι

προφανές ότι σε αυτόν τον κλάδο είναι πιο δύσκολο να επιτευχθεί ασφάλεια σε σχέση με άλλους κλάδους από τους οποίους λείπει η δορυφορική επικοινωνία μέσω διαδικτύου.

Στο πλαίσιο λοιπόν του ISM και του IMO, έχουν θεσπιστεί κανονισμοί και διαδικασίες οι οποίοι βοηθούν τις εταιρείες να ενδυναμώσουν τα συστήματά τους και να παρέχουν την κατάλληλη εκπαίδευση προσωπικού σε σχέση με το Cyber Security στη ναυτιλία. Ένας ακόμη κανονισμός είναι το GDPR που αφορά την προστασία προσωπικών δεδομένων και έχει τεθεί υποχρεωτικά με οδηγία της ΕΕ. Επιπρόσθετα, ο IACS έχει επίσης θεσπίσει 12 συστάσεις σχετικά με την ασφάλεια στον κυβερνοχώρο. Τα tankers εφαρμόζουν το TMSA 3 και το VIQ 7 υποχρεωτικά. Τέλος, οι εταιρείες με δική τους πρωτοβουλία μπορούν να συμμορφωθούν με το ISO 27001 το οποίο παρέχει τις ελάχιστες απαιτήσεις για την ασφάλεια ενός οργανισμού στον κυβερνοχώρο. Από τους παραπάνω κανονισμούς και διαδικασίες άλλα είναι υποχρεωτικά και άλλα όχι έχοντας όμως έναν κοινό σκοπό και αυτό είναι η ασφάλεια στον κυβερνοχώρο.

Οι ναυτιλιακές εταιρείες εφαρμόζουν διαδικασίες οι οποίες αφορούν το Cyber Security. Η καθοδήγησή τους γίνεται είτε με δικό τους καταρτισμένο προσωπικό είτε με τη βοήθεια των νηογνωμόνων οι οποίοι παίζουν πλέον και ρόλο συμβουλευτικό ή ακόμη και από τρίτες συμβουλευτικές εταιρείες. Μια κατευθυντήρια γραμμή που ακολουθούν είναι αυτή της BIMCO με την οποία καλύπτουν ένα πολύ μεγάλο και σημαντικό κομμάτι όσον αφορά την ασφάλεια. Καλύπτονται επίσης και ασφαλιστικά αρκεί να ακολουθούν σωστά τις κατευθυντήριες γραμμές και να έχουν καλά εκπαιδευμένο το προσωπικό τους για την αποφυγή επιπόλαιων λαθών τα οποία μπορούν να συμβούν και να στοιχίζουν στην εταιρεία.

Στη παρούσα εργασία παρουσιάζεται μια ποσοτική έρευνα η οποία αφορά μερικές από τις μεγαλύτερες Ελληνικές ναυτιλιακές εταιρείες. Έχει αποσταλεί ερωτηματολόγιο και έχουν κληθεί να απαντήσουν σε αυτό, τα διευθυντικά στελέχη των ναυτιλιακών αυτών εταιρειών. Με τον τρόπο αυτό παρουσιάζονται αποτελέσματα σχετικά με το Cyber Security στη ναυτιλία. Εάν οι εταιρείες εφαρμόζουν τις απαιτούμενες διαδικασίες, εάν έχουν προετοιμαστεί σωστά σχετικά με τους κανονισμούς, πως διαχειρίζονται μια απειλή, πόσο προστατευμένοι αισθάνονται, κ.α.

1.1 Σκοπός

Η ραγδαία ανάπτυξη της τεχνολογίας έχει επηρεάσει την κοινωνία και κατ επέκταση τους οργανισμούς σε παγκόσμιο επίπεδο. Η παρούσα εργασία εξετάζει την επιρροή αυτή ως προς την ασφάλεια στον κυβερνοχώρο. Έτσι λοιπόν, έχουν θεσπιστεί κανονισμοί και νομοθεσίες

που αφορούν τον σχεδιασμό ενός σχεδίου αντιμετώπισης απειλών και κακόβουλων ενεργειών οι οποίοι βοηθούν στην αποφυγή του ανθρώπινου λάθους λαμβάνοντας τα απαραίτητα μέτρα προστασίας. Μερικά από αυτά τα μέτρα είναι υποχρεωτικά και άλλα όχι. Παρόλα αυτά είναι μέτρα τα οποία έχουν καθοδηγητικό σκοπό.

Ο σκοπός αυτής της ερευνητικής εργασίας, είναι η μελέτη της εφαρμογής cyber security στη ναυτιλία.

Με αφορμή το συγκεκριμένο νομοθετικό πλαίσιο, θα προσπαθήσουμε να απαντήσουμε στα εξής ερωτήματα:

1) Διερεύνηση των κανονισμών και των διαδικασιών που ακολουθούνται για την οργάνωση των ναυτιλιακών εταιρειών σε σχέση με το Cyber security.
2) Εξέταση παραγόντων ενδυνάμωσης του συστήματος Cyber security (IT & OT συστήματα) στη ναυτιλία.
3) Ασφαλιστική κάλυψη σε περίπτωση παραβίασης του κυβερνοχώρου (Cyber Breach).

Ο σκοπός της ερευνητικής εργασίας είναι η μελέτη της εφαρμογής διαδικασιών cyber security στο ναυτιλιακό χώρο.

1.1.1 Θεωρητικοί στόχοι- θεωρητικά ερωτήματα

- **Θεωρητικός Στόχος 1:** βιβλιογραφική επισκόπηση σχετικά με το cyber security στη ναυτιλία
  - **Θεωρητικό ερώτημα 1.1:** ποια είναι η έννοια του cyber security και ποιοι κανονισμοί εφαρμόζονται στη ναυτιλία.
  - **Θεωρητικό ερώτημα 1.2:** ποιοι οι κρίσιμοι παράγοντες που συνετέλεσαν στη δημιουργία του cyber security.
  - **Θεωρητικό ερώτημα 1.3:** ποιες τακτικές εφαρμόζονται για την ενσωμάτωση του cyber security στη ναυτιλία
  - **Θεωρητικό ερώτημα 1.4:** Ποιά είναι τα οφέλη της εφαρμογής του στη ναυτιλία.

- **Θεωρητικός Στόχος 2:** Εξέταση της υπάρχουσας νομοθεσίας ανά τον κόσμο στην ναυτιλία.
  - **Θεωρητικό ερώτημα 2.1:** Πώς εφαρμόζεται η νομοθεσία που αφορά το cyber security στη ναυτιλία παγκοσμίως

- **Θεωρητικό ερώτημα 2.2:** Ποιά guidelines ακολουθούν οι ναυτιλιακές εταιρείες.

1.1.2 Ερευνητικοί στόχοι- ερευνητικά ερωτήματα

Οι ερευνητικοί στόχοι είναι επεξηγηματικοί. Επιχειρείται η ερμηνεία του φαινομένου του cyber security στο ναυτιλιακό χώρο και ο προσδιορισμός των σχέσεων μεταξύ των παραγόντων που επιδρούν στην ασφάλεια πληροφοριών.

- **Ερευνητικός Στόχος 1:** Διαδικασίες που ακολουθούνται για την οργάνωση των ναυτιλιακών εταιρειών σε σχέση με το cyber security.
  - **Ερευνητικό ερώτημα 1.1:** Έχει η εταιρεία τεκμηριωμένη πολιτική προστασίας και διαδικασίες σχετικά με τη διαχείριση προσωπικών δεδομένων και ποίος είναι ο διαχειριστής του;
  - **Ερευνητικό ερώτημα 1.2:** Σημαντικότητα των Guidelines που ακολουθούν οι εταιρείες ώστε να επιτύχουν ασφάλεια στον κυβερνοχώρο.

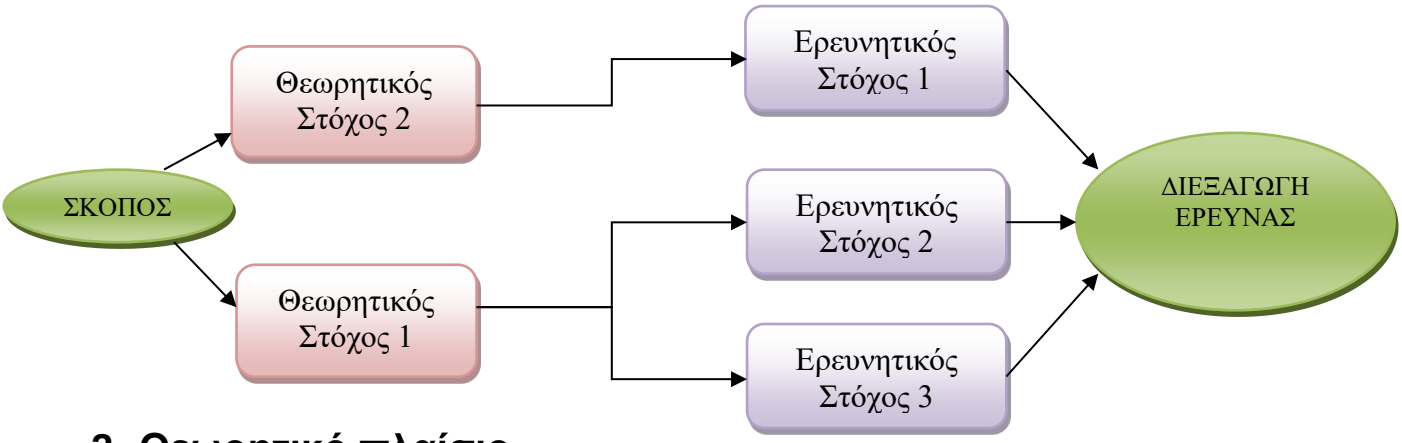
- **Ερευνητικός Στόχος 2:** Εξέταση παραγόντων ενδυνάμωσης του συστήματος cyber security στη ναυτιλία.
  - **Ερευνητικό ερώτημα 2.1:** Εφαρμόζει ενημερωμένες νέες τεχνολογίες και τοίχοι προστασίας Firewall για την αποφυγή απειλών;
  - **Ερευνητικό ερώτημα 2.2:** Πόσο επηρεάζει η εκπαίδευση προσωπικού την ενδυνάμωση του συστήματος Cyber Security της εταιρείας;

    Ερευνητικό ερώτημα 2.3: Εφαρμόζει η εταιρεία αξιολόγηση κινδύνων και διαχείριση κινδύνων;

- **Ερευνητικός Στόχος 3:** Διερεύνηση επιθέσεων.
  - **Ερευνητικό ερώτημα 3.1:** Υπάρχει εμπειρία σε κάποια απειλή για το σύστημα της εταιρείας τα τελευταία τρία χρόνια;
  - **Ερευνητικό ερώτημα 3.2:** Σε ποιο τμήμα παρουσιάζονται οι περισσότερες επιθέσεις και τι μορφής είναι (φυσικοί ή ανθρώπινοι).
  - **Ερευνητικό ερώτημα 3.3:** Μια απειλή επιφέρει αλλαγές στον τρόπο λειτουργίας μιας εταιρείας;

1.1.3 Σύνδεση θεωρητικών και ερευνητικών στόχων:

Οι ερευνητικοί στόχοι θα πρέπει να επιβεβαιώνουν τη θεωρία και για αυτό το λόγο θα πρέπει να υπάρχει σύνδεση μεταξύ ερευνητικών και θεωρητικών στόχων. Παρακάτω βλέπουμε ένα σχήμα που συνδέει τους θεωρητικούς με τους ερευνητικούς στόχους της παρούσας εργασίας.



2. Θεωρητικό πλαίσιο

2.1 Ορισμοί

Οι παρακάτω ορισμοί αφορούν το Cyber Security και το ISO 27001 (Bayuk J. - Healey J. – Rohmeyer P. – Sachs M. –Schmidt J. –Weiss J., 2012) ; (Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, 2015).

- Πληροφορία (Information): Η πληροφορία είναι ένας πόρος, ένα περιουσιακό στοιχείο, που όπως και όλα τα άλλα περιουσιακά στοιχεία έχει αξία για έναν οργανισμό και κατά συνέπεια χρειάζεται επαρκή προστασία.
- Ασφάλεια πληροφοριών (Information Security): Ως ασφάλεια πληροφοριών χαρακτηρίζεται η προστασία και διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητάς τους.
- Εμπιστευτικότητα (Confidentiality): Διασφάλιση ότι η πληροφορία μπορεί να προσπελασθεί μόνον από αυτούς που έχουν κατάλληλη εξουσιοδότηση.
- Ακεραιότητα (Integrity): Προστασία και διασφάλιση της ακρίβειας και της πληρότητας της πληροφορίας, όπως και των μεθόδων επεξεργασίας αυτής.
- Διαθεσιμότητα (Availability): Διασφάλιση ότι μόνον εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στην πληροφορία και τους παρεμφερείς πόρους όταν απαιτείται.

- Αποτίμηση κινδύνου (Risk Assessment): Η αποτίμηση των κινδύνων, των αδυναμιών και των επιδράσεών τους στην πληροφορία και τη διαχείρισή της, όπως και της πιθανότητας πραγματοποίησής τους.
- Διαχείριση κινδύνου (Risk Management): Η αναγνώριση, ο έλεγχος και η ελαχιστοποίηση των κινδύνων ασφάλειας που μπορούν να επηρεάσουν τα πληροφοριακά συστήματα, με αποδεκτό κόστος.

2.2 Cyber Security ορισμός

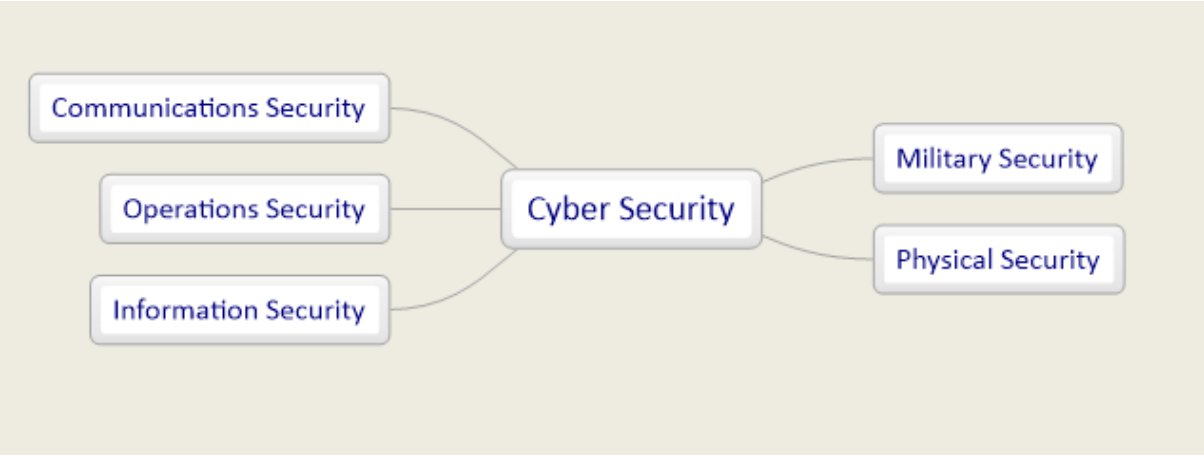
Η «ασφάλεια του κυβερνοχώρου» Cyber security, κατά το oxford dictionary, ορίζεται ως: "*Την κατάσταση της προστασίας από την εγκληματική ή μη εξουσιοδοτημένη χρήση ηλεκτρονικών δεδομένων ή τα μέτρα που λαμβάνονται για την επίτευξη αυτού του στόχου.*"

Ένας άλλος ορισμός από το Merriam – Webster, ορίζει την «ασφάλεια στον κυβερνοχώρο» Cyber security ως: "*Μέτρα που λαμβάνονται για την προστασία ενός υπολογιστή ή ενός συστήματος ηλεκτρονικών υπολογιστών (όπως στο Internet) έναντι μιας μη εξουσιοδοτημένης πρόσβασης ή επίθεσης.*"

Η παραπάνω ερμηνεία, καλύπτει μόνο τη μη εξουσιοδοτημένη πρόσβαση και τη κακή χρήση πληροφοριών. Παραμένει λοιπόν το ερώτημα σχετικά με το «τι γίνεται με λειτουργικά σφάλματα;». Δεν υπάρχει ακριβής ορισμός του όρου ούτος ώστε να δοθεί και να καλύψει το τόσο μεγάλο πεδίο. Ωστόσο, στην κοινότητα των προτύπων, ο ορισμός είναι σημαντικά ευρύτερος ώστε να περιλαμβάνει προστασία έναντι των διαφόρων κινδύνων για τους οργανισμούς και τα δεδομένα τους, ειδικά όταν η έννοια «Cyber security» θεωρείται συνώνυμο της «ασφάλειας των πληροφοριών» (Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, 2015).

Η εικόνα 1 απεικονίζει τους διάφορους τομείς που έχουν σχέση με τον όρο Cyber security(Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, ENISA

2015).



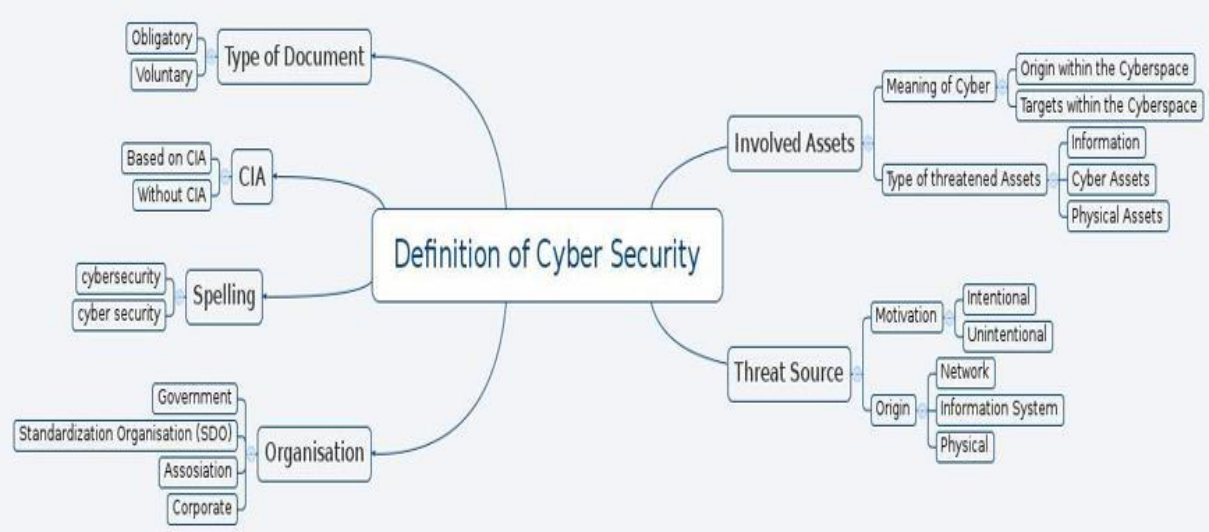
Εικόνα 1 οι διάφοροι τομείς στον όρο Cyber Security (ENISA PUBLICATION)

Οι τομείς που βλέπουμε στο σχήμα είναι (Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, ENISA 2015):

- Ασφάλεια Επικοινωνιών: Είναι η προστασία από απειλή για την τεχνική υποδομή ενός κυβερνοχώρου που μπορεί να οδηγήσει σε μεταβολή των χαρακτηριστικών του προκειμένου να εκτελέσει δραστηριότητες που δεν προορίζονταν από τους ιδιοκτήτες, τους σχεδιαστές ή τους χρήστες του.
- Ασφάλεια λειτουργιών: Είναι η προστασία από την προοριζόμενη διαφθορά διαδικασιών ή ροών εργασίας που θα έχουν αποτελέσματα που δεν ήταν σκόπιμα από τους ιδιοκτήτες, τους σχεδιαστές ή τους χρήστες.
- Ασφάλεια Πληροφοριών: Είναι η προστασία από την απειλή κλοπής, διαγραφής ή αλλοίωσης των αποθηκευμένων ή μεταδιδόμενων δεδομένων στο κυβερνοχώρο.
- Φυσική ασφάλεια: Πρόκειται για την προστασία από φυσικές απειλές που μπορούν να επηρεάσουν ή να προσβάλουν την ευημερία ενός κυβερνοχώρου. Για παράδειγμα θα μπορούσε να είναι η φυσική πρόσβαση σε διακομιστές, η εισαγωγή κακόβουλου υλικού σε ένα δίκτυο ή ο εξαναγκασμός των χρηστών ή των οικογενειών τους να κάνουν κάτι που δεν θέλουν.
- Δημόσια / Εθνική Ασφάλεια: Πρόκειται για την προστασία από απειλή της οποίας η προέλευση προέρχεται από τον κυβερνοχώρο, αλλά μπορεί να απειλήσει φυσικά ή κυβερνητικά περιουσιακά στοιχεία κατά τρόπο που θα έχει πολιτικό, στρατιωτικό ή στρατηγικό όφελος για τον επιτιθέμενο. Παραδείγματα θα μπορούσαν να είναι τα

«Stuxnet» ή οι ευρείες επιθέσεις DOS στις επιχειρήσεις κοινής ωφελείας, το χρηματοπιστωτικό σύστημα επικοινωνιών ή άλλες κρίσιμες δημόσιες ή βιομηχανικές υποδομές.

Στην εικόνα 2 παρακάτω, απεικονίζονται οι συνιστώσες από τις οποίες αποτελείται ο όρος Cyber Security (Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, ENISA 2015).



Εικόνα 2: Συνιστώσες που απαρτίζουν τον ορισμό του Cyber Security (ENISA PUBLICATION) .

Εξήγηση:

1. **Ο τύπος εγγράφου αποτελείται από δύο κατηγορίες**

✓ Υποχρεωτικά έγγραφα, όπου ο ορισμός τους βασίζεται σε νόμους, κανονισμούς ή υποχρεωτικά πρότυπα.

✓ Εθελοντικά έγγραφα, όπου ο ορισμός τους βασίζεται σε συμφωνημένες βέλτιστες πρακτικές ή αξιόπιστες συστάσεις.

2. **CIA – Confidentially – Integrity – Availability (Εμπιστευτικότητα - Ακεραιότητα – Διαθεσιμότητα)**

✓ Βάση των CIA: Ο ορισμός του Cybersecurity χρησιμοποιεί και καλύπτει τους όρους Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας,

✓ Χωρίς CIA: Ο ορισμός του Cybersecurity δεν αναφέρεται ούτε περιλαμβάνει τα θέματα Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας.

3. **Ορθογραφία**

- ✓ Η μορφή ορθογραφίας που χρησιμοποιείται. Με τον τρόπο που χρησιμοποιείται παρέχεται συνέπεια σε έναν ορισμό και στη χρήση του. Cyber security ή Cyber security είναι ουσιαστικά το ίδιο.

4. **Οργανισμοί**

- ✓ Η φύση των οργανισμών μπορεί να επηρεάσει τους παράγοντες ή τους τομείς που αναφέρονται στον ορισμό. Αυτό μπορεί να επηρεάσει την εφαρμογή του ορισμού και, κατά συνέπεια, τη χρησιμότητά του.

5. **Η έννοια του «Cyber»**

- ✓ Ο ορισμός αναφέρεται στην προέλευση μιας απειλής που εισάγεται μέσω του κυβερνοχώρου και όχι σε μια φυσική επίθεση. Ο ορισμός αφορά μόνο στόχους που μειώνουν την αξιοπιστία ενός συστήματος ή μιας διαδικασίας και όχι μια συσκευή που ελέγχεται μέσω ενός συστήματος που προέρχεται από τον Κυβερνοχώρο.

6. **Είδη απειλούμενων περιουσιακών στοιχείων**

- ✓ Σχετικά με τα παραπάνω, η κατηγορία του απειλούμενου συστήματος που καλύπτεται στον ορισμό του Cyber security.

7. **Κίνητρο της πηγής απειλών**

- ✓ Ο ορισμός μπορεί να αντιμετωπίσει την παρακίνηση της απειλής, είτε από πρόθεση, για παράδειγμα ποινική, είτε ακούσια, ως αποτέλεσμα υποπροϊόντος άλλης ενέργειας.

8. **Προέλευση της πηγής απειλών.**

- ✓ Ο ορισμός μπορεί να διαφοροποιήσει την προέλευση της απειλής. Επίσης, μπορεί μόνο να εξετάσει την προστασία από απειλές που προέρχονται από τον Κυβερνοχώρο, γνωστό και ως Διαδίκτυο και είναι αποκλειστικά δικτυακό. Εναλλακτικά, ο ορισμός μπορεί να καλύψει την προστασία των Πληροφοριακών Συστημάτων από τοπικές απειλές όπως «εμπιστευτικές απειλές». Και πάλι, ο ορισμός μπορεί επίσης να αντιμετωπίσει την προστασία από φυσικές επιθέσεις στη μονάδα που φιλοξενεί Πληροφοριακά Συστήματα.

2.3 Ορολογία που χρησιμοποιείται από τους οργανισμούς.

Οι διεθνείς οργανισμοί χρησιμοποιούν και αυτοί κάποια συγκεκριμένη ορολογία σχετικά με το Cyber Security όπως παρατίθενται παρακάτω (Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, ΕΝΙΣΑ 2015).

- **ETSI**

Το ETSI είναι ένας Ευρωπαϊκός Οργανισμός Τυποποίησης (ESO). Είναι ο αναγνωρισμένος οργανισμός περιφερειακών προτύπων που ασχολείται με τηλεπικοινωνιακά, ραδιοτηλεοπτικά και άλλα δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών.

- **ISO/IEC JTC1**

Το JTC 1 είναι το περιβάλλον ανάπτυξης προτύπων όπου οι εμπειρογνώμονες αναπτύσσουν τα παγκόσμια πρότυπα πληροφορικής και επικοινωνιών (ICT) για επαγγελματικές και καταναλωτικές εφαρμογές. Επιπλέον, το JTC 1 παρέχει το περιβάλλον έγκρισης προτύπων για την ενσωμάτωση ποικίλων και πολύπλοκων τεχνολογιών ICT. Τα πρότυπα αυτά βασίζονται στις βασικές τεχνολογίες υποδομής που αναπτύσσονται από τα κέντρα εμπειρογνωμοσύνης της JTC 1 και συμπληρώνονται από προδιαγραφές που αναπτύσσονται σε άλλους οργανισμούς (https://www.iso.org/isoiec-jtc-1.html).

Ορισμός: *Διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας πληροφοριών στον Κυβερνοχώρο* (Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, 2015).

- **ITU**

Είναι η Διεθνής Ένωση Τηλεπικοινωνιών και ο αρμόδιος οργανισμός για τις τηλεπικοινωνίες και την διακίνηση της πληροφορίας.

Ορισμός: *Cybersecurity είναι η συλλογή εργαλείων, πολιτικών, εννοιών ασφάλειας, διασφάλισης ασφάλειας, κατευθυντήριων γραμμών, προσεγγίσεων διαχείρισης κινδύνου, δράσεων, κατάρτισης, βέλτιστων πρακτικών, διασφάλισης και τεχνολογιών που μπορούν να χρησιμοποιηθούν για την προστασία του περιβάλλοντος και της οργάνωσης και των περιουσιακών στοιχείων του χρήστη* (Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, 2015).

- **NIST**

Είναι το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) το οποίο ιδρύθηκε το 1901 και τώρα είναι μέλος του Αμερικανικού Υπουργείου Εμπορίου.

Ορισμός: *Cybersecurity είναι η ικανότητα προστασίας ή υπεράσπισης της χρήσης του κυβερνοχώρου από επιθέσεις* (Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, 2015).

- **NATO**

Είναι το συνεταιρικό κέντρο υπεράσπισης στον κυβερνοχώρο του NATO. Στη συγκεκριμένη περίπτωση δεν υπάρχει συγκεκριμένος ορισμός για την ασφάλεια στον κυβερνοχώρο.

- **CNSS**

Ορισμός: Cybersecurity είναι η πρόληψη βλάβης, προστασίας και αποκατάστασης ηλεκτρονικών υπολογιστών, συστημάτων ηλεκτρονικών επικοινωνιών, υπηρεσιών ηλεκτρονικών επικοινωνιών, καλωδιακής επικοινωνίας και ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των πληροφοριών που περιέχονται σε αυτά, για τη διασφάλιση της διαθεσιμότητάς τους, της ακεραιότητας, της γνησιότητας, της εμπιστευτικότητας και της μη επανάκτησης. Πηγή: Ασφάλεια στον κυβερνοχώρο NSPD-54 / HSPD-23 Η ικανότητα προστασίας ή υπεράσπισης της χρήσης του κυβερνοχώρου από επιθέσεις στον κυβερνοχώρο. Σημείωση 1: Ο ορισμός αυτός περιλαμβανόταν στην έκδοση του λεξιλογίου CNSS του 2010. Σημείωση 2: Ο ορισμός αυτός εξακολουθεί να χρησιμοποιείται στο NIST SP800-39 (βλέπε κεφάλαιο Σφάλμα! Η πηγή αναφοράς δεν βρέθηκε).

Ο όρος του Cyber Security με λίγα λόγια, ισχύει σε ποικίλα πλαίσια, από τις επιχειρήσεις ως την κινητή υπολογιστική, και μπορεί να χωριστεί σε μερικές κοινές κατηγορίες. Οι κατηγορίες είναι οι εξής (Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, ENISA 2015):

- **Η ασφάλεια δικτύων** είναι η πρακτική της διασφάλισης ενός δικτύου υπολογιστών από εισβολείς, είτε με στοχευόμενη επίθεση είτε με ευκαιριακά κακόβουλα προγράμματα (https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security) ; (Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler,

Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak, ENISA 2015).

- **Η ασφάλεια εφαρμογών** επικεντρώνεται στη διατήρηση του λογισμικού και των συσκευών χωρίς απειλές. Μια εκτιθέμενη εφαρμογή, θα μπορούσε να παρέχει πρόσβαση σε δεδομένα τα οποία έχει σχεδιαστεί να προστατεύει. Η επιτυχής ασφάλεια αρχίζει στο στάδιο του σχεδιασμού, πολύ πριν από την ανάπτυξη ενός προγράμματος ή μιας συσκευής.
- **Η ασφάλεια πληροφοριών** προστατεύει την ακεραιότητα και την ιδιωτικότητα των δεδομένων, τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά.
- **Η ασφάλεια λειτουργίας** περιλαμβάνει τις διαδικασίες και τις αποφάσεις για το χειρισμό και την προστασία δεδομένων. Οι άδειες που έχουν οι χρήστες κατά την πρόσβαση σε ένα δίκτυο και οι διαδικασίες που καθορίζουν τον τρόπο και τον τόπο αποθήκευσης ή κοινής χρήσης των δεδομένων εμπίπτουν σε αυτή την ομπρέλα.
- **Η αποκατάσταση μετά από καταστροφή και η συνέχεια της επιχείρησης** καθορίζουν τον τρόπο με τον οποίο ένας οργανισμός ανταποκρίνεται σε ένα περιστατικό ασφάλειας στον κυβερνοχώρο ή σε οποιοδήποτε άλλο γεγονός που προκαλεί την απώλεια λειτουργιών ή δεδομένων. Οι πολιτικές αποκατάστασης από καταστροφές υπαγορεύουν τον τρόπο με τον οποίο ο οργανισμός αποκαθιστά τις λειτουργίες και τις πληροφορίες του ώστε να επιστρέψει στην ίδια λειτουργική ικανότητα όπως πριν από την εκδήλωση οποιασδήποτε επίθεσης. Η συνέχεια της επιχείρησης είναι το σχέδιο που ο οργανισμός επιστρέφει ενώ προσπαθεί να λειτουργήσει χωρίς συγκεκριμένους πόρους
- **Η εκπαίδευση τελικού χρήστη** απευθύνεται στον πιο απρόβλεπτο παράγοντα ασφάλειας του κυβερνοχώρου, τους ανθρώπους. Ο καθένας μπορεί να εισάγει κατά λάθος έναν ιό σε ένα «ασφαλές» σύστημα, παραλείποντας απλώς να ακολουθήσει τις καλές πρακτικές ασφαλείας. Η εκπαίδευση των χρηστών ώστε να διαγράφουν ύποπτα επισυναπτόμενα ηλεκτρονικού ταχυδρομείου, να μην συνδέονται με μη αναγνωρισμένες μονάδες USB και διάφορα άλλα σημαντικά μαθήματα είναι θέμα ζωτικής σημασίας για την ασφάλεια οποιουδήποτε οργανισμού.

2.4 GDPR- General Data Protection Regulation

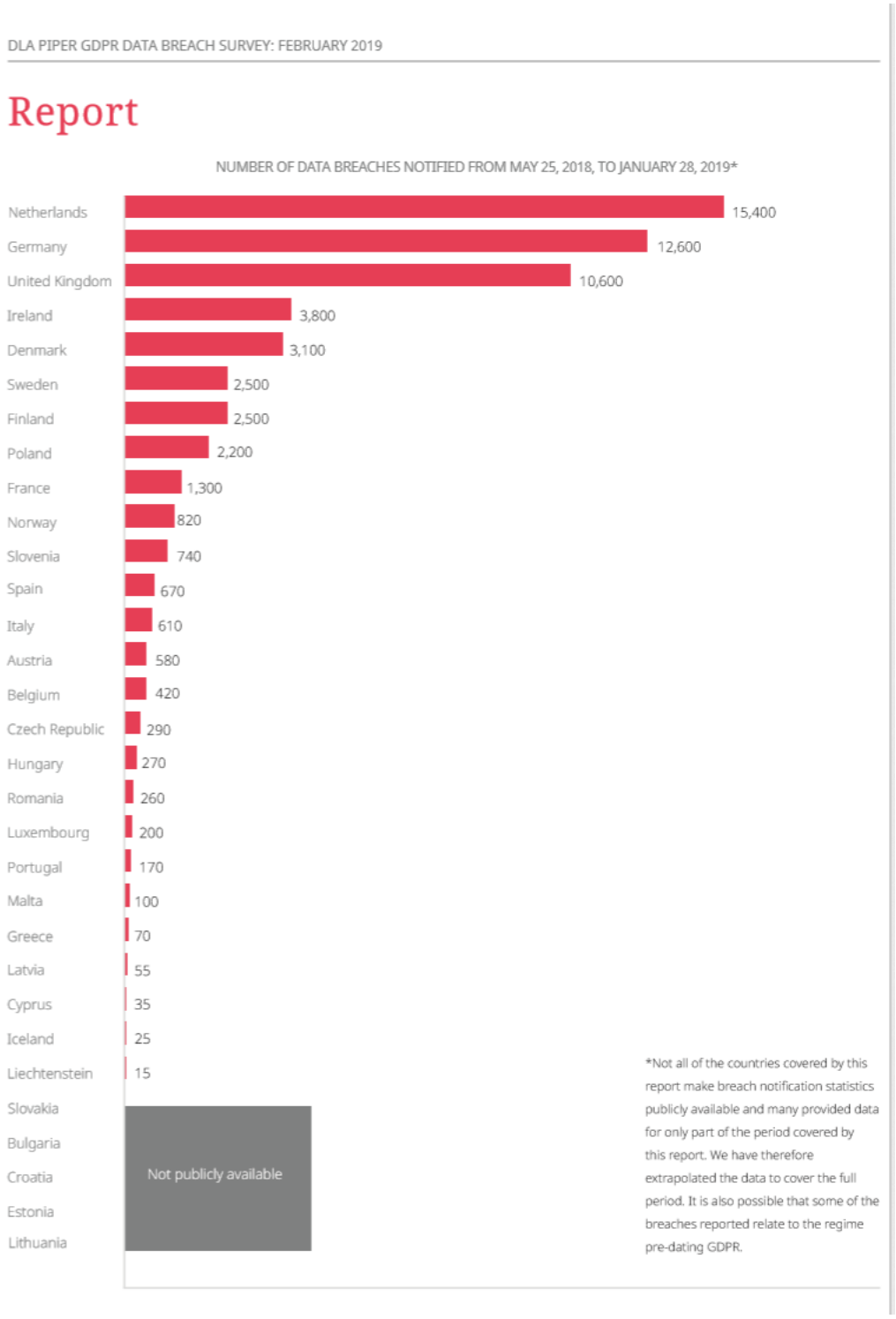
Τον Δεκέμβριο του 2015, η Ευρωπαϊκή Ένωση (ΕΕ) ψήφισε και εφαρμόστηκε ο γενικός κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) (https://gdpr-info.eu/). Αυτό καθορίζει:

- Την προστασία της ιδιωτικής ζωής και της ασφάλειας των δεδομένων.
- Ισχύει για όλα τα κράτη μέλη της ΕΕ από τις 25 Μαΐου 2018.
- Η εποχή των "Big Data" έχει ως στόχο την εναρμόνιση των νόμων προστασίας ποικίλων δεδομένων σε ολόκληρη την ΕΕ.

Τα Προσωπικά δεδομένα είναι κάθε πληροφορία που αφορά ένα άτομο, που σχετίζεται είτε αφορά την ιδιωτική του, επαγγελματική ή δημόσια ζωή του. Αποτελούνται από προσδιορισμένες ή αναγνωρίσιμες πληροφορίες και μπορεί να είναι οτιδήποτε από ένα όνομα, μια διεύθυνση κατοικίας, μια φωτογραφία, μια διεύθυνση ηλεκτρονικού ταχυδρομείου, τραπεζικές λεπτομέρειες, δημοσιεύσεις σε ιστότοπους κοινωνικής δικτύωσης, ιατρικές πληροφορίες ή η διεύθυνση IP ενός υπολογιστή.
Το GDPR αποτελείται από 11 κεφάλαια και 99 άρθρα (https://gdpr-info.eu/) τα οποία παρατίθεται απαριθμητικά:
Κεφάλαιο I - Γενικές διατάξεις (άρθρα 1 έως 4)
Κεφάλαιο II - Αρχές (άρθρα 5 έως 11)
Κεφάλαιο III – Δικαιώματα του υποκειμένου των δεδομένων- 5 Τμήματα (άρθρα 12 έως 23)
Κεφάλαιο IV - Ελεγκτής & Επεξεργαστής - 5 Τμήματα (Άρθρα 24 έως 43)
Κεφάλαιο V - Μεταφορές δεδομένων προσωπικού χαρακτήρα (άρθρα 44 έως 50)
Κεφάλαιο VI - Ανεξάρτητες εποπτικές αρχές (άρθρα 51 έως 59)
Κεφάλαιο VII - Συνεργασία και συνέπεια (άρθρα 60 έως 76)
Κεφάλαιο VIII - Διορθωτικά μέτρα, ευθύνη και κυρώσεις (άρθρα 77 έως 84)
Κεφάλαιο IX - Διατάξεις για την κατάσταση της επεξεργασίας (άρθρα 85 έως 91)
Κεφάλαιο X - Πράξεις για τις αντιπροσωπείες και την εφαρμογή (άρθρα 92 και 93)
Κεφάλαιο XI - Τελικές διατάξεις (άρθρα 94 έως 99)

173 αιτιολογικές σκέψεις: Επίσημη δήλωση που παρέχει την εξήγηση ή τους λόγους για μια τέτοια πρωτοβουλία.

Η DLA Piper είναι μια εταιρεία που παρέχει νομικές υπηρεσίες σε 40 χώρες του κόσμου ανάμεσα σε Αμερική, Ευρώπη, Μέση Ανατολή, Αφρική και Ασία. Διεξήγαγε μια έρευνα η οποία αφορά την παραβίαση προσωπικών δεδομένων έπειτα από την εφαρμογή του GDPR στην Ευρώπη. Η έκθεση αυτή που αφορά το χρονικό διάστημα από 25 Μαΐου 2018 έως 28 Ιανουαρίου 2019 (παγκόσμια ημέρα προστασίας δεδομένων) και καταγράφει τις παραβιάσεις προσωπικών δεδομένων που υπέστησαν μεγάλες εταιρείες σε όλη την Ευρώπη. Στην έρευνα συμμετείχαν 21 από τα 28 κράτη μέλη της ΕΕ και καταγράφηκαν 59430 παραβιάσεις σε όλη την Ευρώπη (DLA Piper, 2019 survey). Παρακάτω φαίνεται ο αριθμός των παραβιάσεων δεδομένων ανά χώρα στο χρονικό διάστημα αυτό (DLA Piper, 2019 survey).



Εικόνα 3 Αριθμός παραβιάσεων στην Ευρώπη από 25 Μαΐου 2018 ως 28 Ιανουαρίου 2019 (DLA Piper Publication)

2.5 Cyber security στη ναυτιλία

Το θέμα της κυβερνοασφάλειας (cyber security) στη ναυτιλία έχει απασχολήσει-προβληματίσει τις ναυτιλιακές εταιρείες τον τελευταίο καιρό. Η συνεχής ανάπτυξη της τεχνολογίας έχει συντελέσει και αποτελεί τον πιο σημαντικό παράγοντα για θέματα ασφάλειας στη ναυτιλία. Είναι ιδιαίτερη περίπτωση, και αυτό συμβαίνει επειδή δεν αρκεί μόνο να υπάρχει κυβερνοασφάλεια στο γραφείο, αλλά και στα πλοία της κάθε εταιρείας διότι σε κάθε περίπτωση αυτά επικοινωνούν μεταξύ τους.

Στην περίπτωση του Cyber security στην ναυτιλία και δεδομένου ότι η βιομηχανία γίνεται ολοένα και πιο μηχανογραφημένη, οι Pen Ten Partners οι οποίοι ασχολούνται με δοκιμές διείσδυσης στον κυβερνοχώρο, για το 2018 αναφέρουν Hacking, παρακολούθηση, κλοπή και βύθιση των πλοίων (https://www.pentestpartners.com/penetration-testing-services/maritime-cyber-security-testing/)

Αυτό οφείλεται κυρίως σε:

- Έλλειψη διαχωρισμού δικτύων στα περισσότερα πλοία.
- Το σύστημα ECDIS είναι ιδιαίτερα ευάλωτο στις επιθέσεις χάκερ.
- Οι ιδιοκτήτες σκαφών και οι φορείς εκμετάλλευσης πρέπει να αντιμετωπίσουν γρήγορα τα ζητήματα αυτά.

Τα γεγονότα μπορεί να είναι αποτέλεσμα από εσκεμμένες κακόβουλες ενέργειες, ακούσια επίθεση χάκερ ή από σφάλμα ενός χρήστη του συστήματος. Θα πρέπει λοιπόν να υπάρχουν δύο επίπεδα ασφάλειας, ένα σε επιχειρησιακό επίπεδο – γραφείο πλοίο και ένα σε σχέση με τους εξωτερικούς κινδύνους όσον αφορά τη δορυφορική πλοήγηση και τις λιμενικές εγκαταστάσεις (Kimberly tam – Kevin Jones, 2019), (https://www.pentestpartners.com/penetration-testing-services/maritime-cyber-security-testing/).

Στην ευρωπαϊκή ένωση έχει εφαρμοστεί η ασφάλεια δικτύων και συστημάτων πληροφοριών τον Μάιο του 2016 (οδηγία EU 2016/1148). Η νομοθεσία όμως αυτή τότε είχε εφαρμοστεί στα λιμάνια και όχι στα πλοία (οδηγία EU 2016/1148). Ο κανονισμός γενικής προστασίας δεδομένων (GDPR) είναι σε εφαρμογή και στα πλοία από τον Μάιο του 2018 (οδηγία EU 2016/679).

Θα μπορούσε λοιπόν να τεθεί η ερώτηση, τι επηρεάζει η ασφάλεια στον κυβερνοχώρο;

Κατ αρχάς θα γίνει διαχωρισμός των συστημάτων σε συστήματα OT τα οποία ελέγχουν το φυσικό κόσμο και τα συστήματα πληροφορικής IT τα οποία διαχειρίζονται δεδομένα. Τα συστήματα OT διαφέρουν από τα παραδοσιακά Συστήματα πληροφορικής IT. Το σύστημα

ΟΤ είναι υλικό και λογισμικό που άμεσα παρακολουθεί/ελέγχει φυσικές συσκευές και διαδικασίες. Το σύστημα πληροφορικής IT, καλύπτει το φάσμα των τεχνολογιών για την επεξεργασία πληροφοριών, συμπεριλαμβανομένου του λογισμικού, τεχνολογίες υλικού και επικοινωνιών. Παραδοσιακά, Το ΟΤ και το IT έχουν χωριστεί, αλλά με το διαδίκτυο, το ΟΤ και το IT έρχονται πιο κοντά, καθώς τα ιστορικά ανεξάρτητα συστήματα ενσωματώνονται. Η διακοπή της λειτουργίας των συστημάτων ΟΤ μπορεί να επιφέρει σημαντικό κίνδυνο για την ασφάλεια του σκάφους το προσωπικό, το φορτίο, τη βλάβη στο θαλάσσιο περιβάλλον και να παρεμποδίσουν τη λειτουργία του πλοίου. Τυπικές διαφορές μεταξύ συστημάτων πληροφορικής και τεχνολογίας πληροφοριών μπορούν να παρατηρηθούν στον παρακάτω πίνακα 1 (BIMCO - ICS CS ON BOARD SHIPS, 2018), (Kimberly Tam, Kevin Jones, June 2019).

Πίνακας 1 διαφορές IT & OT

ΚΑΤΗΓΟΡΙΑ	ΣΥΣΤΗΜΑ IT	ΣΥΣΤΗΜΑ ΟΤ
Απαιτήσεις απόδοσης	• Σε μη πραγματικό χρόνο • Η απάντηση πρέπει να είναι συνεπής • Λιγότερο κρίσιμη αλληλεπίδραση έκτακτης ανάγκης • Ο έλεγχος πρόσβασης μπορεί να είναι περιορισμένος εφαρμοστεί στο βαθμό που αιτείται για ασφάλεια	• Σε πραγματικό χρόνο • Η απάντηση είναι κρίσιμη για το χρόνο • Η ανταπόκριση στην ανθρώπινη και οποιαδήποτε άλλη επείγουσα αλληλεπίδραση είναι κρίσιμη • Η πρόσβαση στα ΟΤ συστήματα πρέπει να ελέγχεται αυστηρά, αλλά δεν πρέπει να παρεμποδίζει ή να παρεμβαίνει στην αλληλεπίδραση ανθρώπου-μηχανής.
Απαιτήσεις διαθεσιμότητας (αξιοπιστίας)	• Απαντήσεις όπως η επανεκκίνηση είναι	• Απαντήσεις όπως η επανεκκίνηση

	αποδεκτές. • Οι ανεπάρκειες διαθεσιμότητας μπορεί να είναι ανεκτές, ανάλογα με τις λειτουργικές απαιτήσεις του συστήματος.	ενδέχεται να μην είναι αποδεκτές λόγω λειτουργικών απαιτήσεων • Οι απαιτήσεις διαθεσιμότητας ενδέχεται να απαιτήσουν συστήματα back-up.
Απαιτήσεις διαχείρισης κινδύνου	• Διαχειρίζεται δομένα • Εμπιστευτικότητα και ακεραιότητα δεδομένων είναι πρωταρχικής σημασίας • Ανοχή σφάλματος μπορεί να είναι λιγότερο σημαντική. • Οι επιπτώσεις κινδύνου μπορεί να προκαλέσουν καθυστέρηση: της εκκαθάρισης του πλοίου, της έναρξης φόρτωσης/ ξεφόρτωσης και των εμπορικών και επιχειρηματικών δραστηριοτήτων.	• Ελέγχει τον φυσικό κόσμο • Η ασφάλεια είναι πρωταρχική, ακολουθούμενη από προστασία της διαδικασίας • Η ανοχή σφάλματος είναι απαραίτητη, ομοιόμορφη μπορεί να μην είναι αποδεκτή η στιγμιαία διακοπή λειτουργίας • Οι επιπτώσεις των κινδύνων είναι η μη συμμόρφωση των κανονισμών, καθώς και η βλάβη του προσωπικού επί του πλοίου, του περιβάλλοντος, του εξοπλισμού ή/και του φορτίου

Λειτουργία συστήματος	• Τα συστήματα είναι σχεδιασμένα για χρήση με γνωστά λειτουργικά συστήματα • Οι αναβαθμίσεις είναι απλές με τη διαθεσιμότητα αυτοματοποιημένων εργαλείων ανάπτυξης	• διαφορετικά και ενδεχομένως ιδιόκτητα λειτουργικά συστήματα, συχνά χωρίς ενσωματωμένες δυνατότητες ασφαλείας • Οι αλλαγές λογισμικού πρέπει να γίνονται με προσοχή, συνήθως από προμηθευτές λογισμικού, εξαιτίας των εξειδικευμένων αλγορίθμων ελέγχου και της πιθανής εμπλοκής του τροποποιημένου υλικού και λογισμικού
Περιορισμοί πόρων	• τα συστήματα καθορίζονται με αρκετούς πόρους για να υποστηρίξουν την προσθήκη εφαρμογών τρίτων όπως οι λύσεις ασφάλειας	• τα συστήματα έχουν σχεδιαστεί για να υποστηρίζουν την επιδιωκόμενη επιχειρησιακή διαδικασία και μπορεί να μην διαθέτουν αρκετούς πόρους μνήμης και υπολογιστών για να υποστηρίξουν την προσθήκη

	δυνατοτήτων ασφαλείας

Από τον παραπάνω πίνακα προκύπτει ότι υπάρχουν σημαντικές διαφορές μεταξύ του ποιος χειρίζεται την αγορά και τη διαχείριση των συστημάτων ΟΤ έναντι συστημάτων πληροφορικής σε ένα πλοίο. Τα τμήματα πληροφορικής δεν συμμετέχουν συνήθως στην αγορά συστημάτων ΟΤ. Η αγορά τέτοιων συστημάτων θα πρέπει να περιλαμβάνει έναν επικεφαλή μηχανικό, ο οποίος γνωρίζει τον αντίκτυπο στα συστήματα επί των πλοίων και έχει γνώσεις IT, αλλά πιθανότατα οι γνώσεις να είναι περιορισμένες σχετικά με το λογισμικό και τη διαχείριση του Cyber Risk. Επομένως, είναι σημαντικό να υπάρξει διάλογος με την υπηρεσία πληροφορικής για να διασφαλιστεί ότι οι κίνδυνοι στον κυβερνοχώρο θα ληφθούν υπόψη κατά τη διαδικασία αγοράς των συστημάτων ΟΤ. Οι διαχειριστές των συστημάτων ΟΤ, θα πρέπει να συνεννοούνται με το τμήμα πληροφορικής, έτσι ώστε να υπάρχει μια γενική εικόνα του πιθανού κινδύνου και να βοηθηθεί η θέσπιση της απαραίτητης πολιτικής και των διαδικασιών για τη συντήρηση του λογισμικού (BIMCO - ICS CS ON BOARD SHIPS, 2018), (Kimberly Tam, Kevin Jones, June 2019).

<u>Στα συστήματα πληροφορικής-IT επηρεάζονται</u>: Δίκτυα πληροφορικής, emails, Διοίκηση, λογαριασμοί, λίστες πληρωμάτων, Προγραμματισμένη συντήρηση, η διαχείριση και η ανακύκλωση ανταλλακτικών, τα ηλεκτρονικά εγχειρίδια, τα ηλεκτρονικά πιστοποιητικά, οι άδειες εργασίας, τα ναυλοσύμφωνα, η ειδοποίηση ετοιμότητας, οι φορτωτικές. Στα συστήματα IT είναι σε κίνδυνο κυρίως τα οικονομικά μιας εταιρείας και η φήμη (Hugh Boyes, 2014), (BIMCO, 2018), (Kimberly Tam, Kevin Jones, June 2019).

<u>Στα συστήματα ΟΤ που αφορούν τη λειτουργία του υλικού και του λογισμικού επηρεάζονται:</u> PLCs, SCADA, Μέτρηση και έλεγχος επί του σκάφους, ECDIS, GPS, Απομακρυσμένη υποστήριξη για κινητήρες, Καταγραφείς δεδομένων, Έλεγχος μηχανής και φορτίου, Δυναμική τοποθέτηση. Στα συστήματα ΟΤ είναι κυρίως σε κίνδυνο η ζωή, η ιδιοκτησία και το περιβάλλον (B.Svilicic – David BrCiC, March 2019), (Kimberly Tam, Kevin Jones, June 2019).

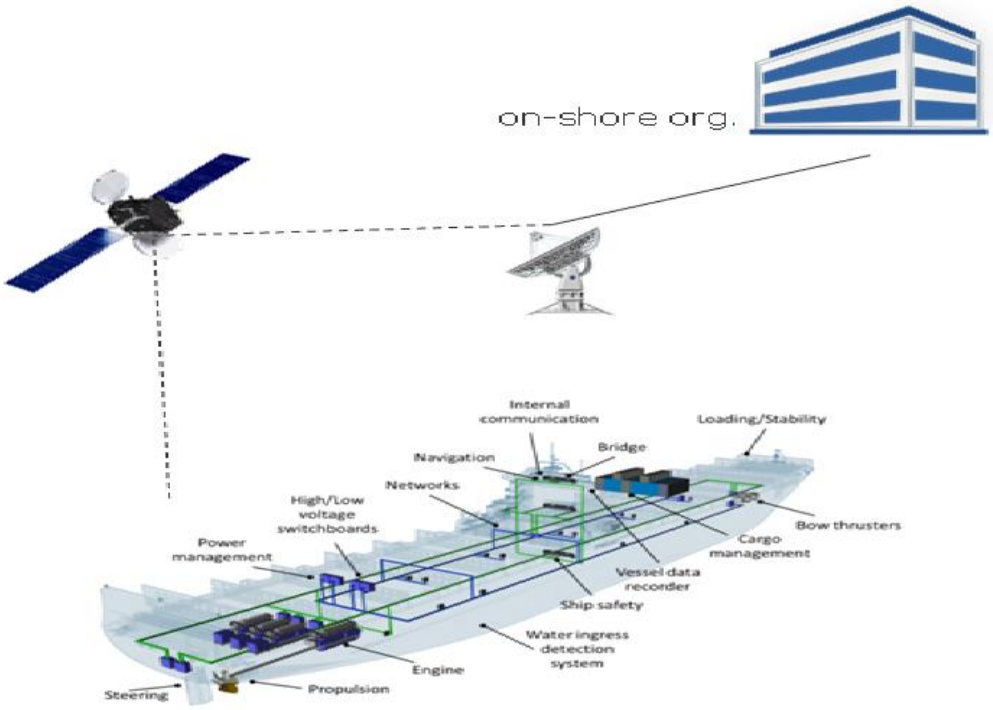
Οι κατευθυντήριες γραμμές σχετικά με την ασφάλεια στον κυβερνοχώρο στον τομέα της ναυτιλίας βασίζονται κυρίως σε:

- IMO
- BIMCO
- ISO/IEC 27001 & ISO / IEC 62443 (OT)
- Classification Bodies and IACS
  DNV GL, ABS κ.ο.κ.
- P&I clubs

2.6 BIMCO

Συγκεκριμένα οι κατευθυντήριες γραμμές του BIMCO (BIMCO - ICS CS ON BOARD SHIPS, 2018) για τον έλεγχο της κυβερνοασφάλειας είναι:

- ✓ Ο πιο σημαντικός παράγοντας στις Οδηγίες BIMCO είναι η ευαισθητοποίηση ως προς το Cyber Security από όλους.
- ✓ Προσδιορισμός των απειλών.
- ✓ Εντοπισμός ευπαθειών.
- ✓ Αξιολόγηση της έκθεσης σε κινδύνους.
- ✓ Ανάπτυξη μέτρων προστασίας και ανίχνευσης.
- ✓ Καθιέρωση σχεδίων έκτακτης ανάγκης.
- ✓ Απάντηση στα περιστατικά ασφάλειας στον κυβερνοχώρο.



Εικόνα 4 απεικόνιση επικοινωνίας γραφείου-πλοίου (DNVGL PUBLICATION)

Πέρα από το πρότυπο ISO 27000 υπάρχουν κανονισμοί οι οποίοι αφορούν συγκεκριμένα ήδη πλοίων. Έτσι, προς το παρόν έχει τεθεί σε εφαρμογή ο κανονισμός TMSA3 ο οποίος αφορά τα τάνκερς. Αυτός ο κανονισμός καλύπτει σε ασφαλιστικό επίπεδο τους ιδιοκτήτες οι οποίοι εφαρμόζοντας τους κανονισμούς μπορούν να έχουν πλήρη ασφαλιστική κάλυψη και από την άλλη τους ασφαλιστές οι οποίοι μπορούν να διαχειρίζονται τον κίνδυνο. Αξίζει να σημειωθεί πως το 2021 έρχεται υποχρεωτικός κανονισμός και για τα Bulk Carriers.

2.7 ISM CODE

Ο κώδικας ISM (International Safety Management Code), ο διεθνής δηλαδή κώδικας για την Διαχείριση της Ασφάλειας (ISM) είναι να παράσχει ένα διεθνές πρότυπο για την ασφαλή διαχείριση και λειτουργία των πλοίων και για την πρόληψη της ρύπανσης (http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

Η προέλευση του Κώδικα επανέρχεται στα τέλη της δεκαετίας του 1980, όταν υπήρχε αυξανόμενη ανησυχία για τα κακά πρότυπα διαχείρισης στη ναυτιλία. Οι έρευνες για τα ατυχήματα αποκάλυψαν σημαντικά σφάλματα εκ μέρους της διοίκησης και τελικά το 1987 η Συνέλευση του IMO ενέκρινε το ψήφισμα A.596 (15), το οποίο κάλεσε την Επιτροπή

Ναυτικής Ασφάλειας να αναπτύξει τις κατευθυντήριες γραμμές σχετικά με τη διαχείριση της ξηράς (http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

Ο Κώδικας καθορίζει τους στόχους διαχείρισης της ασφάλειας μιας εταιρείας και απαιτεί να δημιουργηθεί από την ίδια την εταιρεία η διαχείριση της ασφάλειας (SMS), η οποία ορίζεται ως ο ιδιοκτήτης ή οποιοσδήποτε άλλος οργανισμός ή πρόσωπο, όπως ο διαχειριστής ή ο ναυλωτής του σκάφους που έχει αναλάβει την ευθύνη για την εκμετάλλευση του πλοίου και ο οποίος, αναλαμβάνοντας την ευθύνη αυτή, συμφώνησε να αναλάβει όλα τα καθήκοντα και την ευθύνη που επιβάλλει ο Κώδικας αυτός.

Στη συνέχεια, η Εταιρεία πρέπει να θεσπίσει και να εφαρμόσει μια πολιτική για την επίτευξη αυτών των στόχων. Αυτό περιλαμβάνει την παροχή των απαραίτητων πόρων και την υποστήριξη στη ξηρά.

Κάθε εταιρεία αναμένεται να ορίσει ένα πρόσωπο ή κάποια πρόσωπα στην ξηρά που έχουν άμεση πρόσβαση στο υψηλότερο επίπεδο διοίκησης, προκειμένου να υπάρξει σύνδεση μεταξύ της εταιρείας και εκείνων που βρίσκονται στο πλοίο.

Οι διαδικασίες που απαιτούνται από τον κώδικα πρέπει να τεκμηριώνονται και να καταρτίζονται σε ένα εγχειρίδιο διαχείρισης της ασφάλειας, αντίγραφο του οποίου θα πρέπει να διατηρείται και επί του σκάφους.

(http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx)

Ο θαλάσσιος κίνδυνος στον κυβερνοχώρο αναφέρεται σε ένα μέτρο του βαθμού στον οποίο ένα ενεργητικό τεχνολογίας θα μπορούσε να απειληθεί από μια πιθανή περίπτωση ή γεγονός που μπορεί να οδηγήσει σε λειτουργικές αποτυχίες, αστοχίες ασφάλειας ή ασφάλειας ως συνέπεια της αλλοίωσης, απώλειας ή απώλειας πληροφοριών ή συστημάτων συμβιβασμός (http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

Ως διαχείριση του κυβερνοχώρου νοείται η διαδικασία εντοπισμού, ανάλυσης, αξιολόγησης και επικοινωνίας ενός σχετικού με τον κυβερνοχώρο κινδύνου και η αποδοχή, αποφυγή, μεταφορά ή μετριασμός του σε αποδεκτό επίπεδο, λαμβάνοντας υπόψη το κόστος και τα οφέλη των ενεργειών που αναλαμβάνονται στους ενδιαφερόμενους φορείς (http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

Ο γενικός στόχος είναι να υποστηριχθεί η ασφαλής και ασφαλής ναυτιλία, η οποία είναι λειτουργικά ανθεκτική στους κινδύνους του κυβερνοχώρου (http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

2.7.1 IMO- MSC

Ο IMO έχει εκδώσει σχετικές κατευθυντήριες γραμμές οι οποίες εμπεριέχονται στην MSC-FAL.1 / Circ.3 για τη διαχείριση και την ασφάλεια του θαλάσσιου κυβερνοχώρου.

Οι κατευθυντήριες γραμμές παρέχουν συστάσεις υψηλού επιπέδου σχετικά με τη διαχείριση του κυβερνοχώρου στη ναυτιλία έτσι ώστε να επιτυγχάνεται η διασφάλιση της ναυτιλίας από τις τρέχουσες και αναδυόμενες απειλές και ευπάθειες του κυβερνοχώρου. Αυτές οι κατευθυντήριες γραμμές περιλαμβάνουν λειτουργικά στοιχεία που υποστηρίζουν την αποτελεσματική διαχείριση του κυβερνοχώρου. Οι συστάσεις μπορούν να ενσωματωθούν στις υπάρχουσες διαδικασίες διαχείρισης κινδύνων και να συμπληρώσουν τις πρακτικές διαχείρισης της ασφάλειας που έχουν ήδη θεσπιστεί από τον IMO (http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx).

Η επιτροπή Ναυτιλιακής Ασφάλειας ενέκρινε στις 16 Ιουνίου 2017 το Παράρτημα 10 (Annex 10) το ψήφισμα MSC.428_(98). Το ψήφισμα αναφέρει ότι ένα εγκεκριμένο σύστημα διαχείρισης της ασφάλειας (SMS) πρέπει να λαμβάνει υπόψη τη διαχείριση του κυβερνοχώρου σύμφωνα με τους στόχους και τις λειτουργικές απαιτήσεις του κώδικα ISM. Έτσι, ενθαρρύνει τις διοικήσεις να διασφαλίσουν ότι οι κίνδυνοι στον κυβερνοχώρο αντιμετωπίζονται κατάλληλα στα συστήματα διαχείρισης της ασφάλειας το αργότερο κατά την πρώτη ετήσια επαλήθευση του εγγράφου συμμόρφωσης (DOC) της εταιρείας μετά την 1η Ιανουαρίου 2021. Αν και δεν είναι ακόμη υποχρεωτικό, οι εταιρείες θα έπρεπε να έχουν αρχίσει να αναπτύσσουν πολιτικές στον κώδικα ISM τους ώστε να είναι έτοιμες να διασφαλίσουν ασφάλεια (http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx).

Πιο συγκεκριμένα το ψήφισμα MSC.428_(98) το οποίο αφορά τη διαχείριση κινδύνου της ασφάλειας στα συστήματα στη ναυτιλία, αναγνωρίζοντας την ανάγκη να αυξηθεί η ευαισθητοποίηση σχετικά με τις απειλές και τα τρωτά σημεία του κυβερνοχώρου για την

υποστήριξη ασφάλειας και προστασίας στη ναυτιλία, η οποία είναι λειτουργικά ανθεκτική στους κινδύνους του κυβερνοχώρου, αναγνωρίζοντας επίσης ότι οι διοικήσεις, οι νηογνώμονες, οι πλοιοκτήτες και τα πλοία, οι παραγωγοί εξοπλισμού, οι πάροχοι υπηρεσιών, οι λιμένες και οι λιμενικές εγκαταστάσεις και όλοι οι άλλοι ενδιαφερόμενοι ναυτιλιακοί κλάδοι θα πρέπει να επιταχύνουν τις εργασίες για τη διασφάλιση της ναυτιλίας από τις τρέχουσες και αναδυόμενες απειλές και ευπάθειες του κυβερνοχώρου, λαμβάνοντας υπόψη την MSC-FAL.1 / Circ.3 σχετικά με τις κατευθυντήριες γραμμές για τη διαχείριση του θαλάσσιου κυβερνοχώρου που εγκρίθηκαν από την επιτροπή διευκόλυνσης κατά την 41η συνεδρίασή της (4-7 Απριλίου 2017) και από την Επιτροπή Ναυτικής Ασφάλειας, την 98η σύνοδο (7 έως 16 Ιουνίου 2017), η οποία παρέχει συστάσεις υψηλού επιπέδου για τον θαλάσσιο κυβερνοχώρο οι οποίες μπορούν να ενσωματωθούν στις υπάρχουσες διαδικασίες διαχείρισης κινδύνων και να συμπληρώσουν τις πρακτικές διαχείρισης της ασφάλειας και της ασφάλειας που έχει θεσπίσει ο εν λόγω Οργανισμός (http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx).

Υπενθυμίζοντας την απόφαση Α.741 (18) με την οποία η Συνέλευση ενέκρινε τον Διεθνή Κώδικα Διαχείρισης για την Ασφαλή Λειτουργία των Πλοίων και την Πρόληψη της Ρύπανσης (Κώδικας Διεθνούς Διαχείρισης Ασφάλειας (ISM)) και αναγνωρίζει, μεταξύ άλλων, την ανάγκη κατάλληλης οργάνωσης της διαχείρισης επιτρέπουν την ανταπόκριση στην ανάγκη των επιβατών να επιτύχουν και να διατηρούν υψηλά πρότυπα ασφάλειας και προστασίας του περιβάλλοντος, Σημειώνοντας τους στόχους του κώδικα ISM που περιλαμβάνουν, μεταξύ άλλων, την παροχή ασφαλών πρακτικών στη λειτουργία των πλοίων και την ασφαλή εργασία στην εκτίμηση όλων των διαπιστωθέντων κινδύνων για τα πλοία, το προσωπικό και το περιβάλλον, τη θέσπιση κατάλληλων διασφαλίσεων και τη συνεχή βελτίωση των δεξιοτήτων διαχείρισης του προσωπικού και των πλοίων (http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx).

1. ΕΠΙΒΕΒΑΙΩΝΕΙ ότι ένα εγκεκριμένο σύστημα διαχείρισης της ασφάλειας πρέπει να λαμβάνει υπόψη τη διαχείριση του κυβερνοχώρου σύμφωνα με τους στόχους και τις λειτουργικές απαιτήσεις του κώδικα ISM.

2. ΕΝΘΑΡΡΥΝΕΙ τις αρχές να διασφαλίσουν ότι οι κίνδυνοι στον κυβερνοχώρο αντιμετωπίζονται κατάλληλα στα συστήματα διαχείρισης της ασφάλειας το αργότερο κατά την πρώτη ετήσια επαλήθευση του εγγράφου συμμόρφωσης της εταιρείας μετά την 1η Ιανουαρίου 2021 ·
3. ΑΝΑΓΝΩΡΙΖΕΙ τις απαραίτητες προφυλάξεις που θα μπορούσαν να χρειαστούν για τη διατήρηση της εμπιστευτικότητας ορισμένων πτυχών της διαχείρισης του κυβερνοχώρου.
4. ΖΗΤΑ από τα κράτη μέλη να θέσουν το παρόν ψήφισμα υπόψη όλων των ενδιαφερομένων

(http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx).

2.7.2 TMSA3- MARITIME SECURITY

Το TMSA 3 είναι το σύστημα αξιολόγησης δεξαμενοπλοίων και σχετικά με το cyber security στα δεξαμενόπλοια αναφέρει το element 13 του TMSA 3 και εφαρμόζεται υποχρεωτικά από την 1η Ιανουαρίου 2018 (TMSA 3- MARITIME SECURITY – ELEMENT 13).

Κύριος Στόχος

Η δημιουργία ενός ασφαλούς και προστατευμένου εργασιακού περιβάλλοντος ώστε να αναπτυχθεί μια προορατική προσέγγιση στη διαχείριση της ασφάλειας. Επιπρόσθετα, να μετριαστούν οι κίνδυνοι ασφαλείας και να ελαχιστοποιηθούν οι συνέπειες τυχόν παραβιάσεων της ασφάλειας που επηρεάζουν ή δυνητικά επηρεάζουν το προσωπικό και τα περιουσιακά στοιχεία σε όλες τις τοποθεσίες της εταιρείας (TMSA 3- MARITIME SECURITY – ELEMENT 13).

Διαχείριση Ασφάλειας

Η αποτελεσματική διαχείριση της ασφάλειας απαιτεί τον συστηματικό προσδιορισμό των απειλών σε όλους τους τομείς της επιχείρησης, με μέτρα που εφαρμόζονται για τον μετριασμό των κινδύνων στο χαμηλότερο πρακτικό επίπεδο. Λόγω της συνεχώς μεταβαλλόμενης κατάστασης της ασφάλειας στη θάλασσα, η εταιρεία διαθέτει σύστημα παρακολούθησης και διαχείρισης αλλαγών, που συμπληρώνεται από μια κλιμακωτή προσέγγιση της ασφάλειας(TMSA 3- MARITIME SECURITY – ELEMENT 13).

Η εταιρεία διασφαλίζει ότι:

- Τα σχέδια ασφάλειας καλύπτουν όλες τις πτυχές των δραστηριοτήτων τους.
- Υπάρχουν διαδικασίες για τον εντοπισμό απειλών που καλύπτουν όλες τις επιχειρηματικές δραστηριότητες.
- Έχουν ληφθεί μέτρα για την άμβλυνση και αντιμετώπιση των εντοπισμένων απειλών.
- Οι πληροφορίες ασφαλείας διαχειρίζονται και ελέγχονται.
- Υπάρχουν διαδικασίες για την αναφορά πραγματικών περιστατικών και πιθανών απειλών.
- Εκπονούνται αξιολογήσεις κινδύνου για δραστηριότητες για τον εντοπισμό και την άμβλυνση πιθανών απειλών για την ασφάλεια.
- Το προσωπικό λαμβάνει την κατάλληλη εκπαίδευση ασφαλείας που εφαρμόζεται στις ευθύνες του
- Οι διαδικασίες περιλαμβάνουν τον εντοπισμό απειλών για την ασφάλεια στον κυβερνοχώρο, την ύπαρξη κατάλληλων κατευθυντήριων και μετριαστικών μέτρων και την ενεργό προώθηση της ευαισθητοποίησης.
- Η ταξιδιωτική πολιτική περιλαμβάνει πρόβλεψη για την ελαχιστοποίηση των απειλών για την ασφάλεια του προσωπικού.
- Οι διαδικασίες ασφάλειας ενημερώνονται τακτικά λαμβάνοντας υπόψη τις τελευταίες κατευθύνσεις του κλάδου.
- Η διαχείριση ασφάλειας περιλαμβάνεται στο πρόγραμμα εσωτερικού ελέγχου.
- Εκτιμούνται και ασκούνται ασκήσεις για την δοκιμή της ετοιμότητας.
- Ανεξάρτητη εξειδικευμένη υποστήριξη παρέχεται, κατά περίπτωση, για την αντιμετώπιση των εντοπισμένων απειλών.
- Τα σκάφη διαθέτουν βελτιωμένο εξοπλισμό ασφάλειας και παρακολούθησης.
- Οι βελτιώσεις ασφαλείας εξετάζονται για συμπερίληψη στις προδιαγραφές επαναφοράς και νέα σχέδια κατασκευής.
- Η καινοτόμος τεχνολογία ασφάλειας δοκιμάζεται και εφαρμόζεται ανάλογα με την περίπτωση.

Ασφάλεια στη ναυτιλία

Σκοπός - Καθιέρωση και διατήρηση πολιτικών και διαδικασιών για την αντιμετώπιση και τον μετριασμό των εντοπισμένων απειλών ασφάλειας που καλύπτουν όλες τις δραστηριότητες

της εταιρείας, συμπεριλαμβανομένης της ασφάλειας στον κυβερνοχώρο (TMSA 3- MARITIME SECURITY – ELEMENT 13).

ΠΑΡΑΓΡΑΦΟΣ 13.1 TMSA 3

1) Υπάρχουν τεκμηριωμένα σχέδια ασφάλειας τα οποία καλύπτουν όλες τις πτυχές των δραστηριοτήτων συμπεριλαμβανομένων:

- Τοποθεσιών που βασίζονται στην ξηρά.
- Σκαφών.
- Προσωπικού.

Το προσωπικό που είναι υπεύθυνο για θέματα που αφορούν την ασφάλεια εντοπίζεται.

2) Η εταιρεία έχει τεκμηριώσει τις διαδικασίες που εφαρμόζονται για τον εντοπισμό των απειλών ασφάλειας που ισχύουν για τις περιοχές εμπορίας σκαφών και τις τοποθεσίες που βασίζονται στην ξηρά. Οι απειλές κατά της ασφάλειας μπορεί να περιλαμβάνουν:

- Μικροκλοπές.
- Βανδαλισμούς.
- Λαθρεπιβάτες.
- Κλοπή φορτίου.
- Cyber απειλή.
- ανεπαρκής ασφάλεια λιμένων.
- Εμπορία ανθρώπων, όπλων ή ναρκωτικών.
- Λαθρεμπόριο.
- Πειρατεία.
- Σαμποτάζ και εμπρησμός.
- Τρομοκρατία και τα επακόλουθα αποτελέσματα.

Οι απειλές που θα εντοπισθούν, εξετάζονται όπως απαιτούν οι καταστάσεις.

3) Έχουν αναπτυχθεί μέτρα για τον μετριασμό και την αντιμετώπιση όλων των εντοπισμένων απειλών για τα σκάφη και τις τοποθεσίες που βρίσκονται στη ξηρά. σε σκάφη και σε τοποθεσίες με βάση τις ακτές. Τα μέτρα μετριασμού μπορεί να περιλαμβάνουν:

- Έλεγχο πρόσβασης.

- Τα μέτρα φυσικής ασφάλειας
- άσκηση και εκπαίδευση.
- Αστυνομικές περιπολίες.
- Έρευνες.

Υπάρχουν σχέδια έκτακτης ανάγκης για την αντιμετώπιση ενδεχόμενων παραβιάσεων της ασφάλειας.

4) Υπάρχουν διαδικασίες για την απόκτηση, διαχείριση και αναθεώρηση των σημερινών πληροφοριών που σχετίζονται με την ασφάλεια. Οι πληροφορίες ασφαλείας λαμβάνονται από την εταιρεία από κατάλληλες πηγές που μπορεί να περιλαμβάνουν:

- Διεθνείς και εθνικές υπηρεσίες.
- Περιφερειακά κέντρα παροχής πληροφοριών για την ασφάλεια στη θάλασσα.
- Κράτος σημαίας.
- Οργανισμοί της βιομηχανίας.
- Τοπικοί πράκτορες.
- Στρατιωτικές πηγές.
- Ειδικοί σύμβουλοι.

Το υπεύθυνο άτομο εξετάζει τις πληροφορίες και εκδίδει σχετική καθοδήγηση στις τοποθεσίες, το προσωπικό και τα πλοία που βασίζονται στην ξηρά, ανάλογα με την περίπτωση.

5) Οι διαδικασίες περιλαμβάνουν την αναφορά δυνητικών απειλών ασφάλειας και πραγματικών περιστατικών ασφάλειας Οι διαδικασίες αναφοράς μπορούν να περιλαμβάνουν:

- Εσωτερική αναφορά πλοίων.
- Πλοίο προς την εταιρεία.
- Σκάφος προς εξωτερικές αρχές
- Εταιρεία προς εξωτερικές αρχές

ΠΑΡΑΓΡΑΦΟΣ 13.2 TMSA 3

1) Εκπονούνται επίσημες εκτιμήσεις κινδύνων για τις δραστηριότητες της εταιρείας για τον εντοπισμό και την άμβλυνση πιθανών απειλών για την ασφάλεια.

Οι αξιολογήσεις κινδύνου επανεξετάζονται τακτικά, ενημερώνονται και οι διαδικασίες της εταιρείας τροποποιούνται ανάλογα με τις ανάγκες. Οι αξιολογήσεις ειδικού κινδύνου για τα πλοία επανεξετάζονται πριν από την είσοδο σε περιοχές που χαρακτηρίζονται ως επικίνδυνες. Όταν η εκτίμηση επικινδυνότητας το κρίνει απαραίτητο, αναπτύσσονται, τεκμηριώνονται και εφαρμόζονται ειδικά μέτρα σκλήρυνσης του πλοίου. Εξετάζεται η ύπαρξη κατάλληλων υλικών / εξοπλισμού προστασίας των πλοίων, τα οποία στη συνέχεια μπορούν να καταγράφονται σε ειδικά μέτρα προστασίας του πλοίου / σχέδιο συλλογής

2) Το προσωπικό που είναι υπεύθυνο για την ασφάλεια λαμβάνει εκπαίδευση κατάλληλη για το ρόλο και τις δραστηριότητες της εταιρείας.

Η κατάρτιση αντικατοπτρίζει το πεδίο των δραστηριοτήτων της εταιρείας και, όπου απαιτείται, πληροί τις ελάχιστες διεθνείς ή εθνικές νομοθετικές απαιτήσεις. Εξετάζεται η ανάγκη κατάρτισης ενός αναπληρωτή για βασικούς ρόλους ασφαλείας Μια ενημέρωση για την ασφάλεια παρέχεται σε όλο το προσωπικό ως μέρος της διαδικασίας εξοικείωσης

3) Οι πολιτικές και οι διαδικασίες περιλαμβάνουν την ασφάλεια στον κυβερνοχώρο και παρέχουν κατάλληλα μέτρα καθοδήγησης και μετριασμού.

Οι κίνδυνοι για τα συστήματα πληροφορικής ενδέχεται να περιλαμβάνουν:

- Σκόπιμες και μη εξουσιοδοτημένες παραβιάσεις.
- Αθέλητες ή τυχαίες παραβιάσεις.
- Ανεπαρκής ακεραιότητα του συστήματος, όπως firewalls ή / και συστήματα προστασίας από ιούς.

Τα συστήματα με άμεσες ή έμμεσες επικοινωνιακές συνδέσεις, τα οποία μπορεί να είναι ευάλωτα σε εξωτερική απειλή ή ακατάλληλη χρήση, εντοπίζονται. Μπορεί να περιλαμβάνουν συστήματα πλοήγησης, μηχανικής, ελέγχου και επικοινωνίας. Κατά την ανάπτυξη διαδικασιών, η εταιρεία μπορεί να ανατρέξει στις σχετικές σημερινές οδηγίες του κλάδου.

4) Η εταιρεία προωθεί ενεργά την ευαισθητοποίηση στον κυβερνοχώρο. Χρησιμοποιούνται αποτελεσματικά μέσα για την ενθάρρυνση της υπεύθυνης συμπεριφοράς από το προσωπικό της ξηράς, το προσωπικό των πλοίων και τρίτους. Μια τέτοια συμπεριφορά μπορεί να περιλαμβάνει:

- Κλείδωμα των σταθμών εργασίας χωρίς παρακολούθηση.
- Διασφάλιση κωδικών πρόσβασης.
- Τη μη χρήση μη εξουσιοδοτημένου λογισμικού.
- Υπεύθυνη χρήση των κοινωνικών μέσων.
- Έλεγχο / πρόληψη της κακής χρήσης των φορητών συσκευών αποθήκευσης και μνήμης.

ΠΑΡΑΓΡΑΦΟΣ 13.3 TMSA 3

1) Η πολιτική ταξιδιών είναι σε ισχύ ώστε να πραγματοποιείται ελαχιστοποίηση των απειλών για την ασφάλεια του προσωπικού. Η πολιτική βασίζεται στην εκτίμηση κινδύνου και περιλαμβάνει το προσωπικό των πλοίων, το προσωπικό της ξηράς και τους εργολάβους που ταξιδεύουν για εργασίες της επιχείρησης. Όπου ενδείκνυται, υπάρχουν περιορισμοί και οδηγίες για ταξίδια που χαρακτηρίζονται ως υψηλού κινδύνου. Η ταξιδιωτική πολιτική αναθεωρείται τακτικά ώστε να λαμβάνονται υπόψη οι αλλαγές στις απειλές για την ασφάλεια.

2) Οι διαδικασίες ασφάλειας ενημερώνονται λαμβάνοντας υπόψη την τρέχουσα καθοδήγηση.

Η καθοδήγηση του κλάδου μπορεί να περιλαμβάνει:

- Καλύτερες διαχειριστικές πρακτικές για την προστασία κατά της πειρατείας η οποία βρίσκεται στη Σομαλία
- Τη διακίνηση ναρκωτικών και η Κατάχρηση Φαρμάκων (ICS).
- Τη ναυτική ασφάλεια - Καθοδήγηση σχετικά με τον κώδικα ISPS (ICS),
- Διαγράμματα σχεδιασμού ασφάλειας.
- Οδηγίες για την ασφάλεια στον κυβερνοχώρο από τη βιομηχανία και την κλάση.

- Λειτουργίες διάσωσης μεγάλης κλίμακας στη θάλασσα (ICS).
- Περιφερειακό οδηγό για την καταπολέμηση της πειρατείας και της ένοπλης ληστείας κατά των πλοίων στην Ασία (ReCAAP-ISC).

Στα σκάφη της εταιρείας παρέχονται οι τελευταίες εκδόσεις σχετικών δημοσιεύσεων σχετικά με την ασφάλεια.

3) Η πολιτική ασφάλειας και οι συναφείς διαδικασίες εμπίπτουν στο πρόγραμμα εσωτερικού ελέγχου. Ο έλεγχος αξιολογεί τη συμμόρφωση με όλες τις πτυχές των διαδικασιών ασφαλείας της εταιρείας, συμπεριλαμβανομένης της προσωπικής ευαισθητοποίησης και συμπεριφοράς.

ΠΑΡΑΓΡΑΦΟΣ 13.4 TMSA 3

1) Εκτίμηση των μέτρων ασφαλείας και η ετοιμότητα της εταιρείας. Οι αξιολογήσεις μπορούν να διεξάγονται από εσωτερικό προσωπικό ή από εξωτερικούς πόρους.

2) Ανεξάρτητη εξειδικευμένη υποστήριξη χρησιμοποιείται για την άμβλυνση των εξειδικευμένων απειλών ασφάλειας

Όλες οι συμβάσεις ειδικής υποστήριξης, τόσο επί του σκάφους όσο και στην ξηρά, υποστηρίζονται από ένα εκτεταμένο πεδίο εργασιών. Αυτή η στήριξη μπορεί να ανατεθεί για δραστηριότητες που συμπεριλαμβάνουν την εκπαίδευση, την ασφάλεια και τις αξιολογήσεις απειλών και τα καθήκοντα φύλαξης. Πριν από τη σύναψη μιας σύμβασης, η εταιρεία δεν διεξάγει εμπεριστατωμένη αξιολόγηση δέουσας επιμέλειας του προτεινόμενου συμβαλλομένου, συμπεριλαμβανομένης της συμμόρφωσης με τα σχετικά πρότυπα. Καθοδήγηση σχετικά με το συμβόλαιο των συμβούλων ασφαλείας επί του πλοίου και το πεδίο των εργασιών τους παρέχεται στον πλοίαρχο.

3) Τα σκάφη διαθέτουν βελτιωμένο εξοπλισμό ασφάλειας και παρακολούθησης.

Παραδείγματα τέτοιου εξοπλισμού περιλαμβάνουν:

- Τα κανόνια νερού.
- Εξοπλισμό θερμικής απεικόνισης.

- Ραντάρ πρύμνης.
- Ταινία εκτόξευσης για Windows.
- Συστήματα εισόδου πληκτρολογίου.
- Συστήματα παρακολούθησης και καταγραφής CCTV.
- Ένα δευτερεύον μέσο ανεξάρτητης δορυφορικής τηλεφωνικής επικοινωνίας.

4) Οι βελτιώσεις ασφαλείας εξετάζονται για συμπερίληψη στις προδιαγραφές επαναφοράς και τον σχεδιασμό νέας κατασκευής.

Οι βελτιώσεις και οι προδιαγραφές ενδέχεται να εξαρτώνται από:

- Την περιοχή των συναλλαγών.
- Τον τύπο του σκάφους και το μέγεθος
- Τα επίπεδα επάνδρωσης.

5) Η εταιρεία συμμετέχει στη δοκιμή και εφαρμογή καινοτόμων συστημάτων τεχνολογίας ασφαλείας.
Αυτό μπορεί να περιλαμβάνει:

- Φυσικά μέτρα για τη βελτίωση της ασφάλειας
- Βελτιώσεις λογισμικού σε συστήματα πληροφορικής.

2.7.3 VIQ 7

Το Vessel Inspection Questionnaire (VIQ) αφορά επιθεωρήσεις μεγίστης σημασίας σε δεξαμενόπλοια μεταφοράς καυσίμων και χημικών αερίων. Σε περιπτώσεις των εταιρειών Shell, BP κτλ, το VIQ είναι απαραίτητο. Σε σχέση με το Cyber security δίνεται ιδιαίτερη έμφαση στο κεφάλαιο 7 του κανονισμού (VIQ version 7.0.05, 2019). Αυτό είναι ένα ερωτηματολόγιο το οποίο θα πρέπει να απαντηθεί ορθά από την εταιρεία σε τέτοιου είδους επιθεωρήσεις.

Σχετικά με την κυβερνοασφάλεια παρακάτω, παρουσιάζονται οι παράγραφοι του 7^{ου} κεφαλαίου οι οποίοι σχετίζονται με αυτή:

7.14 Υπάρχουν πολιτικές και διαδικασίες για την ασφάλεια στον κυβερνοχώρο οι οποίες αποτελούν μέρος του Συστήματος Διαχείρισης Ασφάλειας και σχέδιο Cyber Response στο σκάφος;

Σημείωση: Οι διαδικασίες περιλαμβάνουν αξιολόγηση κινδύνου για θέματα όπως:

- Απειλές όπως από κακόβουλο λογισμικό όπως επιθέσεις ηλεκτρονικού "ψαρέματος" κλπ.
- Ταυτοποίηση και προστασία των ευάλωτων συστημάτων (ECDIS κλπ.).
- Μέτρα μετριασμού (έλεγχος USB κλπ.).
- Προσδιορισμός του βασικού προσωπικού εντός της επιχείρησης (συμπεριλαμβανομένου του για ποιόν ο πλοίαρχος αναφέρει ύποπτα περιστατικά).
- Αντίγραφα κρατούν οι βασικές επαφές (όπως ο DPA, ο CSO κλπ.).
- Διαχείριση και εγγραφή κωδικών πρόσβασης.
- Συμμόρφωση με τον ανάδοχο.

Σημείωση: Το σχέδιο Cyber Response περιλαμβάνει οδηγίες σχετικά με:

- Τι είδους «συμπτώματα» πρέπει να αναζητηθούν.
- Τις άμεσες ενέργειες που πρέπει να αναληφθούν, και τέλος
- Το όνομα, τη θέση, τον αριθμό τηλεφώνου και το ηλεκτρονικό ταχυδρομείο για το υπεύθυνο πρόσωπο που θα είναι σε θέση να επικοινωνήσει μαζί σας.

7.15 Γνωρίζει το πλήρωμα την πολιτική της εταιρείας για τον έλεγχο της φυσικής πρόσβασης για όλα τα συστήματα IT/OT επί του πλοίου;

Σημείωση: Οι επιθεωρητές θα πρέπει να προσέχουν εάν η πρόσβαση στις θύρες USB στους τερματικούς σταθμούς IT/OT του πλοίου ελέγχεται ή υπάρχουν μέτρα για να μπλοκάρουν ή να κλειδώνουν τις θύρες σε αυτούς τους ακροδέκτες. Οι διαδικασίες θα πρέπει να περιλαμβάνουν την προστασία του κρίσιμου εξοπλισμού όπως το ECDIS, από επιθέσεις κακόβουλου λογισμικού και ιών. Επίσης, θα πρέπει να περιλαμβάνουν τον έλεγχο της πρόσβασης σε όλα τα τερματικά IT/OT του πλοίου συμπεριλαμβανομένης της πρόσβασης στους διακομιστές οι οποίοι θα πρέπει να βρίσκονται σε ασφαλή τοποθεσία. Οι διαδικασίες

θα πρέπει επίσης να περιλαμβάνουν πρόσβαση από κάθε είδους τρίτους συμβαλλόμενους και τεχνικούς.

7.16 έχει η εταιρεία πολιτική καθοδήγηση σχετικά με τη χρήση ιδιωτικών-προσωπικών συσκευών επί του σκάφους;
Οι προσωπικές συσκευές περιλαμβάνουν κινητό τηλέφωνο, τάμπλετ, φορητό υπολογιστή κτλ. Επίσης, συσκευές αποθήκευσης όπως σκληρούς δίσκους, USB κτλ. Γίνεται έλεγχος αν η πολιτική εφαρμόζεται τόσο από το πλήρωμα όσο και από τους επισκέπτες στο πλοίο όπως για παράδειγμα όλους τους συμβαλλόμενους και τεχνικούς τρίτου μέρους.

7.17 Είναι η ευαισθητοποίηση σχετικά με το Cyber Security, ενεργά προωθημένη επί του πλοίου;
Τα παραδείγματα της ενεργής προώθησης περιλαμβάνουν:

- Υλικό ευαισθητοποίησης σχετικά με την ασφάλεια στον κυβερνοχώρο.
- Κατάρτιση πληρώματος μέσω ταινιών.
- Εξειδικευμένη εκπαίδευση πληρώματος.
- Οδηγίες για τη διασφάλιση των κωδικών πρόσβασης στο σύστημα.
- Υπεύθυνη χρήση των κοινωνικών μέσων.
- Πολιτική σχετικά με τη χρήση των προσωπικών συσκευών και την ένταξή τους στο πλοίο, με τη συμμετοχή λιστών ελέγχου εξοικείωσης.
- Μπορεί να συμπεριλαμβάνει συμφωνίες για την πολιτική των εγκεκριμένων πολιτικών χρήσης (AUP) των εργαζομένων.
- Η εταιρεία να είναι πιστοποιημένη σύμφωνα με το πρότυπο ISO 27000.

2.7.4 IACS

Ο IACS- International Association of Classification Society, είναι μια μη κερδοσκοπική οργάνωση καταχώρησης νηογνωμόνων η οποία θεσπίζει τα ελάχιστα τεχνικά πρότυπα και τις απαιτήσεις που αφορούν την ασφάλεια στη θάλασσα και την προστασία του περιβάλλοντος και εξασφαλίζει τη συνεπή εφαρμογή τους. Σχετικά με το Cyber security στη ναυτιλία ο IACS έχει θεσπίσει κάποιες συστάσεις σχετικά κε την ασφάλεια στον κυβερνοχώρο

(http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-change-in-delivery-of-cyber-resilient-ships/).

Οι συστάσεις του IACS απορρέουν από εκτεταμένη συνεργασία σε ολόκληρη τη βιομηχανία και παρέχουν πολύ αναγκαίες οδηγίες σχετικά με τον τρόπο ανάπτυξης και διατήρησης της ακεραιότητας του κυβερνοχώρου των σκαφών.

Ο IACS δημοσίευσε 9 από τις 12 συστάσεις του σχετικά με την ασφάλεια στον κυβερνοχώρο με στόχο να καταστήσει δυνατή την παράδοση ανθεκτικών στο κυβερνοχώρο πλοίων, των οποίων η αντοχή μπορεί να διατηρηθεί καθ όλη τη διάρκεια της επαγγελματικής τους ζωής.

Αυτές οι συστάσεις είναι το αποτέλεσμα μιας μακροπρόθεσμης πρωτοβουλίας του IACS, η οποία έχει ωφεληθεί σημαντικά από την εισροή και τη στήριξη από τη βιομηχανία.

Ο IACS αρχικά ασχολήθηκε με το θέμα της ποιότητας του λογισμικού με τη δημοσίευση του UR E22 το 2006. Αναγνωρίζοντας την τεράστια αύξηση της χρήσης του κυβερνοχώρου επί του σκάφους και από τότε ανέπτυξε αυτή τη σειρά συστάσεων με σκοπό να αντικατοπτρίζει τις απαιτήσεις ανθεκτικότητας ενός πλοίου με πολλές περισσότερες αλληλεξαρτήσεις.

<u>Ως αποτέλεσμα, οι συστάσεις του IACS αντιμετωπίζουν την ανάγκη για:</u>

- Την κατανόηση της αλληλεπίδρασης μεταξύ των συστημάτων του πλοίου.
- Την προστασία από συμβάντα πέρα από τα πιθανά σφάλματα λογισμικού.
- Σε περίπτωση αποτυχίας προστασίας, την ανάγκη για κατάλληλη ανταπόκριση και τελικά την ανάκτηση των δεδομένων.
- Των μέσων ανίχνευσης που απαιτούνται έτσι ώστε να μπορέσει να εφαρμοστεί η κατάλληλη απάντηση.

Ο IACS αναγνώρισε επίσης σε πρώιμο στάδιο ότι για να μπορέσουν τα πλοία να είναι ανθεκτικά έναντι των περιστατικών στον κυβερνοχώρο, θα έπρεπε να συμμετέχουν όλα τα τμήματα του κλάδου ενεργά και έτσι συγκάλεσε μια κοινή ομάδα εργασίας (JWG) για τα συστήματα Cyber Security. Σημαντικό μέρος του έργου της ομάδας αυτής αποτέλεσε ο εντοπισμός βέλτιστων πρακτικών των κατάλληλων υφιστάμενων προτύπων στον τομέα του κινδύνου και της ασφάλειας στον κυβερνοχώρο και ο εντοπισμός μιας πρακτικής προσέγγισης κινδύνου. Κατά συνέπεια, οι 12 συστάσεις του IACS, συλλογικά, δεν παρέχουν μόνο καθοδήγηση σχετικά με τους πιο πιεστικούς τομείς ανησυχίας, αλλά λειτουργούν ως δομικά στοιχεία για τον ευρύτερο στόχο της ανθεκτικότητας του συστήματος (http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-change-in-delivery-of-cyber-resilient-ships/).

Ο IACS δρομολόγησε τις εν λόγω συστάσεις με την προσδοκία ότι θα εξελιχθούν ταχέως σε σχέση με τις παραδοσιακές τεχνικές και διαδικασίες σχετικά με τη διασφάλιση της ασφάλειας, εξαιτίας της εμπειρίας που αποκτήθηκε από την πρακτική εφαρμογή τους. Επιπλέον, αναγνωρίζει ότι οι εν λόγω συστάσεις είναι μόνο ένα «ενδιάμεσο» προϊόν και ότι θα αποτελέσουν αντικείμενο συγχώνευσης σε ένα ευρύτερο έγγραφο με συνεκτικότερη γλώσσα, αλληλεπικαλύψεις που αφαιρούνται και κοινό υλικό ενοποιημένο. επίσης, αναγνωρίζει ότι η παράδοση αυτών των σημαντικών σειρών συστάσεων είναι μόνο η αρχή της συνεχούς προσπάθειας για τη διατήρηση της ακεραιότητας του κυβερνοχώρου των πλοίων. Ωστόσο, διατηρεί την πεποίθηση ότι η ευέλικτη και διαρθρωμένη προσέγγιση που υιοθετείται, θέτει σε καλό δρόμο την περαιτέρω εξέλιξη και ενίσχυση αυτών των προσφορών, με ταχύτητα και ανταπόκριση, με τρόπο πρακτικό και υποστηρίζοντας τις ανάγκες του μεγαλύτερου αριθμού ενδιαφερόμενων μερών της βιομηχανίας (http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-change-in-delivery-of-cyber-resilient-ships/).

Οι 12 συστάσεις είναι:

- Εγγραφή 153: Συνιστώμενες διαδικασίες για τη συντήρηση λογισμικού του εξοπλισμού και των συστημάτων πλοίων.
- Εγγραφή 154: Σύσταση σχετικά με τις δυνατότητες χειρωνακτικής / τοπικής ρύθμισης για συστήματα μηχανημάτων που εξαρτώνται από το λογισμικό.
- Εγγραφή 155: Σχέδιο έκτακτης ανάγκης για ενσωματωμένα συστήματα υπολογιστών.
- Εγγραφή 156: Αρχιτεκτονική δικτύου.
- Εγγραφή 157: Διασφάλιση Δεδομένων
- Εγγραφή 158: Φυσική ασφάλεια των ενσωματωμένων συστημάτων υπολογιστών
- Εγγραφή 159: Ασφάλεια δικτύων επί των ενσωματωμένων συστημάτων υπολογιστών
- Εγγραφή 160: Σχεδιασμός συστήματος πλοίων.
- Εγγραφή 161: Λίστα απογραφής των συστημάτων που βασίζονται σε υπολογιστές.
- Εγγραφή 162: Ενσωμάτωση.
- Εγγραφή 163: Απομακρυσμένη Πρόσβαση.
- Εγγραφή 164: Επικοινωνία και διεπαφές.

(http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-change-in-delivery-of-cyber-resilient-ships/).

2.7.5 Πρότυπο ISO 27001

Σύμφωνα με το ISO 27001, ένα σύστημα διαχείρισης ασφάλειας πληροφοριών είναι: ¨*Εκείνο το μέρος του συνολικού συστήματος διαχείρισης, το οποίο βασιζόμενο σε μία προσέγγιση επιχειρηματικού κινδύνου, εγκαθιδρυθεί, δημιουργεί, λειτουργεί, παρακολουθεί, ανασκοπεί, διατηρεί και βελτιώνει την ασφάλεια των πληροφοριών*¨ (INTERNATIONAL STANDARD ISO/ IEC 27000:2016).

Μπορεί να ειπωθεί πως ένα σύστημα διαχείρισης ασφάλειας πληροφοριών είναι μία ολοκληρωμένη, οργανωμένη και συνεχή αντιμετώπιση των θεμάτων ασφαλείας.

Ένα σύστημα διαχείρισης ασφάλειας πληροφοριών έχει 2 γενικούς στόχους:
Την Πρόληψη και την Αντιμετώπιση.
Ένα σύστημα πρέπει να είναι έτσι σχεδιασμένο ώστε να εκπληρώνει και τους δύο αυτούς στόχους σε συνδυασμό και όχι τον κάθε ένα χωριστά. Το σύστημα θα πρέπει να περιέχει εκείνα τα στοιχεία που θα του επιτρέπουν να θωρακίζει τον οργανισμό απέναντι σε όσο το δυνατόν περισσότερους κινδύνους και ταυτόχρονα σε περίπτωση εμφάνισης προβλήματος να διαθέτει εκείνους τους μηχανισμούς που θα του επιτρέπουν να το αντιμετωπίσει αποτελεσματικά, με την μικρότερη δυνατή ζημιά και στον μικρότερο δυνατό χρόνο.
Πρέπει να τονιστεί ότι κανένα σύστημα ασφάλειας πληροφοριών δεν είναι 100% αδιάβλητο. Η τεχνολογία βρίσκεται σε συνεχή εξέλιξη και γι' αυτόν τον λόγο οι πρακτικές που ακολουθούμε θα πρέπει να είναι ενημερωμένες έτσι ώστε να μην εκθέτουν σε κίνδυνο τον οργανισμό. Η λύση σε κάθε περίπτωση είναι η όσο το δυνατόν καλύτερη προετοιμασία (πρόληψη) και όσο το δυνατόν καλύτερη αντιμετώπιση σε περίπτωση εμφάνισης περιστατικού(INTERNATIONAL STANDARD ISO/ IEC 27000:2016).

2.7.5.1 Η δομή του προτύπου

Το πρότυπο αποτελείται από 10 βασικές παραγράφους, ενώ ακολουθείται από το παράρτημα Α (Annex A), που είναι κανονιστικό και αναφέρεται στους μηχανισμούς και στις απαιτήσεις ανά είδος υποδομής και ιδιαιτεροτήτων συστήματος (INTERNATIONAL STANDARD ISO/ IEC 27000:2016).

Σκοπός:

Το πρότυπο ISO 27001 παρέχει τις ελάχιστες απαιτήσεις για τη διαχείριση της ασφάλειας πληροφοριών. Απευθύνεται στους υπευθύνους υλοποίησης της ασφάλειας σε έναν οργανισμό. Περιγράφει μία κοινή βάση για την ανάπτυξη επιπέδων ασφαλείας μέσα στον οργανισμό, την αποτελεσματική διαχείριση της ασφάλειας των πληροφοριών και τη δημιουργία εμπιστοσύνης κατά τις συναλλαγές ανάμεσα σε οργανισμούς. Το πρότυπο αυτό δεν είναι πάνω από τις νομικές απαιτήσεις κάθε χώρας και κάθε σύστημα που εφαρμόζεται στις εταιρείες θα πρέπει να συνδυάζει τις απαιτήσεις του προτύπου με τις νομικές απαιτήσεις κάθε χώρας .

Το πρότυπο είναι εφαρμόσιμο σε έναν οργανισμό που θα ήθελε να:

- Σχεδιάσει
- Δημιουργήσει
- Λειτουργήσει
- Παρακολουθήσει
- Ελέγξει
- Διατηρήσει και βελτιώσει το σύστημα διαχείρισης και ασφάλειας πληροφοριών πάντα σε συμφωνία με τους σκοπούς του οργανισμού στα πλαίσια της ασφάλειας (INTERNATIONAL STANDARD ISO/ IEC 27000:2016).

2.7.5.2 Εφαρμογή

Οι απαιτήσεις του προτύπου είναι γενικές και μπορούν να εκπληρωθούν από όλους τους οργανισμούς ανεξάρτητα του μεγέθους, της οργανωτικής δομής του αντικειμένου και του τομέα δραστηριοποίησης. Η κάλυψη των απαιτήσεων των παραγράφων 4 έως 10 του προτύπου είναι υποχρεωτική, ενώ όλα τα περιεχόμενα του παραρτήματος A (Annex A) είναι προαιρετικά και εξαρτάται από τη δυνατότητα εφαρμογής του σε κάθε οργανισμό. Σε κάθε περίπτωση, αυτή η εξαίρεση από τις παραγράφους του παραρτήματος A (Annex A), θα πρέπει να καταγράφεται και να αιτιολογείται κατάλληλα. Τέλος, οι όποιες εξαιρέσεις δε θα πρέπει να επηρεάζουν την ικανότητα να παρέχουν ένα επίπεδο ασφάλειας αντίστοιχο με αυτό που έχει προσδιοριστεί στην εκτίμηση κινδύνου και πάντα σε συμφωνία με τις ισχύουσες νομικές απαιτήσεις (INTERNATIONAL STANDARD ISO/ IEC 27000:2016)

Πιο αναλυτικά οι παράγραφοι 4 έως 10 (INTERNATIONAL STANDARD ISO/ IEC 27000:2016**:**

- Η Παράγραφος 4 αναφέρεται στο Πλαίσιο του οργανισμού το οποίο αποτελείται από:
  - ✓ Την κατανόηση του οργανισμού και του πλαισίου του.
  - ✓ Την κατανόηση των αναγκών και των προσδοκιών των ενδιαφερόμενων μερών της επιχείρησης.
  - ✓ Τον καθορισμό του πεδίου εφαρμογής του συστήματος διαχείρισης της ασφάλειας των πληροφοριών.
  - ✓ Το σύστημα διαχείρισης της ασφάλειας των πληροφοριών.

- Η Παράγραφος 5 αφορά την ηγεσία και αποτελείται από:
  - ✓ Την ηγεσία και τη δέσμευση.
  - ✓ Την πολιτική που εφαρμόζεται.
  - ✓ Τους οργανωτικούς ρόλους, τις ευθύνες και τις αρχές.

- Η Παράγραφος 6 αφορά το σχεδιασμό – προγραμματισμό και πραγματοποιείται:
  - ✓ Με τις δράσεις για την αντιμετώπιση των κινδύνων και των ευκαιριών.
  - ✓ Με τους στόχους για την ασφάλεια των πληροφοριών και τον προγραμματισμό για την επίτευξη τους.

- Η Παράγραφος 7 αφορά την υποστήριξη του συστήματος και πιο συγκεκριμένα:
  - ✓ Τους πόρους που χρησιμοποιεί.
  - ✓ Τις αρμοδιότητες του συστήματος.
  - ✓ Την επίγνωση.
  - ✓ Την επικοινωνία.
  - ✓ Τις τεκμηριωμένες πληροφορίες.

- Η Παράγραφος 8 αναφέρεται στη λειτουργία του συστήματος και πραγματοποιείται από:
  - ✓ Τον λειτουργικό σχεδιασμό και έλεγχο.
  - ✓ Την αξιολόγηση κινδύνου ασφάλειας πληροφοριών - Risk Assessment.
  - ✓ Την διαχείριση κινδύνων ασφάλειας πληροφοριών – Risk Treatment.

- Η Παράγραφος 9 αφορά την αξιολόγηση της απόδοσης και πραγματοποιείται:

- ✓ Με την παρακολούθηση, μέτρηση, ανάλυση, και αξιολόγηση του συστήματος.
- ✓ Με τον εσωτερικό έλεγχο – Internal Audit.
- ✓ Με επισκόπηση της διαχείρισης.

❖ Η Παράγραφος 10 αφορά τη βελτίωση και επιτυγχάνεται με:

- ✓ Τη μη συμμόρφωση και τις διορθωτικές ενέργειες που θα πρέπει να εφαρμοστούν στο σύστημα.
- ✓ Και τέλος με τη συνεχή βελτίωση.

2.8 Ασφαλιστικές

Η ψηφιοποίηση και το IoT (Internet of Things) της βιομηχανίας οδήγησε την ευπάθεια ενός συστήματος στις παραβιάσεις, την απώλεια δεομένων και τις επιθέσεις λιανικής πώλησης (MARSH, 2014). Ένα πλοίο και μια εταιρεία θα πρέπει να έχει την ικανότητα ναυσιπλοΐας και αξιοπιστίας. Αυτό πραγματοποιείται με τη δημιουργία άμυνας και ανθεκτικότητας στον κυβερνοχώρο και επιτυγχάνεται μέσω ενός ολοκληρωμένου πλαισίου διαχείρισης κινδύνου του κυβερνοχώρου. Επίσης, έχοντας σχέδια ανταπόκρισης σε Cyber incidents (περιστατικά στον κυβερνοχώρο) βοηθά να αποδειχθεί ότι ο οργανισμός είναι διατεθειμένος να ανταποκριθεί αποτελεσματικά σε επιθέσεις στον κυβερνοχώρο. Η ασφάλιση του κυβερνοχώρου (Cyber Insurance), αποτελεί μέρος της συνολικής διαδικασίας διαχείρισης κινδύνου ενός οργανισμού. Οι κίνδυνοι στον κυβερνοχώρο είναι σχετικά νέοι και οι ισχυρισμοί σχετικά με αυτούς τους κινδύνους είναι αρκετά περιορισμένοι (MARSH , 2014).

Οι πολιτικές ναυτασφαλίσεων (συμπεριλαμβανομένων των καλύψεων για τα ναυπηγεία και τις εγκαταστάσεις χειρισμού φορτίων) αποκλείουν την ευθύνη για τις απώλειες που σχετίζονται με τον υπολογιστή οι οποίες οφείλονται σε αποτυχία ασφάλειας υπολογιστών και δικτύου δηλαδή σε αποτυχία του συστήματος. Η κάλυψη εξαιρείται για κακόβουλα ή μη κακόβουλα περιστατικά στον κυβερνοχώρο είτε και για τα δύο. Τα ασφαλιστήρια συμβόλαια περιλαμβάνουν τη ρήτρα αποκλεισμού Institute Cyber Attack Exclusion Clause (CL 380) 10/11/2003. Αυτή είναι μια "ρήτρα ύψιστης σημασίας", δηλαδή πρέπει να περιλαμβάνεται σε όλες τις θαλάσσιες πολιτικές και αφαιρεί αποτελεσματικά όλη την κάλυψη από τους κινδύνους του κυβερνοχώρου. Συγκεκριμένα αναφέρεται:

“ ***Ρήτρα 1.1:*** *Με την επιφύλαξη μόνο της παραγράφου 1.2 κατωτέρω, σε καμία περίπτωση η ασφαλιστική αυτή κάλυψη δεν θα πρέπει να καλύπτει ζημιές ή ζημίες που προκλήθηκαν άμεσα ή*

έμμεσα από ή προερχόμενα από ή προερχόμενα από οποιοδήποτε μέσο για την πρόκληση βλάβης οποιουδήποτε υπολογιστή, λογισμικό ηλεκτρονικού υπολογιστή, κακόβουλο κώδικα, ιό υπολογιστή ή διαδικασία ή οποιοδήποτε άλλο ηλεκτρονικό σύστημα

Ρήτρα 2.1: *Όπου αυτή η ρήτρα επικυρώνεται σε πολιτικές που καλύπτουν τους κινδύνους πολέμου, εμφυλίου πολέμου, επανάστασης, εξέγερσης, εξέγερσης ή εμφύλιων συγκρούσεων που προκύπτουν από αυτές, ή οποιασδήποτε εχθρικής πράξης από ή εναντίον μιας αγωνιστικής εξουσίας ή τρομοκρατίας ή οποιουδήποτε προσώπου που ενεργεί από πολιτικό κίνητρο, η ρήτρα 1.1 δεν θα λειτουργήσει για να αποκλείσει τις απώλειες (οι οποίες διαφορετικά θα καλύπτονταν) που προκύπτουν από τη χρήση οποιουδήποτε υπολογιστή, υπολογιστή ή προγράμματος ηλεκτρονικού υπολογιστή ή οποιουδήποτε άλλου ηλεκτρονικού συστήματος στο σύστημα εκτόξευσης ή/και καθοδήγησης ή/και μηχανισμού πυροδότησης οποιουδήποτε όπλου ή πυραύλου."* (Institute Cyber Attack Exclusion Clause – CL. 380, 2003).

<u>Ασφαλιστική:</u>

Ανάλυση ενός συστήματος υπολογιστών: Γίνεται ανάλυση απώλειας ή ζημίας (συμπεριλαμβανομένης της επακόλουθης απώλειας και διακοπής της επιχείρησης). Θα καλύπτονται δηλαδή, φυσικές ζημιές σε απτά περιουσιακά στοιχεία. Από την άλλη «ως μέσο πρόκλησης βλάβης» θα μπορούσε να είναι αυτή η απώλεια, ζημία ή ευθύνη η οποία θα αποκλειόταν από την κάλυψη. Μερικοί ασφαλιστές ενδέχεται να προσφέρουν επεκτάσεις του εγκλήματος στον κυβερνοχώρο σε υφιστάμενες θαλάσσιες ασφαλιστικές συμβάσεις, αλλά πολλές από αυτές παρέχουν ανεπαρκή προστασία. Μια αυτοδύναμη πολιτική ασφάλισης στον κυβερνοχώρο μπορεί να προσφέρει πρόσθετη προστασία.

<u>P&I:</u>

Σύμφωνα με τους συνήθεις κανόνες του P&I, δεν υπάρχει συγκεκριμένος αποκλεισμός από τους κινδύνους του κυβερνοχώρου. Η κανονική κάλυψη του P&I θα εξακολουθήσει να ανταποκρίνεται στις υποχρεώσεις του P&I που προκύπτουν από επιθέσεις στον κυβερνοχώρο που υπόκεινται στους κανόνες των συλλόγων (BIMCO, 2018).

Εξαιρέσεις:

1. οι κίνδυνοι στον κυβερνοχώρο που σχετίζονται με τις συναλλαγές χωρίς χαρτί (ηλεκτρονικές συναλλαγές) καθώς τα συστήματα ηλεκτρονικής διαπραγμάτευσης θα μπορούσαν να είναι ευάλωτα στις επιθέσεις στον κυβερνοχώρο.
2. Όσον αφορά τις υποχρεώσεις του P & I, τα έξοδα ή τις δαπάνες που προκύπτουν από τους κινδύνους πολέμου.
3. Εξαιρούνται οι απώλειες που προκαλούνται από επιθέσεις στον κυβερνοχώρο εάν το πλοίο ή το φορτίο του, χρησιμοποιήθηκε για να προκαλέσει βλάβη, ή ένα πρόγραμμα υπολογιστή, συστήματος ή λογισμικού χρησιμοποιείται για την εκτόξευση, καθοδήγηση ή πυροδότηση ενός όπλου ή ενός πυραύλου.
4. Μια ακόμη εξαίρεση είναι οι κίνδυνοι πολέμου που σχετίζονται με τους ιούς των υπολογιστών. Μια κυβερνητική επίθεση εκ μέρους προσώπων ή οντοτήτων για πολιτικά, κοινωνικά ή θρησκευτικά κίνητρα, μπορεί να θεωρηθεί ως κίνδυνος για πόλεμο και συνεπώς ανάλογα την περίσταση μπορεί να καλύπτεται με ασφάλεια κινδύνου πολέμου.

Κάλυψη P&I: Δημιουργήθηκε μια ειδική συγκέντρωση χρημάτων με το όριο των 30 εκατομμυρίων δολαρίων ΗΠΑ ανά πλοίο συνολικά. Αυτό συμπεριλαμβάνει:

- Μια συμπληρωματική κάλυψη βάσει της ρήτρας για τη συμπερίληψη βιολογικών χημικών κινδύνων 2015
- Την ευθύνη των P&I και των μελών τους να καταβάλουν αποζημίωση ή έξοδα σωματικής βλάβης ή ασθένειας ή θανάτου οποιουδήποτε ναυτικού, καθώς και για τα δικαστικά έξοδα (συμπεριλαμβανομένων των εξόδων απόκλισης, επαναπατρισμού και αναπλήρωσης και αποζημίωσης ανεργίας για ναυάγια) που προέρχονται από κακόβουλη χρήση λογισμικού, κώδικα ή ιούς.

  (BIMCO, 2018).

Σημειώστε ότι οι απώλειες αυτές εξαιρούνται εάν το πλοίο ή το φορτίο του χρησιμοποιείται για να προκαλέσει βλάβη (BIMCO, 2018).

Στην αγορά υπάρχουν ανεξάρτητες ασφαλιστικές καλύψεις στον κυβερνοχώρο. Οι διαφορές στη φύση των ασφαλιστηρίων συμβολαίων στον κυβερνοχώρο είναι σημαντικές (BIMCO, 2018).

Ασφάλιση Αστικής Ευθύνης στον κυβερνοχώρο: Παρέχει οικονομική προστασία για κινδύνους που σχετίζονται με την πληροφορία και την τεχνολογία π.χ. Κίνδυνο διαταραχής

του διαδικτύου, Επιχειρηματική διακοπή και έξοδα, Κίνδυνοι φήμης, Αμυντικά έξοδα και αξιώσεις αποζημίωσης, Συναλλαγές ηλεκτρονικού εμπορίου, Κλοπή ηλεκτρονικών δεδομένων, απάντηση περιστατικού. Επίσης, νέοι συναφείς κίνδυνοι είναι ο κίνδυνος συσσώρευσης όπου με έναν ιό έχουμε πολλαπλά χτυπήματα και ο εκβιασμός στον κυβερνοχώρο όπου μια απειλή χρησιμοποιείται για επίθεση ή διαταραχή ενός συστήματος υπολογιστών με σκοπό της απαίτησης ενός αντικειμένου, συνήθως χρήματα (λύτρα) (BIMCO, 2018).

Έλεγχος για μια πολιτική ασφάλισης του κυβερνοχώρο η οποία θα είναι συμβατή με GDPR. Οι υπάρχουσες πολιτικές ασφάλισης στον κυβερνοχώρο ή στο σκάφος δεν καλύπτουν τον κίνδυνο εμπλοκής του συστήματος πλοήγησης ή της φυσική ζημιάς του πλοίου που προκαλείται από επίθεση κατά της πειρατείας (BIMCO, 2018).

Παρόλα αυτά η ασφαλιστική αγορά έχει ανάγκη από μεγαλύτερη εμπειρογνωμοσύνη για την κατανόηση και την αξιολόγηση των κινδύνων στον κυβερνοχώρο, υπάρχει έλλειψη των δεδομένων απαιτήσεων και επικρατεί μεταβλητότητα των τιμών

Οι ιδιοκτήτες θα πρέπει να εξετάσουν κάποιους παράγοντες και να δείξουν τη δέουσα επιμέλεια έτσι ώστε να είναι καλυμμένοι ασφαλιστικά σχετικά με την ασφάλεια στον κυβερνοχώρο (BIMCO, 2018).

Τι πρέπει να εξετάσουν οι ιδιοκτήτες ώστε να καλύπτονται ασφαλιστικά και όχι μόνο (MARSH, 2014):

1. Να Προσδιορίσουν και να αξιολογήσουν τους κινδύνους τους
- Καθιέρωση εσωτερικών διαδικασιών ασφάλειας στον κυβερνοχώρο για την προστασία από επιθέσεις κωδικού πρόσβασης, αποσυνδέσεις και αποτυχία επικοινωνίας καθώς και προστασία δεδομένων.
- Σχέδιο Διαχείρισης Κινδύνου Cyber Security.
- Καθιέρωση σχεδίου ανταπόκρισης.
2. Να Προσδιορίσουν τους ανθρώπους που μπορούν να βοηθήσουν εκ των προτέρων.
3. Να γίνει μια τεχνική αξιολόγηση του συστήματος πληροφορικής.
- Να συμπεριλάβουν προμηθευτές, τρίτους και οποιουσδήποτε άλλους που μπορεί να έχουν πρόσβαση στο σύστημά τους.

- Μόλις εντοπιστεί κάτι από την ασφάλεια, πώς γίνεται ελαχιστοποίηση αυτού του κινδύνου και ποιές τεχνικές θα πρέπει να αναπτυχθούν ώστε να μειωθούν οι επιπτώσεις.
- Πρέπει να εντατικοποιηθεί ο μετριασμός του κινδύνου.
- Εκπαίδευση ευαισθητοποίησης του προσωπικού για την ασφάλεια στον κυβερνοχώρο
- Θα πρέπει να γνωρίζουν την ασφαλιστική τους κάλυψη και να προσέχουν για συγκεκριμένους αποκλεισμούς στις πολιτικές για επιθέσεις στον κυβερνοχώρο.
- Θα πρέπει να εξετάσουν εάν χρειάζεστε μια ξεχωριστή πολιτική ασφάλισης στον κυβερνοχώρο.

Σε γενικά πλαίσια αν ακολουθούν τον οδηγό της BIMCO για Cyber security είναι κατά 99% καλυμμένοι.

2.9 Νηογνώμονες

Οι νηογνώμονες παίζουν πολύ σημαντικό ρόλο στην καθοδήγηση των ναυτιλιακών εταιρειών σχετικά με το Cyber security. Εκτός από οργανισμοί ελέγχου και πιστοποίησης των ναυτιλιακών εταιρειών, παίζουν πλέον και ρόλο συμβουλευτικό επειδή κατέχουν εξειδικευμένα άτομα με γνώσεις για το συγκεκριμένο θέμα. Παρακάτω παρουσιάζονται μερικοί από αυτούς και συγκρίνονται ώστε να δούμε τα κριτήρια επιλογής ενός νηογνώμονα.

2.9.1 DNVGL

Ο DNVGL είναι ο Νορβηγικός και ο Γερμανικός νηογνώμονας και οι υπηρεσίες που προσφέρει είναι (“Cyber Security Management Plan” DNVGL Confidential document):

- **Συνιστώμενη πρακτική σχετικά με την διαχείριση της ανθεκτικότητας στον κυβερνοχώρο.** Αυτή η πρακτική μπορεί να βρεθεί στον διαδικτυακό τόπο της εταιρείας και παρέχεται δωρεάν. Αυτό βοηθάει στην αξιολόγηση, βελτίωση και επαλήθευση της ανθεκτικότητας του ενεργητικού των εταιρειών και του προσωπικού τους στον κυβερνοχώρο.
- **Αξιολόγηση ασφάλειας στον κυβερνοχώρο**: Πραγματοποιείται από τις υψηλά καταρτισμένες ομάδες του οργανισμού σε συνεργασία με τα πληρώματα και τους υπαλλήλους στα γραφεία της εταιρείας έτσι ώστε να αναγνωριστούν τα κενά στις

άμυνες της εταιρείας και στα αντίμετρα, τόσο προληπτικά όσο και αντιδραστικά, στα συστήματα πληροφορικής και τα συστήματα λειτουργίας. Στόχος είναι η βοήθεια ώστε να δημιουργηθεί και να διατηρηθεί ένα αποτελεσματικό και οικονομικά αποδοτικό σύστημα ασφάλειας στον κυβερνοχώρο της κάθε εταιρείας.

- **Βελτίωση ασφάλειας στον κυβερνοχώρο:** Αυτό επιτυγχάνεται χρησιμοποιώντας συστηματικές μεθόδους αξιολόγησης, ώστε να κλείνουν αποτελεσματικά τα χάσματα στον κυβερνοχώρο και να υποστηρίζεται η ανάπτυξη σχεδίων βελτίωσης που αφορούν τα συστήματα, τον ανθρώπινο παράγοντα και τις διαδικασίες διαχείρισης.
- **Εκπαίδευση:** Παροχή προγραμμάτων εκπαίδευσης τα οποία καλύπτουν, απειλές, περιστατικά, κανονισμούς και μαθήματα πρόληψης απειλών. Τα προγράμματα εκπαίδευσης περιλαμβάνουν και ηλεκτρονική μάθηση εξ αποστάσεως η οποία μπορεί να πραγματοποιηθεί στο σκάφος ή στο γραφείο, έτσι ώστε τα πληρώματα να μπορούν να αντιμετωπίσουν τις βασικές πτυχές οποιουδήποτε συστήματος ασφαλείας στον κυβερνοχώρο καλύπτοντας με αυτόν τον τρόπο, τον ανθρώπινο παράγοντα.
- **Δοκιμές κοινωνικής μηχανικής**: Πραγματοποίηση μέτρησης επιπέδου ευαισθητοποίησης του προσωπικού σε σχέση με την ασφάλεια στον κυβερνοχώρο. Αυτό γίνεται με μετρήσεις από τις δοκιμές διείσδυσης χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής και phishing.
- **EU GDPR:** Βοήθεια συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ (GDPR) μέσω έργων χάσματος και βελτίωσης.
- **Εκπαιδευτικές δοκιμές αντιμετώπισης περιστατικών:** Εκτελούνται ασκήσεις για την εκπαίδευση και την επαλήθευση της απόκρισης στον κυβερνοχώρο τόσο στα πλοία όσο και στο γραφείο μιας εταιρείας. Αυτό συμβαίνει για να είναι προετοιμασμένοι για το χειρότερο,
- **Δοκιμή διείσδυσης - Penetration testing:** Δοκιμή της ανθεκτικότητας των φραγμών των συστημάτων μιας εταιρείας ώστε να μπορεί να διασφαλίσει τα περιουσιακά της στοιχεία και να τα καθιστά ασφαλή. Οι έλεγχοι διείσδυσης προσφέρουν πλήρη και αποτελεσματική επικύρωση των συστημάτων και των διαδικασιών τους.
- **Επαλήθευση - Verification:** Παροχή ελέγχου από τρίτους των απαιτήσεων ασφάλειας στον κυβερνοχώρο καθ’ όλη τη διάρκεια ζωής ενός νεόδμητου πλοίου και στα πλοία που είναι ήδη σε λειτουργία.

- **Πιστοποίηση - certification:** Η DNV GL πιστοποιεί σύμφωνα με το ISO / IEC 27001 (η πιστοποίηση θα περιορίσει τη δυνατότητα παροχής συμβουλευτικών υπηρεσιών).
- **Έγκριση τύπου – Type Aproval:** Προσφέρει ένα πρόγραμμα έγκρισης τύπου για ασφάλεια στον κυβερνοχώρο έτσι ώστε να γίνεται επαλήθευση των εξαρτημάτων που εφαρμόζονται σε πλοία.

2.9.2 ABS

Ο ABS είναι ο αμερικάνικος νηογνώμονας του οποίου το πρόγραμμα σχετικά με την ασφάλεια στον κυβερνοχώρο είναι μια συγκεκριμένη ναυτιλιακή προσέγγιση για τον εντοπισμό και την αντιμετώπιση του κυβερνο-επιχειρησιακού κινδύνου για θαλάσσια και υπεράκτια περιουσιακά στοιχεία και στόλους (CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES- ABS)

<u>ΠΩΣ ΔΟΥΛΕΥΕΙ</u>

Εξίσωση Cyber Risk FCI (Function –Connection –Identity) (Cyber security Advanced Solution – ABS).

- Λειτουργία (Function): Λογισμικό που ελέγχει μηχανές σε περιουσιακά στοιχεία.
- Σύνδεση (Connection). Φύση και αριθμός ψηφιακών διεπαφών που υποδεικνύουν την πολυπλοκότητα της ασφάλειας στον κυβερνοχώρο.
- Ταυτότητα (Identity). Άνθρωποι ή μηχανήματα που στέλνουν ή λαμβάνουν δεδομένα μέσω ψηφιακών διεπαφών.

Υπολογιστής Δείκτη Κινδύνου (Risk Index Calculator)

- Μεθοδολογία θαλάσσιου ειδικού κινδύνου.
- Μέτρηση και υπολογισμός.
- Με δυνατότητα επέκτασης σε περιουσιακά στοιχεία και πλοία

<u>ΥΠΗΡΕΣΙΕΣ</u>

- Αξιολόγηση ασφάλειας στον κυβερνοχώρο (Cyber Security assessment)
- Κατάρτιση ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο (Cyber Security Awareness Training)

- Γραφείο διαχείρισης κυβερνοασφάλειας (OT Cyber Management Office).
- Έλεγχος εγγράφων συστήματος (Controls System Documents)
- Αντιμετώπιση περιστατικών (Cyber Incident Response)
- Διαχείριση αλλαγών (Management of Change)
- Πρόγραμμα Standup (επαναφορά συστήματος)

2.9.3 BUREAU VERITAS – BV

Ο Bureau Veritas είναι ο γαλλικός νηογνώμονας και παρέχει υποστήριξη σε προγραμματιστές, κατασκευαστές και υπεύθυνους λήψης αποφάσεων που στοχεύουν σε προϊόντα πιο ασφαλή και αποδοτικά καθ ‘όλη τη διάρκεια του κύκλου ζωής τους, από το σχεδιασμό έως τη λειτουργία (CYBER SECURITY SOLUTIONS FOR INDUSTRY – BUREAU VERITAS).

Με τον Bureau Veritas ως πάροχο λύσεων που απευθύνεται στο σύστημα, μπορούν να επωφεληθούν το υλικό του συστήματος, το λογισμικό, η παρτίδα, οι άνθρωποι και η διαδικασία. Όποια και αν είναι η ανάγκη της εταιρείας και ο βαθμός ωριμότητάς της στον κυβερνοχώρο, παρέχεται βοήθεια σχετικά με τον χειρισμό των παρακάτω πτυχών (CYBER SECURITY SOLUTIONS FOR INDUSTRY – BUREAU VERITAS):

- **Αξιολόγηση της συμμόρφωσης στον κυβερνοχώρο**
  διάγνωση, ανάλυση απειλών & αξιολόγηση κινδύνων
- **Υπηρεσίες πιστοποίησης σύμφωνα με τα πρότυπα**
  ISO 27001 IEC 62443, CYBER ESSENTIALS
- **Υπηρεσίες πιστοποίησης σύμφωνα με τις κατευθυντήριες γραμμές του Bureau Veritas**
  [BV-sW-200, BV-CAR CYBERSEC]
- **έλεγχοι επιτήρησης**
- **Δοκιμές κατά γνωστών ευπαθειών**
  (CVE, CWE)
- **Εταιρική υποστήριξη συμβουλευτικών υπηρεσιών για Cybersecurity**
  Πλαίσιο αφοσιωμένης υποστήριξης, στρατηγική για ασφάλεια στον κυβερνοχώρο, ασφάλεια από τον σχεδιασμό, προσόντα και παρακολούθηση.
- **Εκπαίδευση και ευαισθητοποίηση**
  Σχετικά με τις απαιτήσεις του IEC 62443 και άλλα πρότυπα.

2.9.4 LR

Ο LR είναι ο αγγλικός νηογνώμονας και συγκεκριμένα με το θέμα της κυβερνοασφάλειας, δημιούργησε μια αποδοτική προσέγγιση όσον αφορά την αξιολόγηση της συμμόρφωσης με τις κατευθυντήριες γραμμές BIMCO, οι οποίες βασίζονται σε μεγάλο βαθμό στην Εθνικό πλαίσιο για τα πρότυπα και την τεχνολογία (NIST). Η αξιολόγηση των απειλών Cyber Security είναι το πρώτο βήμα που συνιστά η BIMCO και η NIST κατά την προσέγγιση της θέσης του κυβερνητικού συστήματος ναυτικής οργάνωσης και χάρη στην πρόσφατη εξαγορά της Nettitude, είμαστε σε θέση να προσφέρουμε ένα ολοκληρωμένο πλαίσιο για την αξιολόγηση απειλών και τη διαχείριση κινδύνου τόσο διαχείριση στόλου γραφείων όσο και πλοία (https://www.lr.org/en/bimco-guidelines/).

Τι προσφέρει:

- **Υπηρεσίες πληροφοριών απειλής - Threat Intelligence Services**

Η αξιολόγηση απειλών και η μοντελοποίηση απειλών αποτελούν ζωτικά εργαλεία για την παροχή συναφών και αποτελεσματικών δραστηριοτήτων ασφάλειας σε ένα σύστημα. Όπως τονίζεται στο πλαίσιο BIMCO, μέχρι να γνωστοποιείται το από πού προέρχονται οι απειλές και τι τρωτά σημεία ή αδυναμίες υπάρχουν, δεν είναι γνωστό που να εφαρμόζονται οι έλεγχοι. Μπορεί να υποστηριχθεί η κατανόηση όλων αυτών των πληροφοριών σε ρεαλιστικά εργαστήρια και μπορεί επίσης να βοηθήσει στην εφαρμογή μιας ενεργού και σχετικής μεθοδολογίας κινδύνου σύμφωνα με τις απαιτήσεις της BIMCO (https://www.lr.org/en/bimco-guidelines/).

- **Αξιολόγηση κινδύνου- Risk Assesment**

παρέχουν στους έμπειρους ανώτερους συμβούλους ασφαλείας πληροφοριών στο χώρο της εταιρείας, για να αυξήσουν την κατανόηση και το προφίλ του κινδύνου γύρω από τα δεδομένα και τα συστήματα, αξιολογώντας τη στάση ασφαλείας των ναυτιλιακών οργανισμών για να καθορίσουν μια κατάλληλη στρατηγική και ένα σχέδιο δράσης για βελτίωση (https://www.lr.org/en/cyber-security/).

- **Έλεγχος διαδικασιών ασφάλειας Cyber**

αναλαμβάνουν έναν έλεγχο διαδικασιών ασφαλείας στον κυβερνοχώρο που βασίζεται σε υψηλή ποιότητα. Ο έλεγχος θα διεξάγεται από έναν ελεγκτή με πιστοποίηση ISO 27001 και το αντικείμενο του ελέγχου θα συμφωνηθεί μεταξύ ελεγκτή και εταιρείας και θα βασίζεται σε

μια επιλογή από συμφωνημένους ελέγχους, σε αντίθεση με κάθε έλεγχο. Αυτό θα διασφαλίσει ότι ο έλεγχος ολοκληρώνεται σε σχετικά σύντομο χρονικό διάστημα (https://www.lr.org/en/cyber-security/).

- **Έλεγχος επί του σκάφους – on board audit**

Ο κύριος στόχος του επιτόπιου ελέγχου είναι να προσδιοριστεί η συμμόρφωση του πλοίου με τις κατευθυντήριες γραμμές του BIMCO και να καθοριστεί η αποτελεσματικότητα των μέτρων ασφαλείας, των πολιτικών, των διαδικασιών και της ετοιμότητας για τα περιστατικά που σχετίζονται με τον κυβερνοχώρο. Ως αποτέλεσμα αυτής της δραστηριότητας, παρέχει πλήρη έκθεση των ευρημάτων με συστάσεις / χάρτες πορείας για βελτίωση και συμμόρφωση με το επιλεγμένο επίπεδο συμμόρφωσης BIMCO (https://www.lr.org/en/cyber-security/).

- **Αξιολόγηση ευπάθειας ή δοκιμή διείσδυσης- Vulnerability assessment or Penetration Testing**

Η αξιολόγηση ευπάθειας μπορεί να παρασχεθεί σε υπολογιστικά συστήματα (πλοήγηση, έλεγχος φορτίου, διαχείριση ισχύος, επικοινωνία κ.λπ.), δίκτυα πλοίων και οποιαδήποτε αυτοματοποίηση στο επιλεγμένο σκάφος. Εάν προσδιοριστεί κάποιος συγκεκριμένος στόχος, μπορεί επίσης να εκτελεστεί δοκιμή διείσδυσης. Η δοκιμή διείσδυσης είναι η προσπάθεια να εκμεταλλευτούν ενεργά τις αδυναμίες στο περιβάλλον από την πλευρά ενός εισβολέα με άμεση πρόσβαση στο δοκιμαζόμενο δίκτυο (https://www.lr.org/en/cyber-security/.

ΣΥΜΠΕΡΑΣΜΑ:

Από την παραπάνω παρουσίαση μερικών νηογνωμόνων προκύπτει ότι οι υπηρεσίες που προσφέρουν στις ναυτιλιακές εταιρείες για τη ασφάλεια των πληροφοριών των πληροφοριών τους είναι ίδιες και αυτό συμβαίνει επειδή ακολουθούν τους κανονισμούς. Ενδεχομένως να αλλάζουν οι χρεώσεις καθώς και ο τρόπος που ενεργούν απέναντι στα θέματα ασφάλειας των ναυτιλιακών εταιρειών. Ωστόσο, πέρα από την ελεγκτική πλευρά που έχουν οι νηογνώμονες, επιβεβαιώνεται η συμβουλευτική πλέον φύση αυτών των εταιρειών απέναντι στις ναυτιλιακές εταιρείες.

2.10 Cyber Security σε μια ναυτιλιακή εταιρεία

Το Cyber Security σε μια ναυτιλιακή χωρίζεται σε δύο κατηγορίες οι οποίες όμως αλληλοσυνδέονται. Το Cyber Security για την εταιρεία και για τα πλοία της. Έτσι λοιπόν μια ναυτιλιακή εταιρεία θα πρέπει να έχει δύο διαφορετικούς οδηγούς οι οποίοι αφορούν την ασφάλεια στον κυβερνοχώρο της και να είναι διαθέσιμοι σε όλους της τους υπαλλήλους. Παρακάτω, κατασκευάστηκαν δύο οδηγοί οι οποίοι αφορούν γραφείο και πλοίο και λειτουργούν σαν εσωτερικές διαδικασίες της εταιρείας οι οποίες βασίζονται στα guidelines καθώς και στους απαιτούμενους κανονισμούς (BIMCO, 2018), (Kenneth J. Knapp, 2009).

2.10.1 Οδηγός Cyber Security εταιρείας

Μια ναυτιλιακή εταιρεία εφαρμόζει κάποιες διαδικασίες οι οποίες λειτουργούν ως οδηγός και είναι διαθέσιμος προς όλους τους εργαζομένους, ώστε να προστατεύει τα δεδομένα και τα συστήματά της από οποιαδήποτε επίθεση στον κυβερνοχώρο (Yong-Chan Lee, Sang-Kyum Park, Woo-Kun Lee, Jun Kang, 2017). Αυτός ο οδηγός περιλαμβάνει:

- **Ορισμούς:** Θεωρείται απαραίτητο κομμάτι έτσι ώστε οι εργαζόμενοι να κατανοήσουν τη σημασία της ασφάλειας του κυβερνοχώρου για την εταιρεία και τους κινδύνους που έρχονται αντιμέτωποι.
- **Έλεγχος πρόσβασης:** Αυτό καθορίζει τα δικαιώματα των χρηστών και την πρόσβασή τους στο σύστημα. Για παράδειγμα, άλλα δικαιώματα πρόσβασης έχουν οι διαχειριστές συστήματος και άλλα δικαιώματα έχουν οι υπάλληλοι πρακτικής άσκησης (Huge Boyes, 2014). Η πρόσβαση καθορίζεται από τα καθήκοντα που πρόκειται να εκτελέσει ο κάθε υπάλληλος ανάλογα με τη θέση του στην εταιρεία. Επίσης, η πρόσβαση των προμηθευτών στην εταιρεία καθορίζεται έτσι ώστε να μην απειλείται το σύστημα ασφάλειας της εταιρείας και δίνεται πρόσβαση σε συγκεκριμένα σημεία που αφορούν τις ανάγκες που έχει η εταιρεία τον συγκεκριμένο προμηθευτή (Kimberly Tam, Kevin Jones, 2019). Αυτό πραγματοποιείται ζητώντας πρόσβαση από τον υπεύθυνο ασφάλειας της εταιρείας έτσι ώστε να είναι ενημερωμένο το σύστημα για τις άδειες πρόσβασης από εξωτερικούς προμηθευτές ανά πάσα στιγμή. Η άδεια αυτή θα πρέπει να έχει συγκεκριμένη χρονική διάρκεια η οποία μετά το πέρας της θα πρέπει να καταργείται (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts, 2017).
- **Προστασία από κακόβουλο λογισμικό (malware):** Αυτό συνεπάγεται την αξιολόγηση του λογισμικού πριν την εγκατάσταση στο σύστημα (Kimberly Tam, Kevin Jones, Maria Papadaki, 2012). Έπειτα την εγκατάσταση και τη διαμόρφωση

ώστε να ενημερώνεται αυτόματα μέσω διαδικτύου. Επίσης θα πρέπει να γίνει διαμόρφωση των ρυθμίσεων του υπολογιστή. Αυτό περιλαμβάνει την απενεργοποίηση της αυτόματης εκτέλεσης USB και ότι μόνο εξουσιοδοτημένα USB μπορούν να συνδεθούν στο δίκτυο, αποκλεισμός περιήγησης σε μη ασφαλής σελίδες, την απενεργοποίηση αναδυόμενων παραθύρων και την απενεργοποίηση μακροεντολών του EXCEL. Επίσης, θα πρέπει να γίνεται καταχώρηση των εταιρικών τηλεφώνων και υπολογιστών για κρυπτογράφηση και συμμόρφωση με τις απαιτήσεις ασφαλείας του συστήματος και δεν θα πρέπει να επιτρέπεται η εγκατάσταση άγνωστου λογισμικού από τους απλούς χρήστες σε εταιρικούς υπολογιστές πριν από τον έλεγχο και την άδεια του IT τμήματος της εταιρείας. Τέλος, θα πρέπει να γίνεται επέκταση του κεντρικού λειτουργικού συστήματος σε διακομιστές και υπολογιστές (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts, 2017).

- **Καταγραφή και Παρακολούθηση:** Τα συστήματα ICT (Information and Communication Technologies) της εταιρείας θα πρέπει να παρακολουθούνται ώστε να διασφαλίζουν την ταυτοποίηση των απειλών. Η καταγραφή και παρακολούθηση πραγματοποιείται στα συστήματα Firewall, στα συστήματα ανίχνευσης και πρόληψης εισβολών, σε πύλες άλλων δικτύων, server, σε φορητούς υπολογιστές και κινητά τηλέφωνα. Θα πρέπει να υπάρχει αυτόματη ειδοποίηση ώστε να παρέχεται άμεση αντίδραση σε οποιαδήποτε απειλή. Για τα αρχεία προσωπικών δεδομένων, θα πρέπει να λαμβάνεται υπόψη η νομοθεσία (2472/1997, GDPR). Τέλος, οι διαχειριστές του συστήματος απαγορεύεται να διαγράψουν ή να απενεργοποιήσουν τους μηχανισμούς καταγραφής για τους δικούς τους λογαριασμούς (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012).
- **Ασφάλεια κωδικού πρόσβασης:** Περιλαμβάνει τους κανόνες δημιουργίας όπως το ελάχιστο μήκος του κωδικού πρόσβασης, να αποτελείται από κεφαλαία και πεζά γράμματα καθώς και αριθμητικούς χαρακτήρες και σύμβολα. Επίσης δεν θα πρέπει να περιλαμβάνεται το όνομα χρήστη στον κωδικό πρόσβασης και να μην επαναλαμβάνονται οι προηγούμενοι κωδικοί. Αυτό γίνεται μέσω μια διαδικασίας ελέγχου του συστήματος η οποία δεν επιτρέπει στον χρήστη την δημιουργία ενός κωδικού που περιλαμβάνει τα παραπάνω. Η αλλαγή του κωδικού θα πρέπει να πραγματοποιείται εντός ορισμένου χρονικού πλαισίου και όχι σε μικρότερο διάστημα από μία μέρα για παράδειγμα της ζωής του κωδικού. Ο χρήστης θα πρέπει να κρατάει

μυστικό τον κωδικό του, να μην τον αποθηκεύει αυτόματα στο σύστημα του υπολογιστή του και μόνο το IT τμήμα επιτρέπεται να γνωρίζει τον κωδικό του (Huge Boyes, 2014).

- **Ασφάλεια επικοινωνιών και δικτύων:** Σε αυτό το στάδιο γίνεται σχεδιασμός ασφάλειας δικτύων αναγνωρίζοντας τις πιθανές απειλές, το επίπεδο εμπιστοσύνης μεταξύ συστήματος και δικτύων που πρόκειται να συνδεθούν στο σύστημα, η διαθεσιμότητα του συστήματος καθώς και η γεωγραφική απόσταση και η μελλοντική εξάπλωση. Επίσης, χρησιμοποιούνται συστήματα εντοπισμού και πρόληψης εισβολών στο σύστημα για την κεντρική διαχείριση και παρακολούθηση των δικτύων καθώς και εικονικά δίκτυα VLAN. Χρησιμοποιείται ισχυρή κρυπτογράφηση έτσι ώστε να διασφαλιστεί η εμπιστευτικότητα των δεδομένων που μεταδίδονται μέσω κάποιου δημόσιου δικτύου. Το δίκτυο υποδομών της επιχείρησης χωρίζεται σε πολλά εικονικά δίκτυα ανάλογα με τις ανάγκες και της απαιτήσεις του σχεδιασμού ασφαλείας. Τα συστήματα όπως φυσικής ασφάλειας, τηλεφωνικό κέντρο και λειτουργικά όπως κλιματισμός, συνδέονται αποκλειστικά σε VLAN χωρίς τη δυνατότητα πρόσβασης στο κύριο δίκτυο του συστήματος. Στο δίκτυο WiFi μπορούν να συνδέονται φορητοί υπολογιστές και εταιρικά κινητά, προσωπικές συσκευές καθώς και μπορεί να υπάρχει και σύνδεση στο ιντερνέτ από επισκέπτες. Τέλος, η φυσική ασφάλεια η οποία αφορά τον εξοπλισμό δικτύου προτείνεται να προστατεύεται με την τοποθέτηση σε κατάλληλα διαμορφωμένα ράφια ή σε άξονες δικτύου και να έχουν πρόσβαση μόνο εξουσιοδοτημένα άτομα σε αυτά (Kimberly Tam, Kevin Jones, Maria Papadaki, 2012).
- **Δημιουργία αντιγράφων ασφαλείας:** Θα πρέπει να δημιουργούνται αντίγραφα ασφαλείας κυρίως για τα κρίσιμα αρχεία τα οποία αφορούν τις ρυθμίσεις του συστήματος καθώς και στους εταιρικούς υπολογιστές όλα τα αρχεία που είναι αποθηκευμένα στον φάκελο «τα έγγραφα μου» των χρηστών. Όλα αυτά τα δεδομένα θα πρέπει να κρυπτογραφούνται και να διατηρούνται στο σύστημα. Αυτή η διαδικασία πραγματοποιείται μέσω κάποιου μηχανισμού του συστήματος η οποία δημιουργεί αντίγραφα ασφαλείας αυτόματα και στη συνέχεια τα κρυπτογραφεί. Η περίοδος που πρέπει να διατηρούνται τα αντίγραφα αυτά ορίζεται συνήθως σε ένα χρόνο και έπειτα από το πέρας αυτού πραγματοποιείται καταστροφή σύμφωνα με το πρότυπο ISO 27001. Ειδικά αντίγραφα ασφαλείας δημιουργούνται μόνο κατά την

αναβάθμιση του συστήματος. Τέλος θα πρέπει να γίνεται δοκιμή και επαναφορά αντιγράφων ασφαλείας κάθε ορισμένο χρονικό διάστημα ώστε να δοκιμάζεται η ακεραιότητα και η πληρότητα του περιεχομένου τους (ISO 27001, Regulations) (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012).

- **Ασφάλεια φορητών συσκευών:** Θα πρέπει να εφαρμόζεται κρυπτογράφηση πλήρους δίσκου και οι συσκευές που δεν είναι κρυπτογραφημένες δεν θα πρέπει να χρησιμοποιούνται για επιχειρησιακούς σκοπούς. Εάν πραγματοποιηθεί απώλεια, ζημιά ή κλοπή της συσκευής θα πρέπει να αναφερθεί άμεσα στον υπεύθυνο ασφαλείας του τμήματος πληροφορικής. Για τη σύνδεση στις συσκευές απαιτείται PIN και δεν θα πρέπει να μοιράζονται με τα υπόλοιπα μέλη μιας οικογένειας. Θα πρέπει επίσης να συνδέονται σε ασφαλή δίκτυα. Οι φορητοί υπολογιστές θα πρέπει να ελέγχονται αυτόματα για μη συμμόρφωση μέσω των προτύπων ασφαλείας της εταιρείας, σε περίπτωση μη συμμόρφωσης απαγορεύεται αυτόματα η πρόσβαση σε δίκτυο της εταιρείας. Επίσης η οθόνη είναι ρυθμισμένη να κλειδώνει αυτόματα έπειτα από 15 λεπτά αδράνειας. Η πρόσβαση σε μη ασφαλής σελίδες είναι περιορισμένη και το λογισμικό προστασίας είναι προεγκατεστημένο σε όλους τους φορητούς υπολογιστές της εταιρείας (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012)
- **Περιορισμός πρόσβασης στο δίκτυο από τις προσωπικές φορητές συσκευές:** οι προσωπικές φορητές συσκευές όπως και οι συσκευές επισκεπτών στην εταιρεία έχουν δικαίωμα να συνδέονται μόνο στα ασύρματα δίκτυα της εταιρείας τα οποία αφορούν τους επισκέπτες. Μετά την απομάκρυνση από την εταιρεία η εταιρεία διατηρεί το δικαίωμα να διαγράφει απομακρυσμένα εταιρικά δεδομένα από συσκευές σε περίπτωση συμβάντος η τερματισμού της απασχόλησης (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012).
- **Τηλεργασία:** Η τηλεργασία αφορά τη δυνατότητα των υπαλλήλων της εταιρείας να εργάζονται από διαφορετικές περιοχές εκτός της εταιρείας. Γι αυτό το λόγο οι εργαζόμενοι που χρησιμοποιούν τέτοιου είδους συσκευές θα πρέπει να γνωρίζουν σχετικά με τους κινδύνους που αντιμετωπίζουν και να μην αφήνουν τις συσκευές τους ανοιχτές χωρίς επίβλεψη ώστε να αποφευχθεί η διαρροή δεδομένων. Επίσης στις συσκευές αυτές εφαρμόζονται πρόσθετα στοιχεία ασφαλείας όπως ακριβώς και στις

συσκευές κινητών τηλεφώνων. Επιπρόσθετα, όταν τερματίζεται κάποια σχέση εργασίας οι συσκευές επιστρέφονται στην εταιρεία και τα δεδομένα που εμπεριέχουν καταστρέφονται. Τέλος, δύναται να εφαρμοστεί έλεγχος των ιδιόκτητων συσκευών σχετικά με τις εταιρικές πληροφορίες (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012).

- **Ασφάλεια ηλεκτρονικού ταχυδρομείου:** Αυτό αφορά τους ιδιωτικούς λογαριασμούς των χρηστών της εταιρείας οι οποίοι είναι κατασκευασμένοι για να εξυπηρετούν επιχειρηματικούς σκοπούς και έχουν περιορισμένη πρόσβαση σε προσωπική επικοινωνία. Το σύστημα αποστολής και λήψης email επιτρέπει την την ανταλλαγή μηνυμάτων ορισμένου μεγέθους (π.χ. ως 30Mb). Οι υπάλληλοι είναι υπεύθυνοι προσωπικά για τη σωστή χρήση των λογαριασμών τους και θα πρέπει να συμβαδίζει σε σχέση με τις πολιτικές της εταιρείας οι οποίες αφορούν την ασφάλεια. η εταιρεία κατά κανόνα δεν έχει πρόσβαση στις επικοινωνίες μέσω ηλεκτρονικού ταχυδρομείου κατ εξαίρεση όμως όταν κριθεί απαραίτητο επειδή μπορεί κάτι να επηρεάσει την εταιρεία ως προς τα επίπεδα ασφάλειάς της η εταιρεία μπορεί να επέμβει με την παρακολούθηση των επικοινωνιών (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012).
- **Αποδεκτή χρήση μέσω διαδικτύου:** Είναι η πρόσβαση των χρηστών στο διαδίκτυο μέσω εγκεκριμένου από την εταιρεία εξοπλισμού. Η χρήση προσωπικών μόντεμ απαγορεύονται βάση πολιτικής της εταιρείας. Η εταιρία επίσης έχει περιορισμένη πρόσβαση σε διαδικτυακούς τόπους που θεωρεί επικίνδυνους, έχει δικαίωμα να αναθεωρεί περιεχόμενα σελίδων και απαγορεύει την είσοδο σε σελίδες που εμπεριέχουν ακατάλληλο περιεχόμενο. Ο χρήστης έχει αποκλειστική ευθύνη σχετικά με τις αγοροπωλησίες που πραγματοποιεί μέσω διαδικτύου και απηθηκεύει προσωπικά δεδομένα και κάρτες (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).
- **Χειρισμός αφαιρούμενων μέσων:** Απαγορεύεται η πρόσβαση από μη εξουσιοδοτημένες συσκευές στο σύστημα της εταιρείας. Η μεταφορά πληροφοριών από εξωτερικούς παράγοντες στην εταιρεία γίνεται μόνο μέσω ενός υπολογιστή ο οποίος είναι για επισκέπτες και δεν είναι συνδεδεμένος στο ιντερνέτ. Όλα τα εξωτερικά μέσα όπως κάμερες, USB και εξωτερικούς σκληρούς επιτρέπεται να συνδέονται στο σύστημα ύστερα από εξουσιοδότηση από το IT. Για οποιαδήποτε

προσπάθεια σύνδεσης από κάποια συσκευή πραγματοποιείται αυτόματη σάρωση. Θα πρέπει να διασφαλίζεται η κατάλληλη χρήση και η ασφάλεια των πληροφοριών σε εξωτερικές συσκευές αποθήκευσης καθώς και να διασφαλίζεται η αποθήκευση των συσκευών σε ασφαλές μέρος για την αποφυγή κλοπής και κατόπιν εισβολής στο σύστημα. Σε περίπτωση κλοπής η καταστροφής συσκευής οι εργαζόμενοι έχουν αποκλειστική ευθύνη και θα πρέπει να ενημερώνουν άμεσα τους υπεύθυνους (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).

- **Ευαισθητοποίηση και κατάρτιση:** Σε αυτό το στάδιο οι χρήστες του συστήματος θα πρέπει να γνωρίζουν τους βασικούς κανόνες σχετικά με τους κινδύνους για την ασφάλεια στον κυβερνοχώρο και την αδυναμία των τεχνικών ελέγχων να αποτρέψουν κάποια πιθανή επίθεση. Οι τακτικές που πρέπει να ακολουθούνται είναι:
    - Όχι απάντηση σε μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία σχετίζονται με οικονομικές συναλλαγές ή προσωπικές πληροφορίες εκτός εάν ο χρήστης γνωρίζει την πηγή.
    - Όχι άνοιγμα συνημμένων αρχείων ή συνδέσμων. Κατ εξαίρεση μόνο κατόπιν επιβεβαίωσης με τον αποστολέα.
    - Όχι παροχή κωδικών πρόσβασης με οποιοδήποτε τρόπο.
    - Όχι ενημέρωση λογισμικού χωρίς σχετική άδεια και απενεργοποίηση τοίχους προστασίας.

  Η εκπαίδευση σχετικά με την ασφάλεια στον κυβερνοχώρο είναι υποχρεωτική και εφαρμόζεται σε όλο το προσωπικό μέσω ηλεκτρονικής διδασκαλίας ή διδασκαλίας στην τάξη. Σε περιπτώσεις νεοεισερχόμενων στην εταιρεία η διαδικασία ολοκληρώνεται κατά την περίοδο προσαρμογής (Krzysztof Cabaj, Dulce Domingos, Zbigniew Kotulski, Ana Respico, 2018).
- **Διαχείριση Εγκατάστασης λογισμικού:** Όλα τα λογισμικά που χρησιμοποιεί η εταιρεία θα πρέπει να είναι αγορασμένα από την ίδια από το τμήμα IT και να γίνεται έλεγχος του προμηθευτεί αλλά και του τρόπου που δουλεύουν. Η εγκατάσταση του λογισμικού στην εταιρεία πραγματοποιείται μόνο από τον υπεύθυνο του τμήματος IT καθώς και τυχόν πληροφορίες παρέχονται από το συγκεκριμένο τμήμα. Επίσης θα πρέπει να βεβαιώνεται ότι ο πάροχος υπηρεσιών είναι εξουσιοδοτημένος και εκτελεί τη συντήρηση του λογισμικού (Kimberly Tam, Kevin Jones, 2019).

- **<u>Διαχείριση ευπάθειας:</u>** Οι σταθμοί εργασίας και οι διακομιστές που ανήκουν στην εταιρεία θα πρέπει να έχουν εγκατεστημένες τις ενημερώσεις ασφαλείας λειτουργικού συστήματος για την προστασία τους από τις γνωστές ευπάθειες. Η ευπάθεια θα πρέπει να συμμορφώνεται με τις ακόλουθες ελάχιστες βασικές απαιτήσεις για να εξασφαλιστεί η ασφάλεια του συστήματος και των δεδομένων του τα οποία βρίσκονται στο προεπιλεγμένο λειτουργικό σύστημα, service pack, επείγουσες επιδιορθώσεις και επίπεδο επιπέδου. Οι ενημερώσεις ασφαλείας θα πρέπει να δοκιμάζονται πριν από την εγκατάσταση από τους διαχειριστές του συστήματος. Οι διακομιστές και οι σταθμοί εργασίας ενημερώνονται περιοδικά μέσω κεντρικής πλατφόρμας (για παράδειγμα 3 μήνες για διακομιστές, 1 μήνα για σταθμούς εργασίας). Όταν απελευθερωθούν οι κρίσιμες ενημερώσεις, η ευπάθεια αναγνωρίζεται αμέσως (Kimberly Tam, Kevin Jones, 2019).
- **<u>Αξιολόγηση ευπάθειας:</u>** η εταιρεία θα πρέπει να διενεργεί εκτιμήσεις ευπάθειας όλων των περιουσιακών της στοιχείων και των πληροφοριών εντός της περιμέτρου του κτιρίου των γραφείων της (διακομιστές, σταθμοί εργασίας, δίκτυα, κτλ). Αυτό θα πρέπει να γίνεται σε κατάλληλη χρονική στιγμή ώστε να μη γίνει διακοπή κάποιας λειτουργίας. Τα αποτελέσματα θα πρέπει να αντιμετωπίζονται ως εμπιστευτικές πληροφορίες. Η σάρωση θα πραγματοποιείται μέσω ενός εργαλείου κεντρικά εγκατεστημένου το οποίο θα αποδίδει τιμές σοβαρότητας των ευπαθειών του συστήματος. Το IT τμήμα θα πρέπει να εξετάζει τα ευρήματα ανάλογα με τη σοβαρότητα που έχουν για το σύστημα για παράδειγμα τα κρίσιμα σημεία ευπάθειας θα πρέπει να αντιμετωπιστούν εντός ενός μηνός από την ανακάλυψή τους ενώ τα τρωτά σημεία υψηλής σοβαρότητας θα πρέπει να αντιμετωπιστούν μέσα σε 3 μήνες από την ανακάλυψή τους. Τέλος έπειτα από το διάστημα των τριών μηνών θα πρέπει να πραγματοποιηθεί νέα αξιολόγηση έτσι ώστε να διασφαλιστεί ότι τα σημεία κρίσιμης σοβαρότητας δεν απειλούν πια το σύστημα (Kimberly Tam, Kevin Jones, 2019).
- **<u>Διαχείριση προμηθευτών:</u>** Σε γενικές γραμμές η εταιρεία θα πρέπει να γνωρίζει πολύ καλά τους προμηθευτές της και να διαχειρίζεται πολύ σωστά αυτό το κομμάτι ώστε να αποφευχθεί οποιαδήποτε διείσδυση στο σύστημά της. Για το λόγο αυτό θα πρέπει να υπάρχει γραπτή σύμβαση μεταξύ εταιρείας- προμηθευτή όπου θα αναγράφονται όλες οι απαιτήσεις ασφαλείας της εταιρείας και θα πρέπει να τηρούνται από τον

προμηθευτή. Ο προμηθευτής θα πρέπει να συμφωνεί σε μη αποκάλυψη πληροφοριών της εταιρείας ώστε να διατηρείται η εμπιστευτικότητα μεταξύ πελάτη-προμηθευτή. Επίσης θα πρέπει να υπάρχει συμφωνία επεξεργασίας προσωπικών δεδομένων σε περιπτώσεις που χρειάζεται και θα πρέπει να βασίζεται στα πρότυπα που επιτάσσει η εκάστοτε νομοθεσία. Τέλος το σύστημα ποιότητας του προμηθευτή σχετικά με τις δραστηριότητες του κύκλου ζωής του λογισμικού κτλ θα πρέπει να εμπεριέχει τεκμηριωμένες διαδικασίες για την ασφάλεια στον κυβερνοχώρο (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts, 2017).

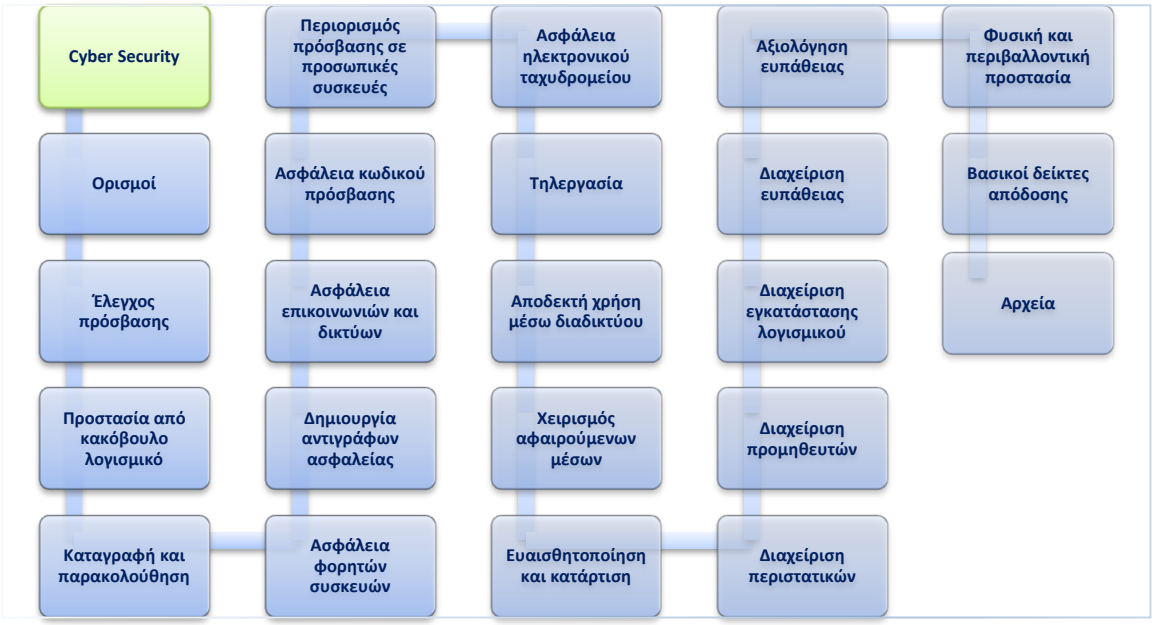
- **Διαχείριση περιστατικού:** Σε αυτή την περίπτωση, σε πρώτη φάση η εταιρεία θα πρέπει να έχει τη δυνατότητα να κατηγοριοποιήσει το περιστατικό. Τα περιστατικά κατηγοριοποιούνται ως εξής:
    1. Άρνηση παροχής υπηρεσίας.
    2. Κακόβουλος κώδικας.
    3. Μη εξουσιοδοτημένη πρόσβαση στο σύστημα.
    4. Ακατάλληλη χρήση από άτομο που δεν έχει τη γνώση στο σύστημα.

  Όλα τα παραπάνω κατηγοριοποιούνται σε σχέση με το πόσο επηρεάζουν την ακεραιότητα, την διαθεσιμότητα και την εμπιστευτικότητα του συστήματος (Kimberly Tam, Kevin Jones, 2019).

  Κάποια παραδείγματα περιστατικών είναι όταν μολύνεται το σύστημα από κάποιο κακόβουλο λογισμικό, βλάβες ή υπερφόρτωση υλικού ή λογισμικού, παραβίαση ψηφιακών δεδομένων, μη εξουσιοδοτημένη πρόσβαση σε κάποιο σταθμό εργασίας, διακομιστές κ.α., λήψη ανεπιθύμητων μηνυμάτων, κατεστραμμένα αρχεία ή τα αρχεία δεν λειτουργούν, κτλ. Στη συνέχεια θα πρέπει να τεθεί κατάσταση προτεραιότητας αντιμετώπισης περιστατικού σε σχέση με τον παγκόσμιο κύκλο κυβερνοασφάλειας. Τα κριτήρια αφορούν τον αντίκτυπο και το πόσο επείγον είναι το περιστατικό για την εταιρεία. Οι κύριες φάσεις χειρισμού των περιστατικών από την εταιρεία είναι:
    1. Προετοιμασία
    2. Ανίχνευση
    3. Ταξινόμηση
    4. Περιορισμός- εξάλειψη
    5. Ανάκτηση
    6. Δραστηριότητα μετά το συμβάν

- **<u>Φυσική και περιβαλλοντική προστασία:</u>** Αυτό συνεπάγεται ότι η εταιρεία αποτελείται από ασφαλείς περιοχές με πρόσβαση σε αυτή με τη χρήση χειριστηρίων εισόδου. Επίσης, μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση σε ασφαλείς περιοχές και αυτό ύστερα από έγκριση του υπεύθυνου ασφάλειας. Υπάρχει προστασία από περιβαλλοντικές απειλές και χρήση UPS σε περιπτώσεις διακοπής ρεύματος ώστε να αποφευχθεί η διαγραφή των αρχείων. Επιπρόσθετα, η είσοδος στην εταιρεία θα πρέπει να γίνεται βάση ελέγχου όπως επιβάλλει η πολιτική ελέγχου φυσικής πρόσβασης (Huge Boyes, 2014).
- **<u>Βασικοί δείκτες απόδοσης:</u>** είναι οι στόχοι KPIs. Γίνεται ανασκόπηση του συστήματος από τη διοίκηση της εταιρείας ώστε να αποφευχθούν επιθέσεις και να τεθεί το σύστημα αποδοτικό (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts , 2017).
- **<u>Αρχεία:</u>** Σχετικά με τα αρχεία θα πρέπει να ελέγχονται τα δικαιώματα πρόσβασης να εφαρμόζονται ετήσιοι έλεγχοι δικαιωμάτων πρόσβασης και τέλος να εφαρμόζεται δοκιμή δημιουργίας αντιγράφων ασφαλείας(BIMCO, 2018).

Στο παρακάτω σχήμα βλέπουμε όλα τα σημεία που δίνει έμφαση και τις διαδικασίες που ακολουθεί μια ναυτιλιακή εταιρεία σχετικά με το Cyber Security για το γραφείο



Εικόνα 5 Διαδικασίες Cyber Security Εταιρείας

2.10.2 Οδηγός Cyber Security Onboard

Με τον ίδιο τρόπο που μια εταιρεία έχει την ανάγκη να προστατεύσει τα δεδομένα και τα συστήματά της στο γραφείο χρησιμοποιεί έναν παρόμοιο οδηγό και για τα πλοία της. Παρακάτω βλέπουμε κάποιους βασικούς κανόνες οι οποίοι συνδέονται με το Cyber Security Onboard.

Εικόνα 6 Διαδικασίες Cyber Security επί του πλοίου

Πιο αναλυτικά σχετικά με τον οδηγό των διαδικασιών για Cyber Security που εφαρμόζονται στο πλοίο:

- **Σκοπός:** Ο σκοπός του οδηγού που αφορά τα πλοία είναι να καθοριστούν οι απαιτήσεις ασφαλείας που σχετίζονται με τον κυβερνοχώρο και αφορούν τον κώδικα ISM σε μια ναυτιλιακή.
- **Ορισμοί:** Όπως και στον οδηγό για το γραφείο έτσι και στον οδηγό για το πλοίο ορίζονται οι ορισμοί οι οποίοι αφορούν την ασφάλεια στον κυβερνοχώρο.
- **Έλεγχος πρόσβασης:** Το πλήρωμα θα πρέπει να διαθέτει δικαιώματα στο δίκτυο του πλοίου ανάλογα με τα καθήκοντα που καλείται να εκτελέσει και δεν πρέπει να χορηγούνται πρόσθετα δικαιώματα σε άτομα. Αυτό θα δίνεται μόνο από τον διαχειριστή του συστήματος και κανείς άλλος δεν θα έχει δικαίωμα να αλλάζει ή να

προβάλλει τα δικαιώματα των χρηστών. Ο διαχειριστής μπορεί επίσης να δώσει δικαιώματα προνομιακής πρόσβασης σε άτομα που κάνουν μια πιο εξειδικευμένη δουλειά στο πλοίο καθώς και να καθορίσουν το χρονικό διάστημα σύνδεσης όπου το πλήρωμα θα αποσυνδέεται από τον υπολογιστή όταν ολοκληρωθούν οι εργασίες και θα τίθεται συγκεκριμένος χρόνος όπου θα ενεργοποιείται η προφύλαξη οθόνης (Hugh Boyes, 2014).

- **Προστασία από κακόβουλο λογισμικό:** για να μειωθεί ο κίνδυνος προσβολής από κάποιο ιό θα πρέπει όπως εφαρμόζεται και στο γραφείο να εφαρμόζονται και στο πλοίο αντίστοιχα μέτρα προστασίας. Το σύστημα στο πλοίο ελέγχεται κεντρικά από τους διαχειριστές του συστήματος δηλαδή από την εταιρεία (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts, 2017). Το πρόγραμμα προστασίας υποστηρίζει on line ενημερώσεις για κακόβουλο λογισμικό, καθημερινές προγραμματισμένες σαρώσεις, αφαίρεση αυτόματων σαρώσεων μέσων που δεν είναι του συστήματος και η χρήση USB θα πρέπει να είναι εξουσιοδοτημένη από το τμήμα πληροφορικής της εταιρείας (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).
- **Ασφάλεια κωδικών πρόσβασης:** Οι κωδικοί πρόσβασης θα πρέπει να προστατεύονται και να μην είναι σε κοινή θέα πάνω στο πλοίο και δεν επιτρέπεται να αλλάζουν οποιουδήποτε πάνω στο πλοίο. Οι πλοίαρχοι θα πρέπει να αλλάζουν κωδικούς σε κάθε αλλαγή αρχηγίας ώστε να διασφαλίζεται η εμπιστευτικότητα των πληροφοριών και των συστημάτων στο πλοίο. Επίσης, οι κωδικοί πρόσβασης δεν πρέπει να διαμοιράζονται μέσω ηλεκτρονικού ταχυδρομείου. Επιπρόσθετα, οι κωδικοί δεν θα πρέπει να ίδιοι με τους προηγούμενους και θα πρέπει να τηρούν κάποιους συγκεκριμένους κανόνες κατά τη δημιουργία τους όπως ακριβώς γίνεται και στο γραφείο (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017) (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts, 2017)
- **Ασφάλεια δικτύου:** για να είναι ασφαλές ένα δίκτυο θα πρέπει να λαμβάνονται υπ όψιν οι αρχές ασφαλείας κατά τον σχεδιασμό του. Οι αρχές ασφάλειας περιλαμβάνουν το επίπεδο κρισιμότητας των πληροφοριών που μεταφέρονται, τις πιθανές απειλές, το επίπεδο εμπιστοσύνης μεταξύ συστημάτων και δικτύου που πρόκειται να συνδεθούν σε αυτό, τη διαθεσιμότητα του δικτύου η οποία απαιτεί επίπεδα, τα μέτρα προστασίας σε σχέση με τοποθεσίες που έχουν πρόσβαση στο δίκτυο, τον διαχωρισμό των δικτύων βάση διαφορετικών επιχειρηματικών επιπέδων

και τέλος τείχη προστασίας και χρήση εικονικών δικτύων με τα οποία εξασφαλίζεται μόνο η εξουσιοδοτημένη κυκλοφορία στο δίκτυο (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).

- **Αντίγραφα ασφαλείας:** με τον ίδιο τρόπο του γραφείου έτσι και για το πλοίο θα πρέπει να δημιουργούνται αντίγραφα ασφαλείας και για το πλοίο. Αυτά θα πρέπει να αποθηκεύονται σε ασφαλή τοποθεσία, να αναπτυχθεί μια αυτοματοποιημένη διαδικασία για την δημιουργία τους και οι διαχειριστές του συστήματος να διασφαλίζουν ότι τα αντίγραφα ολοκληρώθηκαν με επιτυχία και να επαληθεύουν την ποσότητα που δημιουργήθηκε. Η μέθοδος που χρησιμοποιείται είναι αυτοματοποιημένη και πραγματοποιείται κάθε ορισμένο χρονικό διάστημα από τους διαχειριστές του συστήματος. Για παράδειγμα μια φορά την εβδομάδα μπορούμε να έχουμε ένα πλήρες αντίγραφο ασφαλείας (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).
- **Έλεγχος πρόσβασης ιδιωτικών συσκευών:** Σχετικά με τις προσωπικές συσκευές έχουν δικαίωμα να συνδέονται μόνο στο ασύρματο δίκτυο του πληρώματος και οι επισκέπτες στο ίδιο δίκτυο μόνο κατόπιν έγκρισης του πλοιάρχου (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).
- **Διαχείριση αφαιρούμενων μέσων:** Αυτό το κομμάτι αφορά όλες τις αφαιρούμενες συσκευές αποθήκευσης. Η πολιτική της εταιρείας απαγορεύει την πρόσβαση τέτοιου είδους συσκευών χωρίς εξουσιοδότηση στα συστήματα του πλοίου. Οι θήρες ΟΤ για πρόσβαση σε αυτές τις συσκευές ξεμπλοκάρονται μόνο για επιχειρησιακούς σκοπούς και αυτό γίνεται λίγο πριν από κάθε είδος εργασίας. Η μεταφορά δεδομένων πραγματοποιείται μόνο μέσω ενός υπολογιστή για επισκέπτες και ελέγχεται αυστηρά και η φόρτιση φορητών συσκευών μέσω USB θήρας απαγορεύεται. Κάθε πλοίο διαθέτει συγκεκριμένο αριθμό εξουσιοδοτούμενων μέσων τα οποία ορίζονται από τον υπεύθυνο ασφάλειας της εταιρείας καθώς ορίζεται και ποιος θα έχει δικαιώματα πρόσβασης σε αυτά (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).
- **Ασφάλεια ηλεκτρονικού ταχυδρομείου:** Το e-mail του πλοίου θα πρέπει να χρησιμοποιείται αποκλειστικά και μόνο για επιχειρησιακούς σκοπούς της εταιρείας και η προσωπική χρήση απαγορεύεται ρητά. Υπεύθυνος για τη σωστή χρήση του

ηλεκτρονικού ταχυδρομείου είναι ο πλοίαρχος και η χρήση του θα πρέπει να ακολουθεί τους κανόνες ασφαλείας της εταιρείας (Kimberly Tam, Kevin Jones, 2019).

- **Αποδεκτή χρήση Internet:** Η χρήση του διαδικτύου στο πλοίο είναι περιορισμένη και αυτό γίνεται ώστε να μην επηρεάζεται η ασφαλή λειτουργία του σκάφους και να παρέχεται ασφάλεια πληροφοριών. Ο κατάλογος των επιτρεπόμενων σελίδων εξετάζεται ετησίως από τον υπεύθυνο για την ασφάλεια στον κυβερνοχώρο της εταιρείας. Το πλήρωμα μπορεί να χρησιμοποιεί το Internet μόνο από προσωπικές συσκευές με τη σύνδεση στο δίκτυο πληρώματος που παρέχεται στο πλοίο. Το ακατάλληλο περιεχόμενο επίσης ελέγχεται μέσω firewall στο δίκτυο πληρώματος. Τέλος, στο πλήρωμα απαγορεύεται να παρακάμπτει τους κανόνες ασφαλείας ώστε να τίθεται σε κίνδυνο η εταιρεία και η πρόσβαση μπορεί να παρακολουθείται σε περιπτώσεις που η εταιρεία κρίνει ότι υπόκειται σε κίνδυνο (BIMCO, 2018).
- **Απάντηση περιστατικού και σχέδιο αποκατάστασης:** Τα περιστατικά που παρουσιάζονται ενδέχεται να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα του συστήματος του σκάφους. Για αυτό το λόγο τα περιστατικά κατηγοριοποιούνται ως εξής:
    1. Άρνηση παροχής υπηρεσίας.
    2. Κακόβουλος κώδικας.
    3. Μη εξουσιοδοτημένη πρόσβαση.
    4. Ακατάλληλη χρήση.

  Όπως και στο γραφείο έτσι και για το πλοίο έχουμε αναφορικά κάποια συμπτώματα ασφαλείας τα οποία μπορούν να επηρεάσουν την ομαλή λειτουργία του σκάφους. Αυτά περιλαμβάνουν την δυσλειτουργία του συστήματος υλικού ή λογισμικού, κάποιος ιός ο οποίος δεν ενημερώνεται σε σταθμούς λειτουργίας, όταν δεν λειτουργούν οι κωδικοί πρόσβασης, άνοιγμα ύποπτων συνημμένων, εκτέλεση άγνωστων προγραμμάτων, κατεστραμμένα αρχεία, σφάλματα σταθμών εργασίας κ.α.

  Θα μπορούσαν να συμπεριληφθούν και άλλα πολλά όμως αυτό αποσκοπεί στο επίπεδο συνειδητοποίησης και όσα αναφέρονται παραπάνω αποτελούν ένα μικρό παράδειγμα. Όταν δεν υπάρχει βεβαιότητα για κάποιο περιστατικό, αυτό αντιμετωπίζεται ως πραγματικό και σε κάθε περίπτωση θα πρέπει ο πλοίαρχος να επικοινωνεί με τον υπεύθυνο ασφαλείας της εταιρείας (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).

- **<u>Φυσική ασφάλεια:</u>** Ο κρίσιμος εξοπλισμός του σκάφους θα πρέπει να προστατεύεται από τυχόν φυσικές καταστροφές ή απροσεξία του πληρώματος. Τα συστήματα δεν πρέπει ποτέ να παραμένουν χωρίς επίβλεψη και το πλήρωμα θα πρέπει να μην καπνίζει και να μην τρώει σε αυτές τις κρίσιμες περιοχές. Τα συστήματα UPS θα πρέπει να είναι σε θέση να προστατεύουν τα συστήματα σε περιπτώσεις διακοπής ρεύματος. Σχετικά με τους επισκέπτες υπάρχει ειδικό δίκτυο γι αυτούς επί του σκάφους και δεν επιτρέπεται η πρόσβασή τους οπουδήποτε θέτει σε κίνδυνο το σκάφος και κατ επέκταση τη εταιρεία. Τυχόν επιδιορθώσεις του συστήματος θα πραγματοποιούνται μόνο από εξουσιοδοτημένο προσωπικό (Huge Boyes, 2014).
- **<u>Επίγνωση και εκπαίδευση:</u>** Το σημείο αυτό αφορά την ευαισθητοποίηση και την εκπαίδευση του πληρώματος σε σχέση με το Cyber Security. Όπως και στο γραφείο έτσι και στο πλοίο δίνονται κάποιες βασικές οδηγίες σχετικά με τη χρήση αλλά και με τη συμπεριφορά του πληρώματος ώστε να διασφαλίζονται οι πληροφορίες της εταιρείας και τα περιουσιακά της στοιχεία από κακόβουλους χρήστες (Krzysztof Cabaj, Dulce Domingos, Zbigniew Kotulski, Ana Respico, 2018).
- **<u>Αρχεία:</u>** Όπως και στο γραφείο θα πρέπει και στο πλοίο για τα αρχεία να διατηρείται μητρώο πρόσβασης και να ελέγχονται τα δικαιώματα των χρηστών που έχουν πρόσβαση σε αυτά. Τέλος να εφαρμόζεται δοκιμή δημιουργίας αντιγράφων ασφαλείας (BIMCO, 2018).

3. Μεθοδολογία έρευνας

«η ερευνητική διαδικασία έχει ως αφορμή ένα προβληματισμό και προσπαθεί να απαντήσει σε ένα ερευνητικό ερώτημα. Ένας ερευνητής καλείται να σχεδιάσει τη μεθοδολογία που θα υιοθετήσει σε σχέση με τον προβληματισμό του και σε συνάρτηση με το υπό εξέταση πεδίο και θέμα του (Δημητρόπουλος,2004).

Η μεθοδολογία έρευνας αναφέρεται στις παραμέτρους της ερευνητικής προσπάθειας του ερευνητή, οι οποίες αφορούν στις γενικές μεθοδολογικές προσεγγίσεις, στις μεθόδους, στις τεχνικές, στα μέσα, στα υλικά και στις διαδικασίες που θα επιλέξει για τη διεξαγωγή της έρευνας του» (Δημητρόπουλος,2004).

Οι φάσεις μιας έρευνας είναι τρείς (Cohen L – Manion L. ,1994):

- Προπαρασκευαστική φάση: Σε αυτή τη φάση επιλέγουμε το ερευνητικό θέμα και αποφασίζουμε ποια ερευνητική διαδικασία θα ακολουθηθεί ώστε να συλλεχθούν τα απαραίτητα στοιχεία και να λύσουμε το πρόβλημα.
- Εκτελεστική φάση: Σε αυτή τη φάση γίνεται η συλλογή των δεδομένων όπως είναι η βιβλιογραφία και η ερμηνεία.
- Κοινοποίηση αποτελεσμάτων: Σε αυτή τη φάση γίνεται η συγγραφή της ερευνητικής μελέτης και στη συνέχεια κοινοποίηση στην επιστημονική κοινότητα.

Σε μια έρευνα έχω θέματα λήψης απόφασης όπου θέτω το πρόβλημα-θέμα και βλέπω «τι πρέπει να κάνω». Έτσι, το ερευνητικό μου ερώτημα απαντάται στην ερώτηση «τι πρέπει να ξέρω». Επίσης, μια έρευνα θα πρέπει να απαντάει στα εξής ερωτήματα: ποιος, που, πότε, γιατί, με ποιόν τρόπο (Κυριαζόπουλος Π. –Σαμαντά Ε. , 2011).

3.1 Ποσοτική μεθοδολογία

Ποσοτική είναι η έρευνα η οποία πραγματοποιείται με τη χρήση ερωτηματολογίου και η ανάλυση των δεδομένων γίνεται στατιστικά (Δημητρόπουλος Ε., 2004). Στην παρούσα έρευνα το ερωτηματολόγιο έχει σταλεί σε στελέχη ναυτιλιακών εταιρειών στην Ελλάδα. Τα στελέχη αυτά απαρτίζουν τη διεύθυνση της εταιρείας, του HSQE καθώς και του νομικού και του IT τμήματος. Έτσι η έρευνα μπορεί να χαρακτηριστεί ως εμπειρική μικρής έκτασης η οποία καταγράφει τις απόψεις των εργαζομένων σε θέσεις ευθύνης. Στη παρούσα έρευνα εφαρμόζεται η ποσοτική μεθοδολογία η οποία υπόκειται στη φιλοσοφία του θετικισμού (positivism). Η συλλογή των στοιχείων που απαντούν στα ερωτήματα της έρευνας γίνεται με τη βοήθεια ερωτηματολογίου με τη μέθοδο της δειγματοληψίας. Στη ποσοτική μεθοδολογία έχουμε παραγωγική προσέγγιση. Επίσης, η συγκεκριμένη έρευνα είναι περιγραφική εφόσον απαντά σε ερωτήματα σε συγκεκριμένη χρονική περίοδο (Ιούνιος – Ιούλιος 2019) (Νόβα-Κατσούνη, 2006).

3.1.1 Δείγμα

Δείγμα ονομάζεται το σύνολο των του πληθυσμού από το οποίο προκύπτει το αποτέλεσμα μιας έρευνας. Το δείγμα επιλέχθηκε με βάση τη γνώση σχετικά με το αντικείμενο της έρευνας, από τα άτομα που έχει απευθυνθεί η έρευνα, αλλά και την θέση που κατέχει ο καθένας τους στην ναυτιλία. Ο αριθμός είναι περιορισμένος και αποτελείται από 87

ερωτηματολόγια. Αυτό καθιστά την έρευνα ιδιαίτερα σημαντική. Οι απαντήσεις είναι σχεδόν το 50% αλλά στην πραγματικότητα το ξεπερνά διότι μερικά άτομα από το σύνολο του δείγματος δεν ήταν σε θέση να απαντήσουν λόγω θέσης ή φύση εταιρείας.

3.2 Ερευνητικό εργαλείο

Το ερευνητικό εργαλείο το οποίο χρησιμοποιήθηκε είναι η χρήση ερωτηματολογίου το οποίο ενσωματώθηκε σε Google forms και στη συνέχεια εστάλη μέσω email στους ερωτηθέντες. Στη συνέχεια έγινε επεξεργασία των αποτελεσμάτων σε ένα μέρος με τη χρήση SPSS ενώ τι υπόλοιπο κομμάτι απαντήθηκε απ ευθείας από το Google forms.

3.3 Ανάλυση δεδομένων

Από την διεξαγωγή της έρευνας, πήραμε 37 απαντήσεις. Το ερωτηματολόγιο ήτανε χωρισμένο σε τέσσερα κεφάλαια από τα οποία τα πρώτα τρία αναλύθηκαν περιγραφικά ενώ το τελευταίο κεφάλαιο που αφορά τη σημαντικότητα των ερωτήσεων όσων αφορά τις εταιρείες των ερωτηθέντων, αναλύθηκαν με τη βοήθεια του προγράμματος SPSS. Αυτό έγινε επειδή οι συγκεκριμένες ερωτήσεις βασίστηκαν στην κλίμακα Likert με ένα εύρος από το 1 «πολύ σημαντικό » έως το 5 «καθόλου σημαντικό».

3.4 Περιορισμοί

Οι περιορισμοί σχετικά με την παρούσα έρευνα ήταν αρκετοί.

- Η έρευνες οι οποίες διεξάγονται με τη χρήση διαδικτύου έχουν μια δυσκολία στο να απαντηθούν από τους συμμετέχοντες σε αυτή. Επειδή, αναφερόταν σε διευθυντικά στελέχη οι απαντήσεις στην αρχή ήτανε περιορισμένες.
- Η τηλεφωνική επικοινωνία ήταν απαραίτητη στον κάθε έναν από τον πληθυσμό του δείγματος, έτσι ώστε να επιτευχθεί ο καλύτερος δυνατός αριθμός απαντήσεων.
- Περιορισμός λόγω χρόνου παράδοσης του Project.
- Η παρούσα έρευνα πραγματοποιήθηκε στα πλαίσια εταιρικού Project, αυτό είχε ως αποτέλεσμα τη συνεννόηση μιας μικρής ομάδας ατόμων. Αυτό καθιστά από μόνο του δύσκολη τη διεξαγωγή της παρούσας έρευνας.
- Στον πληθυσμό του δείγματος υπήρχανε μη κατάλληλα άτομα να απαντήσουν το ερωτηματολόγιο λόγω διαφορετικού εργασιακού τίτλου, όπως για παράδειγμα

διευθυντικά στελέχη σε συμβουλευτικές εταιρείες ή άτομα που δεν εργαζόντουσαν πια σε ναυτιλιακές εταιρείες.

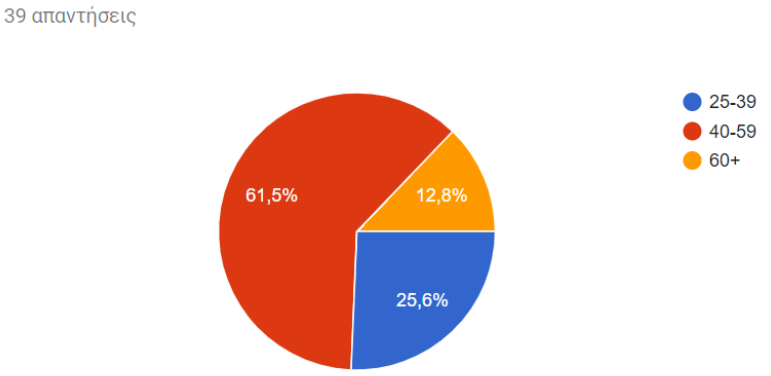
- Σε μερικές περιπτώσεις ήταν κλειδωμένος ο σύνδεσμος του ερωτηματολογίου από το τμήμα IT της εταιρείας. Αυτό συνέβαινε στα πλαίσια διασφάλισης της ασφάλειας της εταιρείας και χρειάστηκε τηλεφωνική επικοινωνία και επεξήγηση σχετικά με το τι αφορά ώστε να ξεκλειδώσουν τον σύνδεσμο και να καταφέρει ο ερωτηθέντας να απαντήσει στις ερωτήσεις.

4. Παρουσίαση αποτελεσμάτων

Στο κεφάλαιο αυτό θα δούμε αναλυτικά τα αποτελέσματα της έρευνας όπως αυτή απαντήθηκε από το δείγμα. Η παρούσα έρευνα η οποία πραγματοποιήθηκε με τη χρήση ερωτηματολογίου χωρίζεται σε τέσσερα κεφάλαια. Τα κεφάλαια αυτά αφορούν τις προσωπικές πληροφορίες των ερωτηθέντων, τις προσωπικές πληροφορίες της εταιρείας που εργάζονται, πληροφορίες της εταιρείας σε σχέση με το Cyber Security στη ναυτιλία και τέλος ένα κεφάλαιο με κάποιες διαδικασίες στο οποίο το δείγμα καλείται να απαντήσει πόσο σημαντική θεωρεί την ερώτηση για την εταιρεία του και για τον ίδιο.

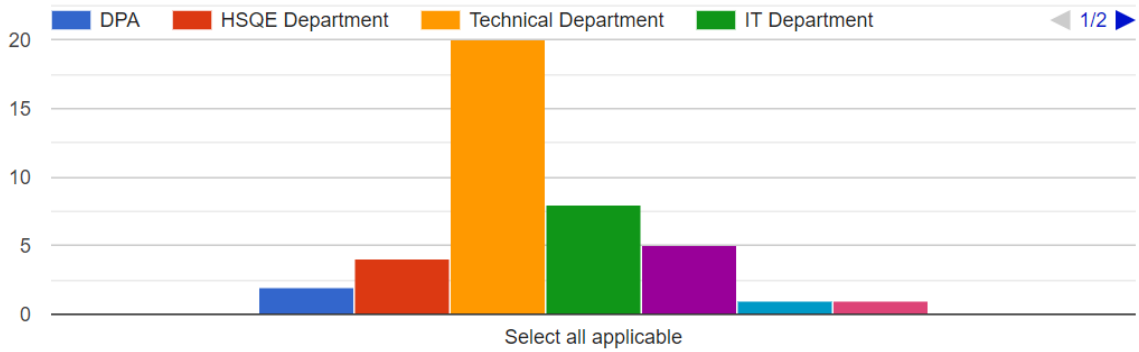
4.1 Προσωπικές πληροφορίες

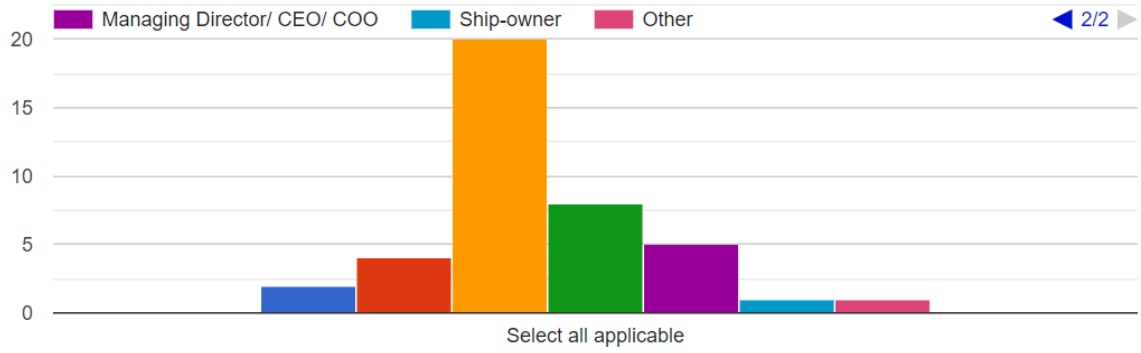
1. **Η ηλικία του δείγματος περιλαμβάνει τια παρακάτω ομάδες και διαχωρίζεται ως εξής όπως φαίνεται από το παρακάτω γράφημα.**



Από το παραπάνω γράφημα προκύπτει ότι σε ποσοστό 25,6% δηλαδή 10 άτομα από τα 39 που απάντησαν στην έρευνα είναι μεταξύ 25-39 ετών, το 61,5% δηλαδή 24 άτομα είναι μεταξύ 40-59 ετών και τέλος μόλις το 12,8% του δείγματος δηλαδή 5 άτομα είναι από 60 και πάνω. Η πλειοψηφία αποδεικνύει ότι τις υψηλά ιστάμενες κατέχουν άτομα μιας μέσης ηλικίας με τους νεότερους να ακολουθούν.

2. Επιλογή θέσης εργασίας



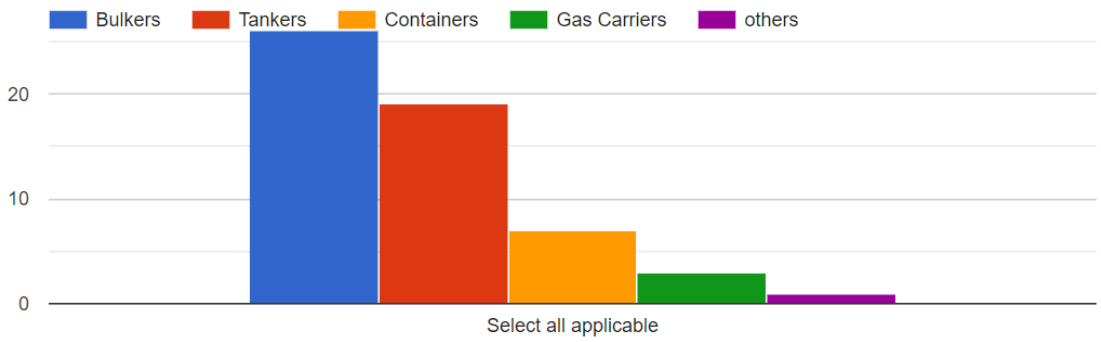


Οι θέσεις εργασίας που κατέχει το δείγμα φαίνεται στον παρακάτω πίνακα:

Α/Α	ΘΕΣΗ	ΠΛΗΘΥΣΜΟΣ
1	DPA	2
2	HSQE	4
3	Technical Department	20
4	IT Department	8
5	Managing Director/ CEO/ COO	5
6	Ship-Owner	1
7	Other	1

4.2 Γενικές πληροφορίες εταιρείας

1. **Το είδος των πλοίων που διαχειρίζονται οι εταιρείες διακρίνεται από το παρακάτω γράφημα:**



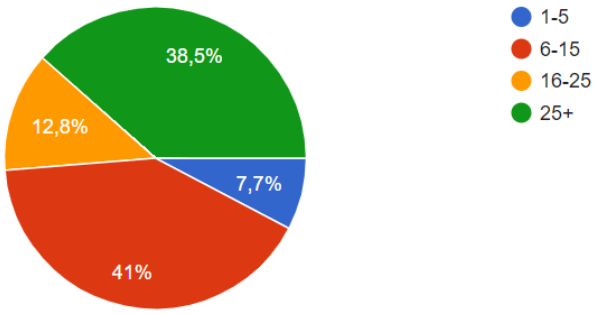
Στον παρακάτω πίνακα παρουσιάζονται αναλυτικά το είδος των πλοίων που διαχειρίζεται η κάθε εταιρεία από τις 39 που απάντησαν στη έρευνα:

Α/Α	ΕΙΔΟΣ ΠΛΟΙΩΝ	ΠΛΗΘΥΣΜΟΣ
1	Bulkers	26
2	Tankers	19
3	Containers	7
4	Gas Carriers	3
5	Other	1

Από τον παραπάνω πίνακα φαίνεται ότι η πλειοψηφία του είδους των πλοίων είναι Bulkers, ακολουθούν τα Tankers και έχουμε πολύ ένα αρκετά μικρότερο ποσοστό από τις υπόλοιπες κατηγορίες.

2. Αριθμός πλοίων εταιρείας

39 απαντήσεις



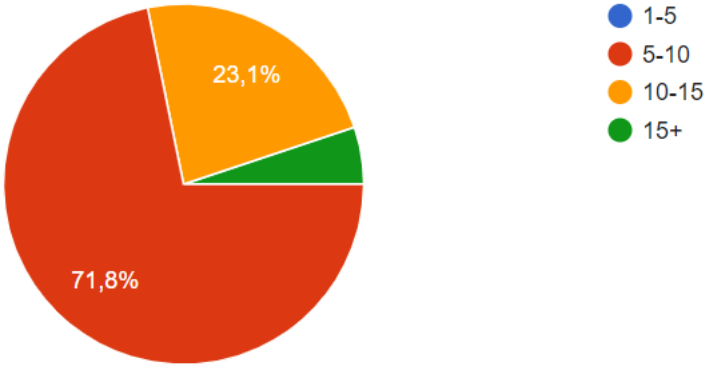
Α/Α	ΑΡΙΘΜΟΣ ΠΛΟΙΩΝ	ΠΛΗΘΥΣΜΟΣ
1	1-5	3
2	6-15	16
3	16-25	5
4	25+	15

Από τον παραπάνω πίνακα προκύπτει ότι η πλειοψηφία των εταιρειών του δείγματος είναι μεσαίου μεγέθους (6-15 πλοία) με ποσοστό 41%. Πιο συγκεκριμένα 16 άτομα από τα 39

που απάντησαν την έρευνα επέλεξαν αυτή την κατηγορία αριθμού των πλοίων της εταιρείας τους. Ακολουθούνε οι μεγάλες εταιρείες (25+ πλοία) με ποσοστό 38,5% και με 15 απαντήσεις.

3. **Η πλειοψηφία της ηλικίας των πλοίων ανά εταιρεία διακρίνεται στο παρακάτω διάγραμμα:**

39 απαντήσεις



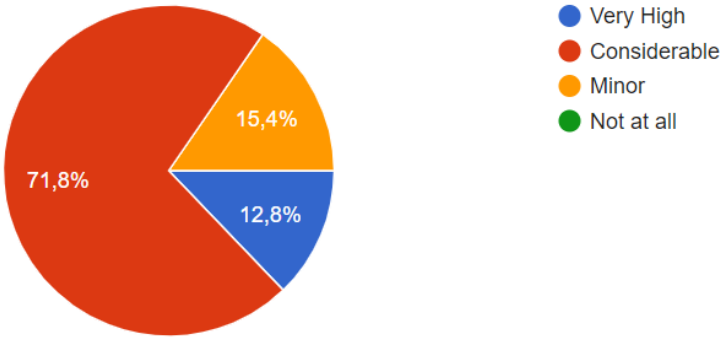
Α/Α	ΗΛΙΚΙΑ ΠΛΟΙΩΝ	ΠΛΗΘΥΣΜΟΣ
1	1-5	0
2	5-10	28
3	10-15	9
4	15+	2

Από τα παραπάνω προκύπτει ότι η πλειοψηφία της ηλικίας των πλοίων με ποσοστό 71,8% είναι νέα πλοία (1-5 έτη) και αυτή την απάντηση να την έχουν δώσει 28 από τους 39 που απάντησαν στην έρευνα. Έπονται οι εταιρείες με πλοία μέσης ηλικίας (10-15 έτη) οι οποίες φτάνουν το 23,1% δηλαδή 9 απάντησαν από τους 39. Τέλος, μόλις το 5,1% δηλαδή 2 εταιρείες κατέχουν μεγαλύτερα σε ηλικία βαπόρια και καμία εταιρεία δεν αποτελείται εξ ολοκλήρου από νεόδμητα βαπόρια.

4.3 Πληροφορίες της εταιρείας σχετικά με το Cyber Security

1. **Πιστεύετε ότι οι απειλές στον κυβερνοχώρο θέτουν σημαντικό κίνδυνο για τη βιομηχανία;**

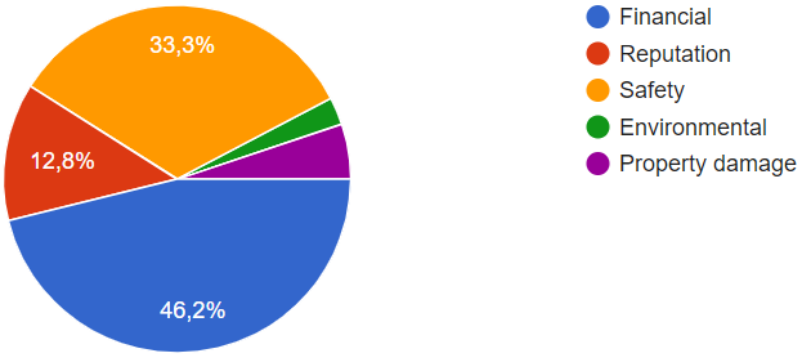
39 απαντήσεις



Από το παραπάνω διάγραμμα φαίνεται ότι το μεγαλύτερο ποσοστό 71,7% (28 άτομα) απάντησε ότι θεωρούν τις απειλές στον κυβερνοχώρο σημαντικές για τον κίνδυνο που υφίσταται η βιομηχανία της ναυτιλίας. Ακολουθεί το ποσοστό του 15,4% (6 άτομα) το οποίο θεωρεί ότι είναι μικρής σημασίας και τελειώνοντας, μόλις το 12,8% (5 άτομα) απάντησε ότι ο κίνδυνος αυτός είναι πολύ υψηλός ενώ κανένας δεν απάντησε ότι δεν συμφωνεί σε κάποια από τα παραπάνω.

2. **Ποιο θεωρείτε μεγαλύτερο κίνδυνο σε περίπτωση περιστατικού για την ασφάλεια στον κυβερνοχώρο;**

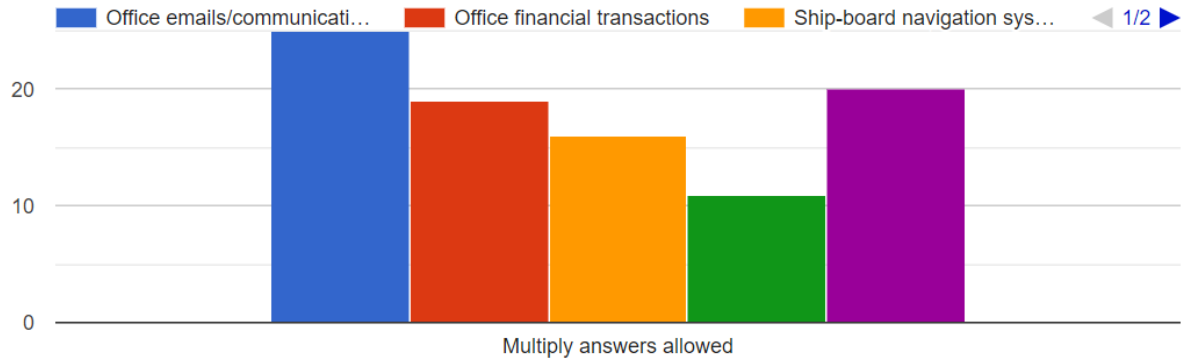
39 απαντήσεις

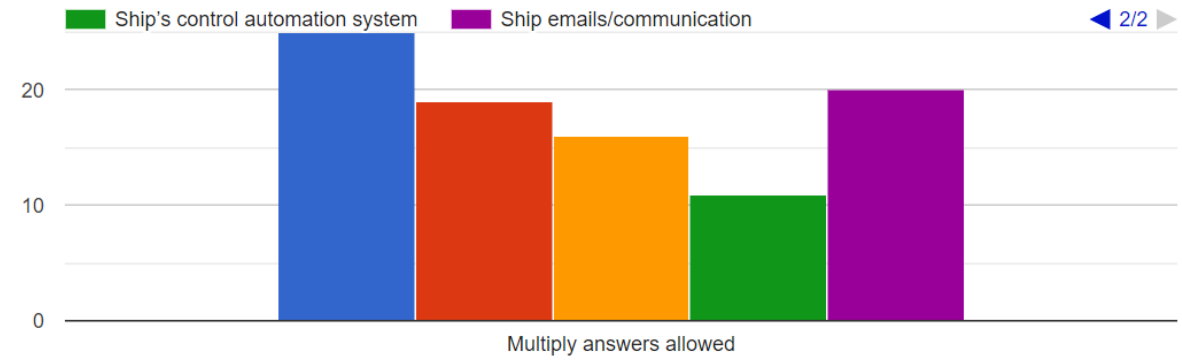


Σε περίπτωση κάποιου περιστατικού το οποίο επηρεάζει την ασφάλεια στον κυβερνοχώρο σε σχέση με το είδος του κινδύνου, οι ερωτηθέντες απάντησαν με ποσοστό πλειοψηφίας

46,2% (18 άτομα) ότι ο μεγαλύτερος κίνδυνος θεωρούν πως είναι χρηματοοικονομικός. Έπειτα, με ποσοστό 33,3% (13 άτομα) σημασία έδωσαν στην ασφάλεια. Στη συνέχεια 12,8% (5 άτομα) επέλεξαν τη φήμη. Τέλος, δύο άτομα απάντησαν ο κίνδυνος της καταστροφής ιδιοκτησίας και μόλις ένας απάντησε τον περιβαλλοντικό κίνδυνο.

3. Ποιο από τα παρακάτω συστήματα πιστεύετε ότι εκτίθεται στον μεγαλύτερο κίνδυνο στον κυβερνοχώρο;



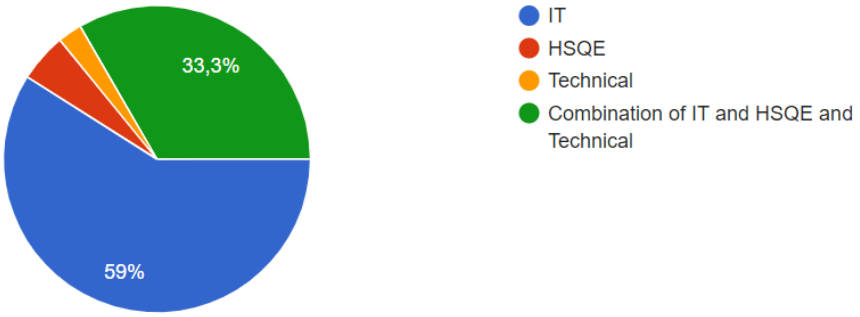


Στην ερώτηση σχετικά με τα συστήματα που εκτίθενται περισσότερο σε κίνδυνο σε μια εταιρεία, οι ερωτηθέντες είχανε δικαίωμα να επιλέξουν παραπάνω από μια απάντηση. Έτσι λοιπόν, οι 25 από τους 39 ερωτηθέντες απάντησαν πως το σύστημα που εκτίθεται περισσότερο σε κίνδυνο σε μια εταιρεία είναι η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου μιας εταιρείας. Ακολουθεί η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου του πλοίου με 20 απαντήσεις. Στη συνέχεια 19 απαντήσεις αφορούν τις

χρηματοοικονομικές συναλλαγές του γραφείου, 15 το σύστημα πλοήγησης του πλοίου και τέλος, 11 το σύστημα αυτόματου ελέγχου του πλοίου.

4. **Ποιο είναι το αρμόδιο τμήμα το οποίο είναι υπεύθυνο για την ασφάλεια στον κυβερνοχώρο στην εταιρεία σας;**

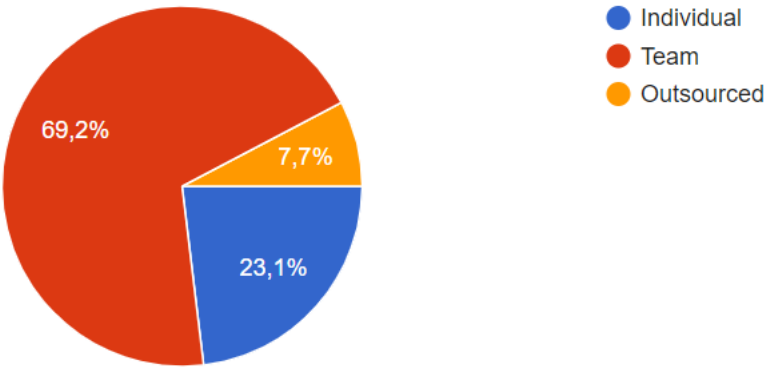
39 απαντήσεις



Από το παραπάνω γράφημα βλέπουμε ότι η πλειοψηφία των απαντήσεων σε σχέση με το ποιο τμήμα είναι υπεύθυνο για την ασφάλεια του κυβερνοχώρου στην εταιρεία του κάθε ερωτηθέντα, αφορά το IT τμήμα με 23 απαντήσεις από τις 39 και ακολουθεί η απάντηση «συνδυασμός IT, HSQE και τεχνικό τμήμα» με 13 απαντήσεις από τις 39. Τέλος, 2 άτομα απάντησαν ότι υπεύθυνο είναι το τμήμα HSQE και μόλις 1 το τεχνικό τμήμα.

5. **Υπάρχει άτομο ή ομάδα ατόμων στην εταιρεία οι οποίοι να είναι υπεύθυνοι για την κυβερνοασφάλεια της εταιρείας ή αυτό ανατίθεται σε εξωτερικούς συνεργάτες;**

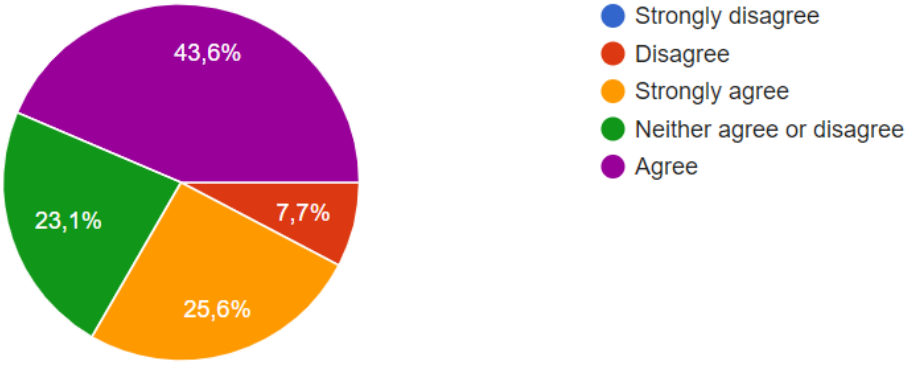
39 απαντήσεις



Από το παραπάνω γράφημα φαίνεται ότι η πλειοψηφία με 27 άτομα από τα 39 των εταιρειών που απάντησαν, έχουν κάποια ομάδα στην εταιρεία τους η οποία είναι υπεύθυνη για την κυβερνοασφάλεια. Μόλις 3 άτομα απάντησαν ότι εμπιστεύονται την ασφάλεια στον κυβερνοχώρο σε εξωτερικούς συνεργάτες και 9 απάντησαν ότι υπάρχει συνδυασμός των παραπάνω.

6. Η εταιρεία είναι προετοιμασμένη για μια πιθανή επίθεση στον κυβερνοχώρο.

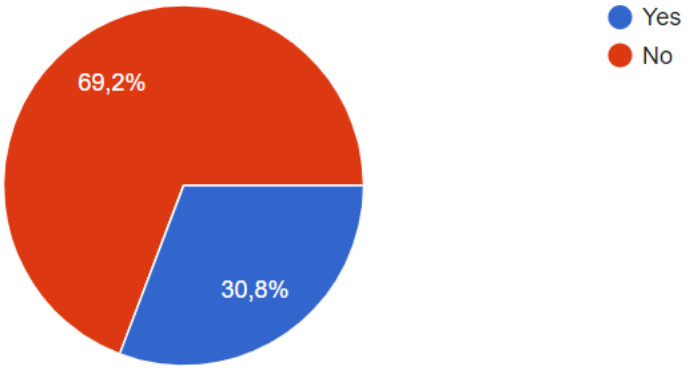
39 απαντήσεις



Η πλειοψηφία στην ερώτηση εάν είναι προετοιμασμένη η εταιρεία για μια πιθανή επίθεση στον κυβερνοχώρο απάντησε ότι συμφωνεί με 17 απαντήσεις από τις 39. Οι 10 απάντησαν ότι συμφωνούν απόλυτα και ακολουθούν οι όχι κ πολύ σίγουροι με 9 απαντήσεις. Τέλος αυτοί που διαφωνούν είναι μόλις 3.

7. Η εταιρεία έχει στη διάθεσή της κάποια μέτρα προστασίας τα οποία δεν τεκμηριώνονται.

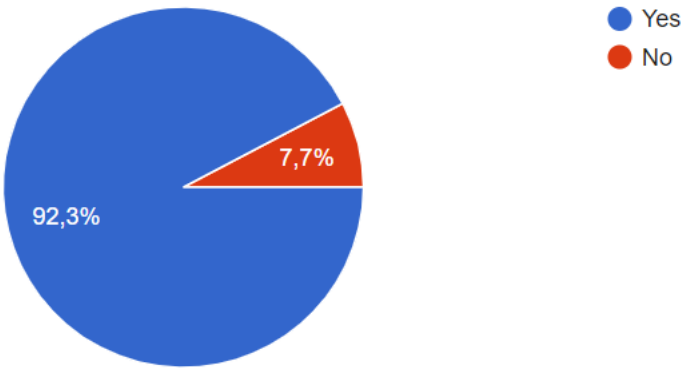
39 απαντήσεις



Στην παραπάνω ερώτηση η πλειοψηφία με 27 από τα 39 άτομα απάντησε πως δεν διαθέτουν μέτρα τα οποία δεν τεκμηριώνονται ενώ 12 από τα 39 άτομα απάντησαν πως έχουν μη τεκμηριωμένα μέτρα ασφαλείας.

8. Η εταιρεία έχει τεκμηριωμένη πολιτική προστασίας και διαδικασίες για την ασφάλεια στον κυβερνοχώρο.

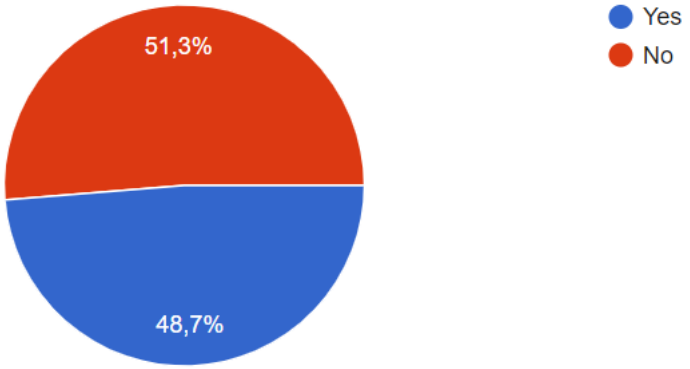
39 απαντήσεις



Η πλειοψηφία με 36 απαντήσεις από τις 39 απάντησε πως η πολιτική προστασίας της εταιρείας για την ασφάλεια στον κυβερνοχώρο είναι τεκμηριωμένη και μόλις 3 απαντήσεις ήταν αρνητικές.

9. Η εταιρεία έχει στη διάθεσή της ένα σύστημα διαχείρισης της ασφάλειας του κυβερνοχώρου το οποίο ελέγχεται από κάποιο εξωτερικό συμβαλλόμενο μέρος.

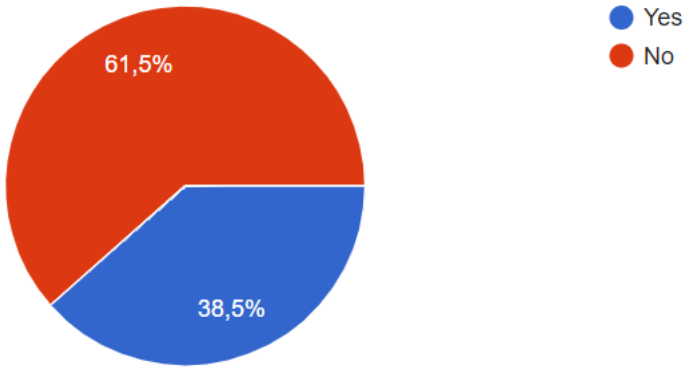
39 απαντήσεις



Από το παραπάνω γράφημα προκύπτει πως 20 άτομα απάντησαν πως η εταιρεία δεν έχει αναθέσει την διαχείριση ασφάλειας του κυβερνοχώρου της σε κάποιο εξωτερικό συνεργάτη ενώ 19 άτομα απάντησαν ότι αυτό γίνεται μέσω κάποιου εξωτερικού συμβαλλόμενου μέρους.

10. Η εταιρεία έχει εμπειρία από κάποιο περιστατικό απειλής της ασφάλειας του κυβερνοχώρου τα τελευταία τρία χρόνια.

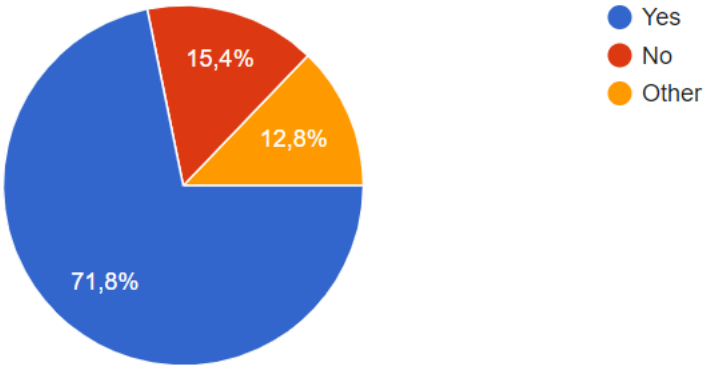
39 απαντήσεις



Σχετικά με την εμπειρία απειλής τα τελευταία τρία χρόνια στις εταιρείες του δείγματος η πλειοψηφία απάντησε πως δεν είχαν κάποια εμπειρία με 24 απαντήσεις από τις 39 ενώ οι υπόλοιποι 15 από τους 39 απάντησαν θετικά.

11. Έχει η εταιρεία διαδικασία αξιολόγησης η οποία αντιμετωπίζει απειλές και τρωτά σημεία;

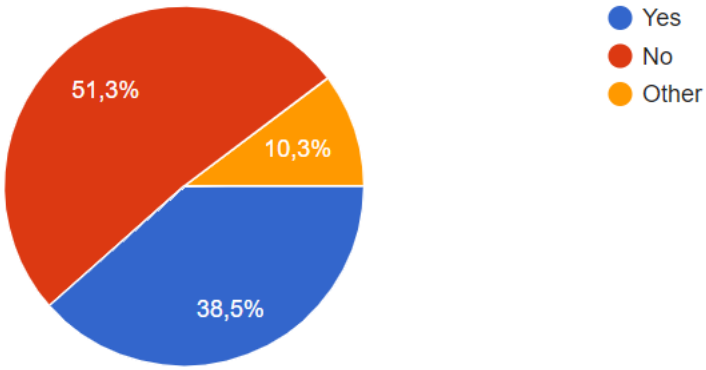
39 απαντήσεις



Από το παραπάνω γράφημα προκύπτει ότι 28 από τους 39 απάντησαν ότι η εταιρεία τους έχει διαδικασία αξιολόγησης κινδύνου. Έπειτα, μόλις 6 απάντησαν ότι δεν εφαρμόζεται κάτι τέτοιο και οι υπόλοιποι 5 απάντησαν άλλο.

12. Έχει γίνει από την εταιρεία σας κάποια δοκιμή διείσδυσης του συστήματος;

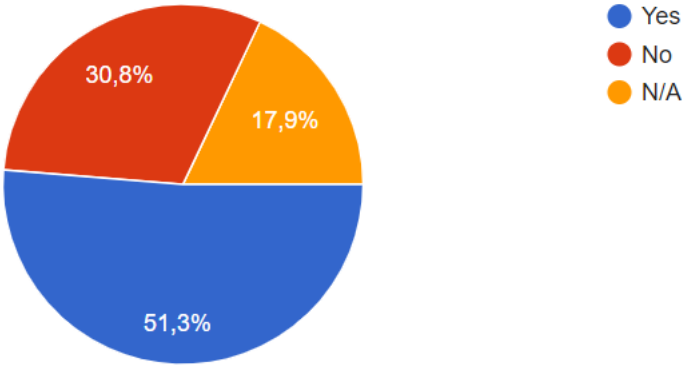
39 απαντήσεις



Όπως φαίνεται στο γράφημα η πλειοψηφία των ερωτηθέντων δεν έχει εφαρμόσει κάποια δοκιμή διείσδυσης του συστήματος της εταιρείας τους με 20 απαντήσεις από τις 39, 15 απάντησαν ότι έχουν κάνει κάποια δοκιμή ενώ 4 έδωσαν άλλη απάντηση.

13. Είναι η εταιρεία σας προετοιμασμένη για τις απαιτήσεις του TMSA3;

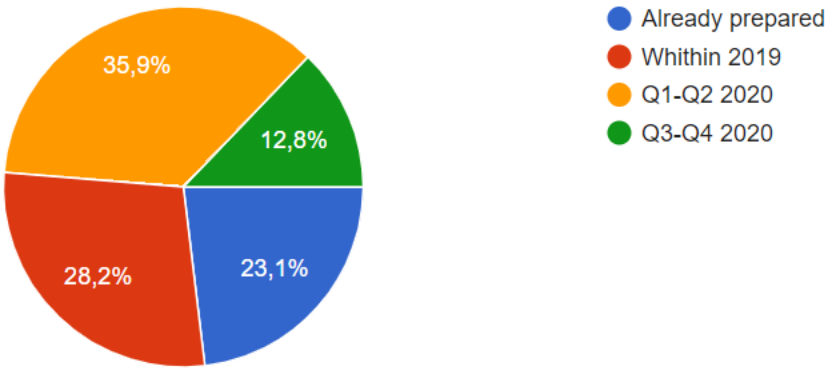
39 απαντήσεις



Από το παραπάνω γράφημα προκύπτει ότι 20 από τις 39 απαντήσεις του δείγματος είναι θετικές. Είναι δηλαδή προετοιμασμένοι σχετικά με τις απαιτήσεις του TMSA3. Οι 12 δεν είναι ενώ 7 δεν απαντούν επειδή προφανώς η εταιρεία τους δεν έχει tankers.

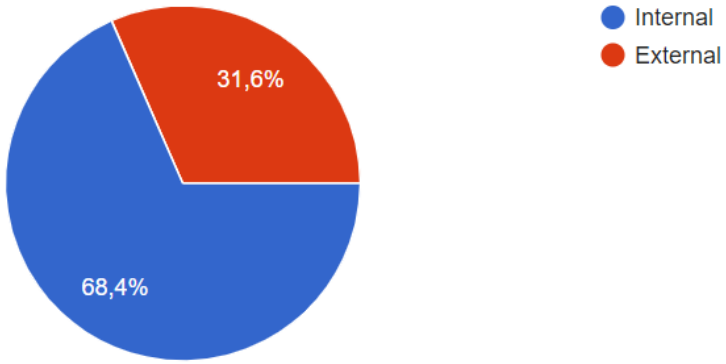
14. Πότε προγραμματίζει η εταιρεία να προετοιμαστεί για τις απαιτήσεις του IMO σχετικά με Cyber Security οι οποίες ισχύουν από 1η Ιανουαρίου 2021;

39 απαντήσεις



Σχετικά με το χρονοδιάγραμμα της εταιρείας που αφορά την προετοιμασία της σχετικά με τις απαιτήσεις του IMO που αφορούν το Cyber Security, η πλειοψηφία με 14 από τις 39 απατήσεις απάντησε ότι προγραμματίζει να προετοιμαστεί μεταξύ του 1ου και 2ου τριμήνου του 2020, 11 από το δείγμα απάντησαν μέσα στο 2019, μόλις 9 είναι ήδη προετοιμασμένοι και τέλος 5 μεταξύ 3ου και 4ου τριμήνου του 2020.

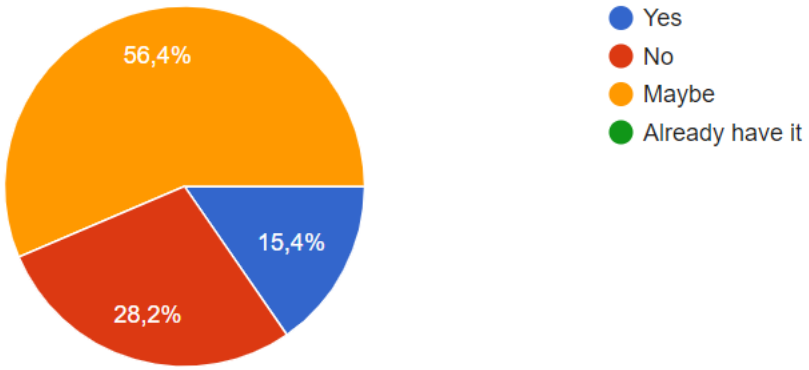
15. Σκοπεύει η εταιρεία να προετοιμαστεί εσωτερικά ή με εξωτερική υποστήριξη σχετικά με τις απαιτήσεις του IMO;



Από το παραπάνω γράφημα προκύπτει ότι, η εταιρεία σκοπεύει να προετοιμαστεί εσωτερικά σχετικά με τις απαιτήσεις του IMO με 27 από τις 39 απαντήσεις ενώ εξωτερικά απάντησαν 12 από τα 39 άτομα του δείγματος.

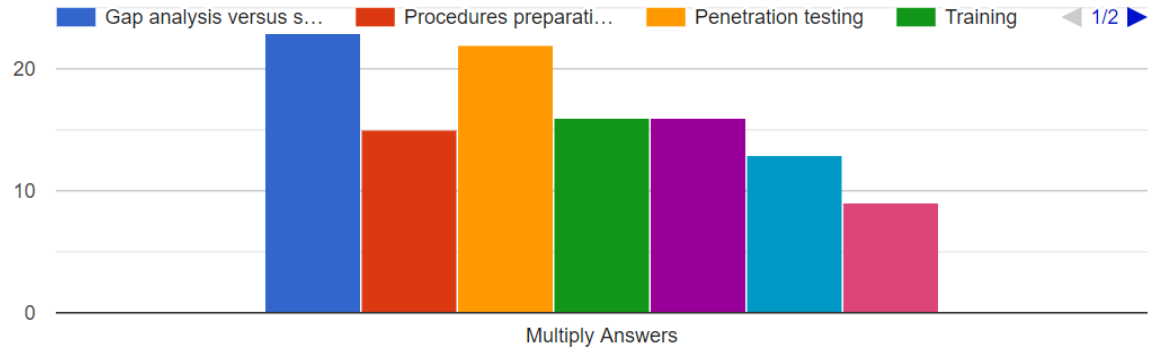
16. Σκοπεύει η εταιρεία να αποκτήσει πιστοποίηση ISO 27001;

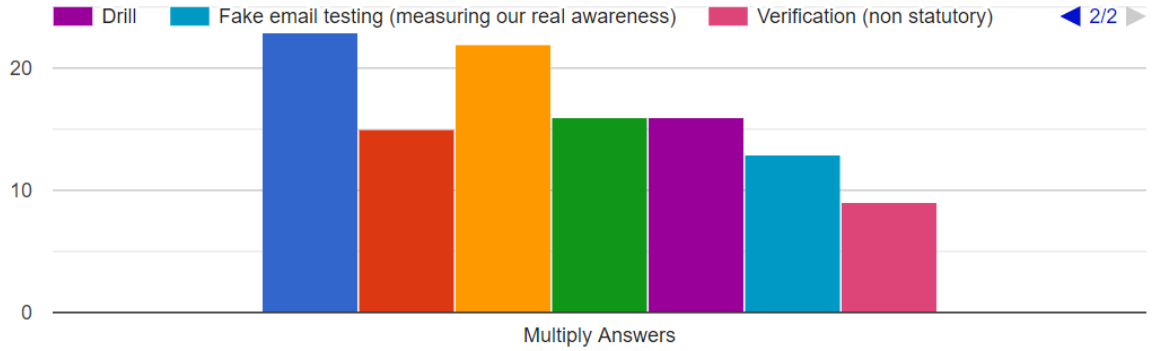
39 απαντήσεις



Από το παραπάνω γράφημα φαίνεται ότι η πλειοψηφία του δείγματος με 22 από τις 39 απαντήσεις σκέφτεται να αποκτήσει πιστοποίηση ISO 2700, οι 11 απάντησαν ότι δεν σκοπεύουν, οι 6 απάντησαν ότι σκοπεύουν ενώ κανένας δεν έχει τέτοια πιστοποίηση ήδη.

17. Για ποιες από τις παρακάτω κατηγορίες θα σας ενδιέφερε να λάβετε εξωτερική υποστήριξη;





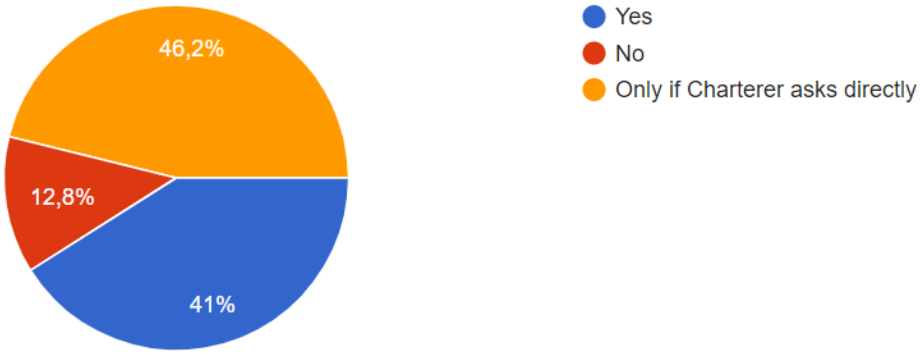
Από την παραπάνω ερώτηση σχετικά με την ενδεχόμενη εξωτερική υποστήριξη και τις κατηγορίες που έχει δικαίωμα να επιλέξει το δείγμα οι απάντηση μπορεί να δοθεί σε περισσότερες από μία επιλογές. Έχουμε λοιπόν σαν αποτέλεσμα:

Α/Α	Κατηγορίες ενδεχόμενης εξωτερικής υποστήριξης	Απαντήσεις
1	GAP ανάλυση σε σχέση με τα πρότυπα (IMO, BIMCO, ISO27001)	23

2	Υποστήριξη προετοιμασίας διαδικασιών.	15
3	TEST διείσδυσης του συστήματος της εταιρείας.	22
4	εκπαίδευση	16
5	Άσκηση (drill)	16
6	Ψευδή δοκιμή μέσω ηλεκτρονικού ταχυδρομείου (μέτρηση της πραγματικής επίγνωσης)	13
7	Επαλήθευση (μη υποχρεωτική)	9

18. Θα χρησιμοποιούσατε εξωτερικές υπηρεσίες περιοδικά (π.χ. ετησίως) για να αποδείξετε καλές επιδόσεις στους ναυλωτές (π.χ. δοκιμές διείσδυσης, ασκήσεις, ψευδείς δοκιμές ηλεκτρονικού ταχυδρομείου);

39 απαντήσεις

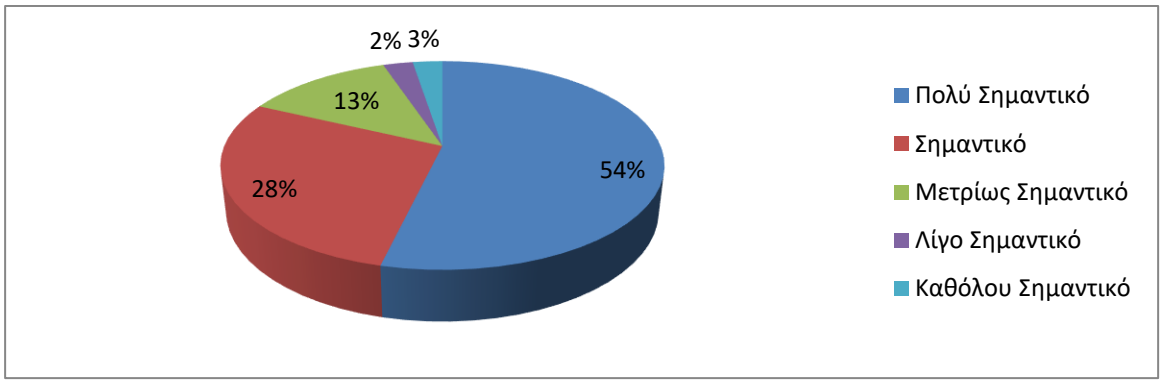


Από το παραπάνω γράφημα προκύπτει ότι στα πλαίσια της απόδειξης καλών επιδόσεων στους ναυλωτές η πλειοψηφία με 18 από τις 39 απαντήσεις του δείγματος απάντησαν ότι θα χρησιμοποιούσαν εξωτερικές υπηρεσίας μόνο εάν τους ζητηθεί απ ευθείας από τον ναυλωτές. Έπειτα οι 16 από τους 39 απάντησαν ναι και τέλος μόνο οι 5 από τους 39 απάντησαν

4.4 Ερωτήσεις σημαντικότητας

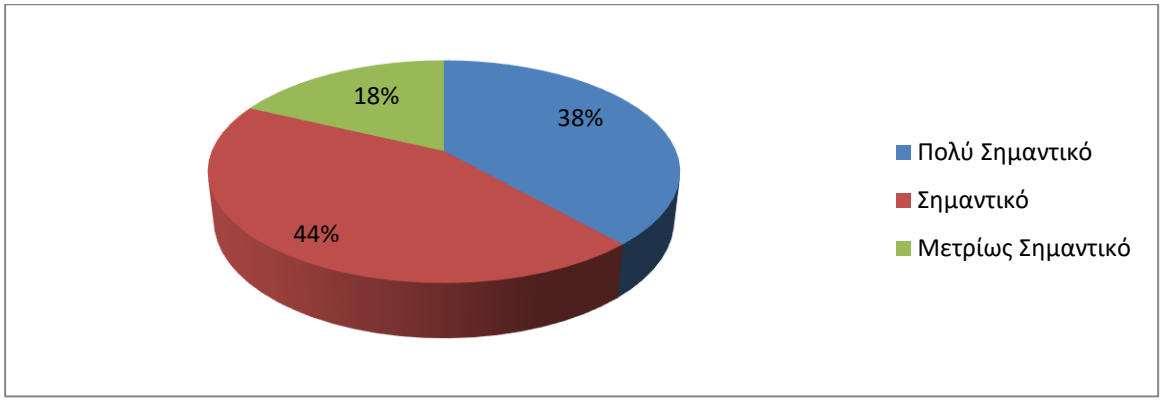
Σε αυτό το μέρος θέτονται στους ερωτηθέντες δώδεκα ερωτήσεις ώστε να επιλέξουν πόσο σημαντικά είναι τα ζητούμενα για την εταιρεία τους. Η απαντήσεις στο σύνολο των ερωτήσεων βασίστηκαν στην κλίμακα Likert, με το 1 να θεωρείται ως «Πολύ Σημαντικό» και το 5 ως «Καθόλου Σημαντικό».

1. **Οι εταιρείες πρέπει να είναι σε θέση να αποδείξουν την τήρηση των εσωτερικών τους διαδικασιών.**



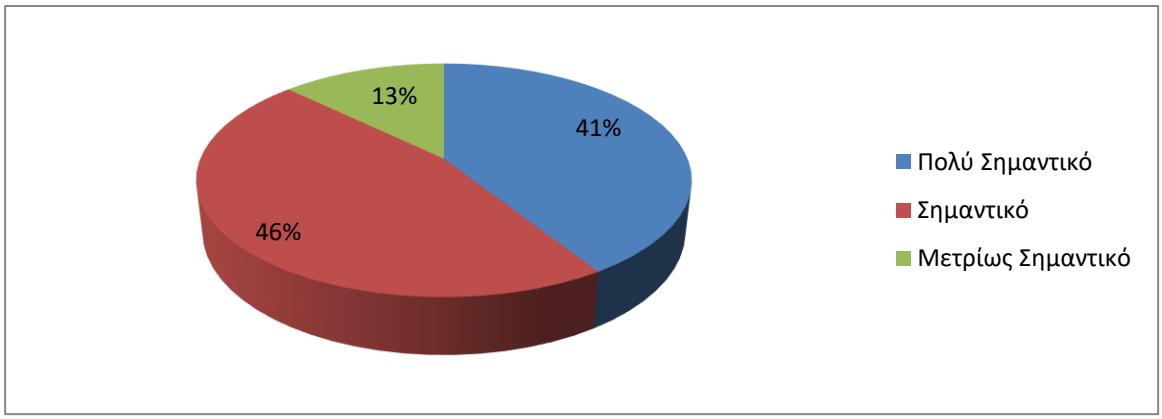
Από το διάγραμμα παρατηρείται ότι η πλειοψηφία των ερωτηθέντων, και συγκεκριμένα 21 από τα 39 άτομα, θεωρεί πολύ σημαντική την ετοιμότητα της εταιρείας ώστε να αποδείξει τις εσωτερικές της διαδικασίες, καθώς και 11 από τους 39, θεωρεί την ετοιμότητα της εταιρείας σημαντική. Ενώ, 7 από τους 39 ερωτηθέντες θεωρούν ότι είναι μετρίως έως και καθόλου σημαντική.

2. **Οι πολιτικές και οι διαδικασίες πρέπει να καταγράφονται και να επανεξετάζονται περιοδικά.**



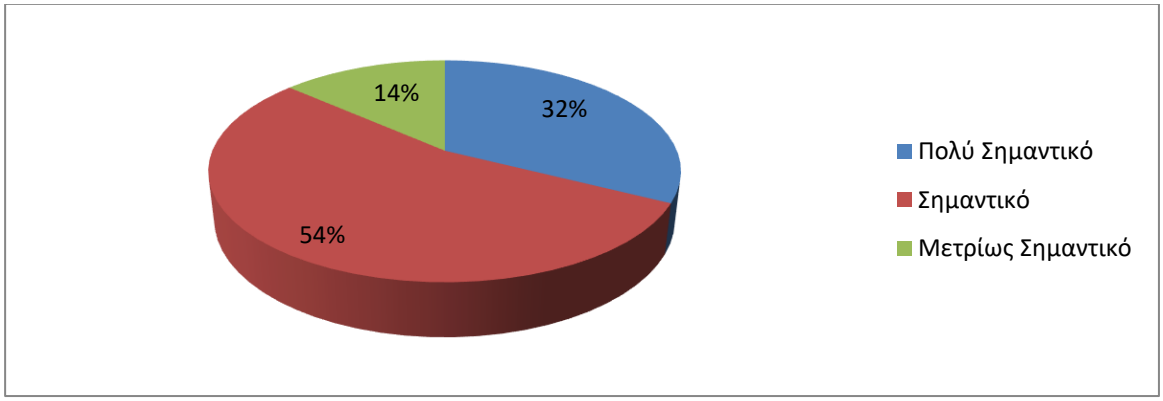
Επιπλέον, όπως παρουσιάζεται και στο διάγραμμα, η μέγιστη πλειοψηφία σε ποσοστό 82,05% (32 από τα 39 άτομα) πιστεύει ότι είναι σημαντικό και πολύ σημαντικό, να καταγράφονται και να επανεξετάζονται περιοδικά οι πολιτικές και οι διαδικασίες της εταιρείας. Το υπόλοιπο 17,95% πιστεύει ότι αυτή η διαδικασία είναι μετρίως σημαντική, ενώ κανείς δεν θεωρεί ότι είναι ασήμαντη.

3. **Το όνομα χρήστη, ο κωδικός, τα USB, και οι φορητοί υπολογιστές πρέπει να είναι διαθέσιμα.**



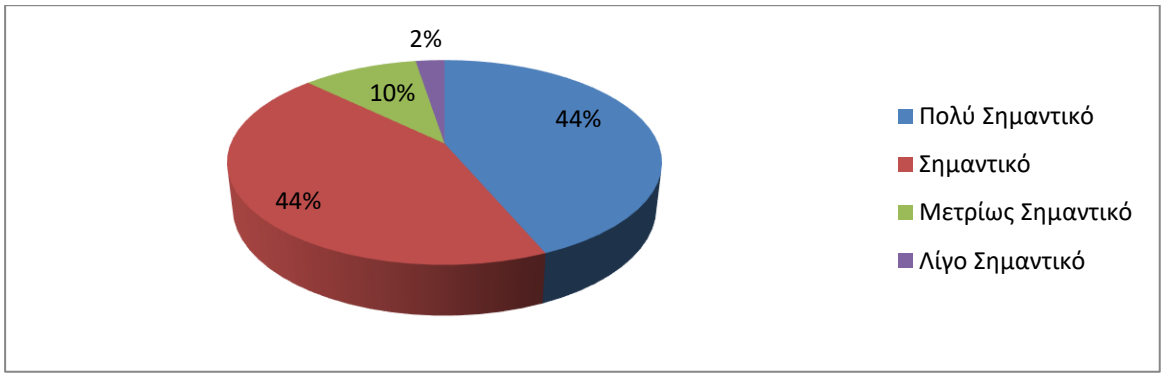
Η μέγιστη πλειοψηφία, με 34 από τους 39 συμμετέχοντες στην έρευνα πιστεύει ότι είναι σημαντικό και πολύ σημαντικό να είναι διαθέσιμο το όνομα χρήστη, ο κωδικός πρόσβασης, τα USB και οι φορητοί υπολογιστές των εταιρειών. Ενώ, μόνο 5 άτομα το θεωρούν μετρίως σημαντικό.

4. **Ταυτοποίηση των αποθηκευμένων και μετάβαση όλων των δεδομένων απορρήτου.**



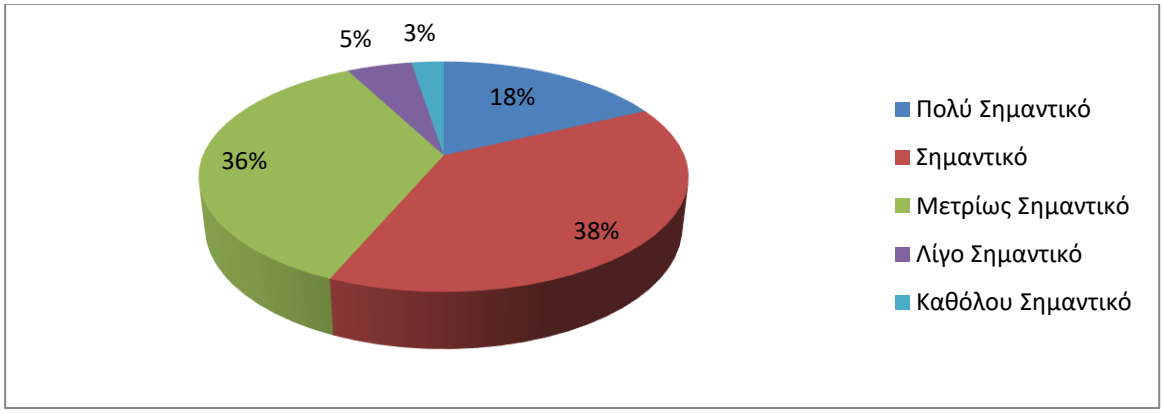
Συνεχίζοντας, και στην περίπτωση της ταυτοποίησης και διάδοσης όλων των δεδομένων απορρήτου, η πλειοψηφία με ποσοστό 82,1% πιστεύει ότι είναι πολύ σημαντικό και σημαντικό. Από την άλλη, ποσοστό της τάξεως του 17,9% θεωρεί ότι η διαδικασία αυτή είναι μετρίως σημαντική, ενώ κανείς από τους συμμετέχοντες δεν την θεωρεί ασήμαντη.

5. **Η απαίτηση συμμόρφωσης με το GDPR πρέπει να είναι σαφής.**



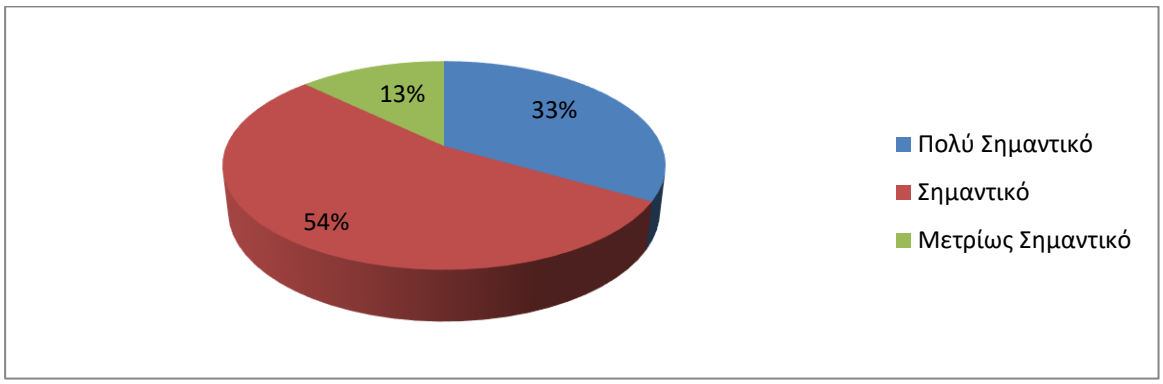
Επιπρόσθετα, πολύ σημαντικό και σημαντικό, αντίστοιχα, θεωρούν 17 από τους 39 συμμετέχοντες (ποσοστό 43,59% έκαστο) την σαφή συμμόρφωση των εταιρειών με το GDPR. Ενώ, το 10,26% και το 2,56% την θεωρούν μετρίως σημαντική και λίγο σημαντική, αντίστοιχα.

6. **Λεπτομέρειες σχετικά με τον έλεγχο τρίτων προμηθευτών, ιδίως για παρόχους πληροφορικής.**



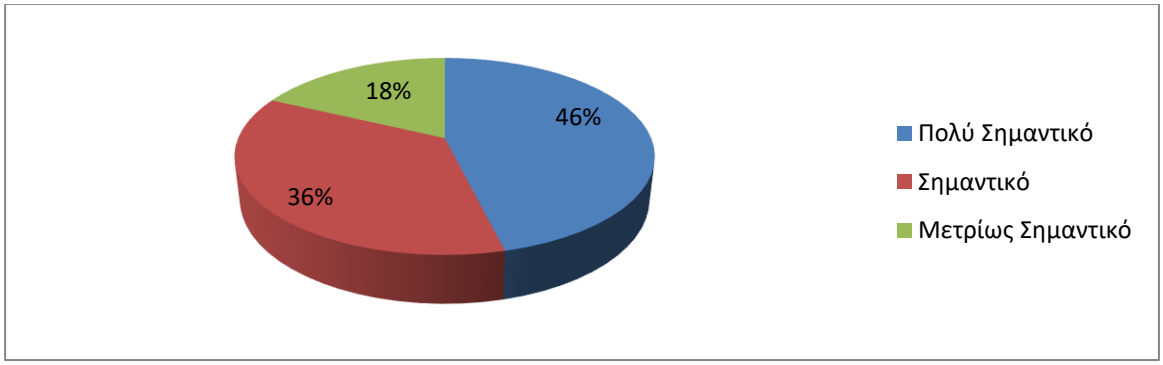
Η ερώτηση σχετίζεται με τον έλεγχο τρίτων προμηθευτών, ιδίως για παρόχους πληροφορικής. Στην περίπτωση αυτή, παρατηρείται ότι η πλειοψηφία με ποσοστό 38,46% θεωρεί ότι είναι σημαντικός ο έλεγχος. Αμέσως μετά ποσοστό της τάξεως του 35,9% θεωρεί τον έλεγχο μετρίως σημαντικό, ενώ το 17,95% πολύ σημαντικό. Τέλος, το 5,13% και το 2,56% θεωρούν ότι ο έλεγχος προς τρίτους προμηθευτές είναι λίγο έως καθόλου σημαντικός, αντίστοιχα.

7. **Κατάλογος συστημάτων πληροφορικής.**



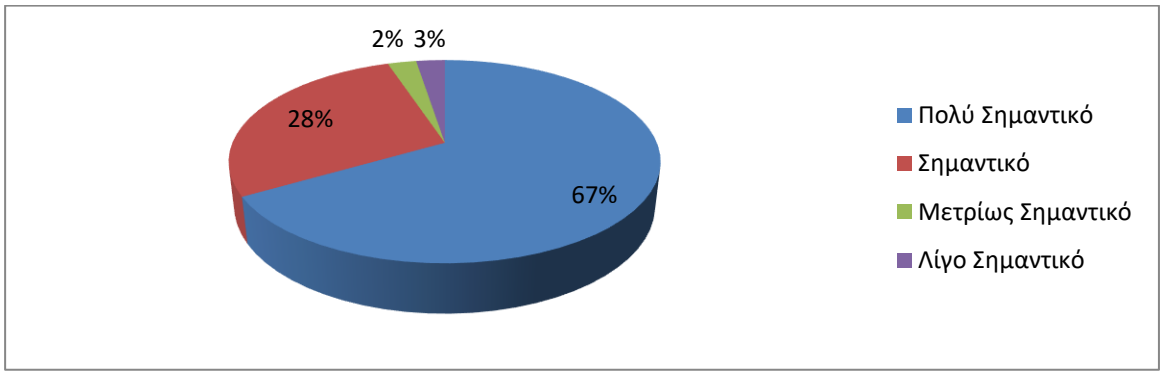
Όσον αφορά την ύπαρξη καταλόγων συστημάτων πληροφορικής, παρατηρείται ότι η πλειοψηφία, δηλαδή 21 άτομα (ποσοστό 53,85%) πιστεύουν ότι είναι σημαντική, καθώς επίσης και 13 άτομα (ποσοστό 33,33%) ότι είναι πολύ σημαντική, ενώ 5 άτομα (ποσοστό 12,82%) ότι η ύπαρξη καταλόγων είναι μετρίως σημαντική.

8. **Λεπτομέρειες σχετικά με την εκπαίδευση του προσωπικού, τόσο του γραφείου όσο και των πλοίων και της συχνότητας.**



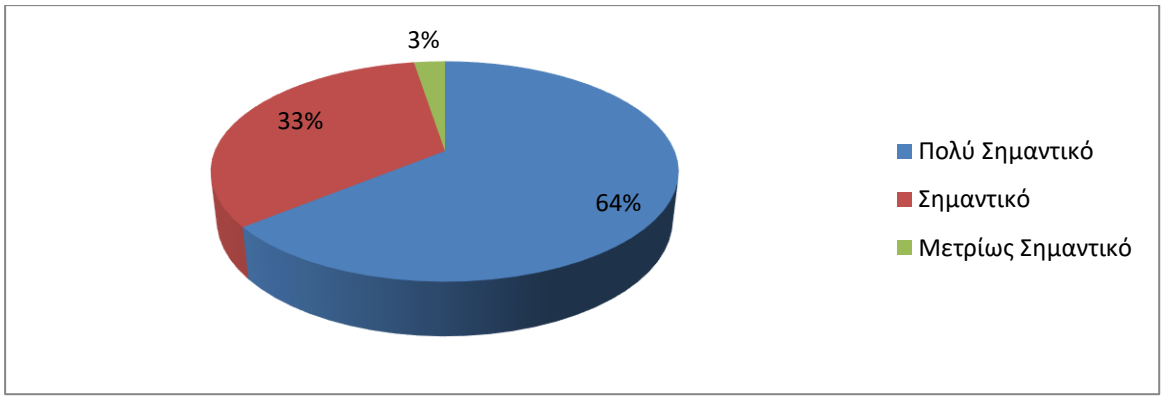
Όσον αφορά την γνώση λεπτομερειών σχετικά με την εκπαίδευση του προσωπικού, όπως φαίνεται και από το διάγραμμα, η πλειοψηφία με ποσοστό 46,15% (18 άτομα) την θεωρούν πολύ σημαντική, ποσοστό της τάξεως του 35,90% (14 άτομα) σημαντική, ενώ ποσοστό της τάξεως του 17,95% (7 άτομα) μετρίως σημαντική. Όπως μπορεί να γίνει αντιληπτό, οι συμμετέχοντες στην έρευνα δεν θεωρούν αυτή την παραδοχή ασήμαντη.

9. **Επιβεβαίωση ότι η Εταιρεία έχει ενημερωμένα τείχη προστασίας και έχει ενημερώσει αυτόματα το λογισμικό προστασίας από ιούς σε όλες τις συσκευές.**



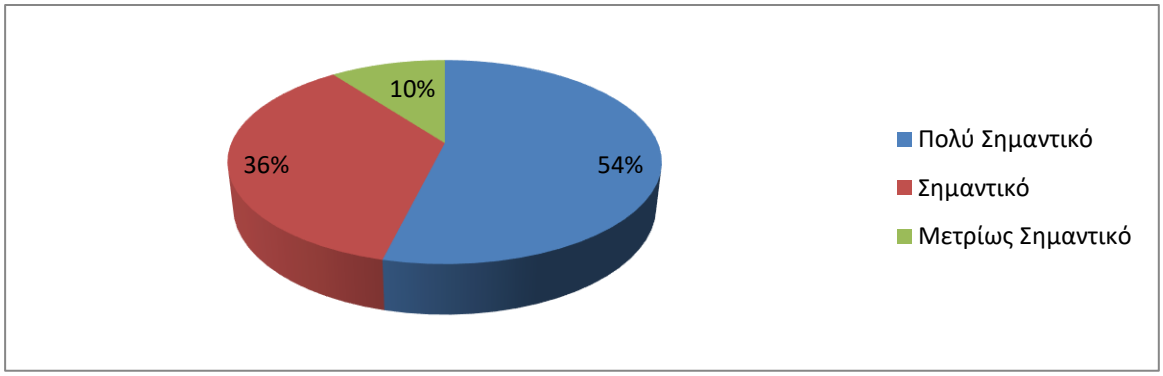
Από το διάγραμμα φαίνεται ότι η συντριπτική πλειοψηφία με ποσοστό 94,88% θεωρεί ότι η επιβεβαίωση ότι η εταιρεία έχει ενημερώσει τα τείχη προστασίας και το λογισμικό της από ιούς σε όλες τις συσκευές της είναι πολύ σημαντική (ποσοστό 66,67%) και σημαντική (28,21%). Ενώ, ποσοστό της τάξεως του 2,56% θεωρεί ότι είναι μετρίως σημαντικό ή λίγο σημαντικό, αντίστοιχα.

10. Ταχεία αντίδραση της εταιρείας σε παραβίαση ή σε περιστατικό στον κυβερνοχώρο. - Σχέδιο αντιμετώπισης περιστατικών.



Συνεχίζοντας, η συντριπτική πλειοψηφία των συμμετεχόντων, 38 άτομα, με ποσοστό 97,43%, πιστεύουν ότι είναι πολύ σημαντικό (25 άτομα – 64,10%) και σημαντικό (13 άτομα – 33,33%) η αντίδραση της εταιρείας σε παραβίαση ή περιστατικό στον κυβερνοχώρο να είναι ταχεία, καθώς και ότι θα πρέπει να υπάρχει σχέδιο αντιμετώπισης τέτοιου είδους περιστατικών. Ενώ, ένα άτομο με ποσοστό 2,56%, θεωρεί ότι η ταχεία αντίδραση της εταιρείας είναι μετρίως σημαντική.

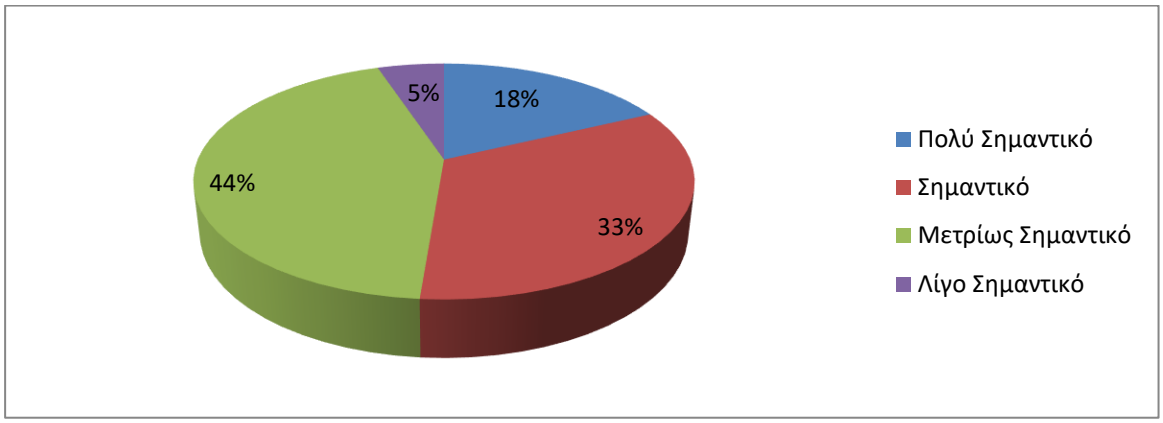
11. Επιβεβαίωση ότι η Εταιρεία έχει τεκμηριωμένο Σχέδιο Συνέχισης Επιχειρήσεων ή Σχέδιο Ανάκαμψης κατά Καταστροφών.



Ακόμη, η πλειοψηφία με ποσοστό 53,85% και 35,90% θεωρεί ότι είναι πολύ σημαντικό και σημαντικό, αντίστοιχα, η εταιρεία να έχει τεκμηριωμένο σχέδιο επιχειρησιακής συνέχειας ή

σχέδιο ανάκαμψης κατά των καταστροφών. Ενώ, οι υπόλοιποι συμμετέχοντες με ποσοστό 10,26% θεωρούν την ύπαρξη των σχεδίων αυτών μετρίως σημαντική.

12. Πώς αξιολογείτε τις αλλαγές που θα επιφέρει η ασφάλεια στον κυβερνοχώρο στον τρόπο με τον οποίο λειτουργεί μια ναυτιλιακή εταιρεία;



Στην τελευταία ερώτηση σχετικά με τις αλλαγές που θα επιφέρει η ασφάλεια στον κυβερνοχώρο στον τρόπο με τον οποίο λειτουργεί μια ναυτιλιακή εταιρεία, το μεγαλύτερο ποσοστό, 43,59%, τις αξιολογεί ως μετρίως σημαντικές. Συνεχίζοντας το ποσοστό της τάξεως του 33,33% τις αξιολογεί ως σημαντικές, καθώς και ως πολύ σημαντικές τις αξιολογεί ένα ποσοστό της τάξεως του 17,95%. Ωστόσο, ποσοστό 5,13% αξιολογεί τις αλλαγές αυτές ως λίγο σημαντικές.

5. Συζήτηση

Το Cyber Security στη ναυτιλία είναι θέμα μείζονος σημασίας και όπως είναι γνωστό θα είναι απαραίτητο να εφαρμόζονται κανονισμοί σχετικά με αυτό σε όλες τις εταιρείες από τον Ιανουάριο του 2021. Γι αυτό λοιπόν διεξήχθη η παρούσα έρευνα. Για να μας δείξει πόσο έτοιμες είναι οι εταιρείες και το προσωπικό τους σε σχέση με το θέμα της κυβερνοασφάλειας. Πιο συγκεκριμένα διερευνήθηκε η εφαρμογή των κανονισμών και των διαδικασιών, η εξέταση των παραγόντων ενδυνάμωσης των συστημάτων διαχείρισης της πληροφορίας που διαθέτουν και τέλος ο τρόπος που διαχειρίζονται πιθανές απειλές για τα συστήματά τους.

Ερευνητικός στόχος 1:	Ερευνητικά Ερωτήματα	Αποτελέσματα
Διαδικασίες που ακολουθούνται για την οργάνωση των ναυτιλιακών εταιρειών σε σχέση με το Cyber security.	**ΕΕ1.1:** Έχει η εταιρεία τεκμηριωμένη πολιτική προστασίας και διαδικασίες σχετικά με τη διαχείριση προσωπικών δεδομένων και ποίος είναι ο διαχειριστής του;	Το 92.3% απάντησε ότι έχει τεκμηριωμένη πολιτική προστασίας δεδομένων και πως γι αυτό είναι υπεύθυνο το IT και το HSQE τμήμα ενώ ένα πολύ μικρό ποσοστό απάντησε πως χρησιμοποιούν εξωτερικές εταιρείες. Επίσης η πλειοψηφία απάντησε πως θεωρούν πολύ σημαντικό να αποδείξουν την ύπαρξη τεκμηριωμένης πολιτικής με ποσοστό 53,85%.
	ΕΕ 1.2: Σημαντικότητα των Guidelines που ακολουθούν οι εταιρείες ώστε να επιτύχουν ασφάλεια στον κυβερνοχώρο.	Θεωρούν ότι είναι σημαντικά. Επίσης είναι έτοιμοι για το TMSA3 με ποσοστό 51,3%. Σχετικά με τις απαιτήσεις του IMO για το Cyber Security, μόλις 9 είναι ήδη προετοιμασμένοι, οι περισσότεροι προγραμματίζουν να προετοιμαστούν μεταξύ 1^{ου} και 2^{ου} τριμήνου του 2020 ενώ 11 στο 2019. Σχετικά με το ISO 27001 η πλειοψηφία απάντησε ότι ίσως και να τους ενδιέφερε με ποσοστό 56,4% (22 άτομα).

Ερευνητικός Στόχος 2:	Ερευνητικά Ερωτήματα	Αποτελέσματα

Εξέταση παραγόντων ενδυνάμωσης συστήματος Cyber Security της εταιρείας.	**ΕΕ2.1:** Εφαρμόζει ενημερωμένες νέες τεχνολογίες και τοίχοι προστασίας Firewall για την αποφυγή απειλών;	Οι εταιρείες εφαρμόζουν ενημερωμένες τεχνολογίες και τοίχοι προστασίας Firewall και αυτό το θεωρούν πολύ σημαντικό ώστε να διασφαλίζεται η ασφάλειά τους στον κυβερνοχώρο με ποσοστό 66,67% (28 άτομα).
	ΕΕ2.2: Πόσο επηρεάζει η εκπαίδευση προσωπικού την ενδυνάμωση του συστήματος Cyber Security της εταιρείας;	Η εκπαίδευση προσωπικού είναι πολύ σημαντικός παράγοντας για την ενδυνάμωση του συστήματος σε μια εταιρεία και αυτό φαίνεται από το ποσοστό των 46,5% (18 άτομα) οι οποίοι απάντησαν ως πολύ σημαντικό και το 35,9% (14 άτομα) ως σημαντικό.
	ΕΕ 2.3: Εφαρμόζουν οι εταιρείες αξιολόγηση και διαχείριση κινδύνων.	Οι εταιρείες εφαρμόζουν αξιολόγηση και διαχείριση κινδύνων με ποσοστό 71,8% (21 άτομα).

Ερευνητικός Στόχος 3: Διερεύνηση επιθέσεων.	**Ερευνητικά Ερωτήματα**	**Αποτελέσματα**
	ΕΕ 3.1: Υπάρχει εμπειρία σε κάποια απειλή για το σύστημα της εταιρείας τα τελευταία τρία χρόνια;	Οι ερωτηθέντες απάντησαν ότι είχαν εμπειρία σε απειλές τα τελευταία τρία χρόνια σε ποσοστό 38,5% (15 άτομα).
	ΕΕ 3.2: Σε ποιο τμήμα παρουσιάζονται οι περισσότερες απειλές και είναι κυρίως φυσικοί ή	Παρουσιάζονται κυρίως απειλές στα Email επικοινωνίας της εταιρείας και του πλοίου. Μέτρια

	ανθρώπινοι;	παρουσιάζονται στο οικονομικό τμήμα και ελάχιστα στα συστήματα διαχείρισης του πλοίου.
	ΕΕ 3.3: Μια απειλή επιφέρει αλλαγές στον τρόπο λειτουργίας μιας εταιρείας;	Η πλειοψηφία εδώ απάντησε μέτρια σημαντική με ποσοστό 43,59% ενώ 33,33% σημαντική και μόλις το 17,95% πολύ σημαντική.

5.1 Σχολιασμός ευρημάτων

Ερευνητικός στόχος 1: Διαδικασίες που ακολουθούνται για την οργάνωση των ναυτιλιακών εταιρειών σε σχέση με το cyber security.

Σχολιασμός: Το 92,3% του πληθυσμού του δείγματος εφαρμόζει στην εταιρεία του τεκμηριωμένη πολιτική προστασίας δεδομένων αναφορικά με το Cyber Security. Η πολιτική αυτή βασίζεται σε κανονισμούς και διαδικασίες που είτε απαραίτητα εφαρμόζονται είτε παίζουν καθοδηγητικό ρόλο. Οι κανονισμοί είναι οι TMSA3, IMO, ISO 27001 κ.α. Η καθοδήγηση των εταιρειών, πραγματοποιείται εσωτερικά σε συνδυασμό κυρίως των τμημάτων IT και HSQE. Αυτό γίνεται από εξειδικευμένο προσωπικό. Επίσης, η πλειοψηφία με ποσοστό 53,85% θεωρεί σημαντικό να μπορεί ανά πάσα στιγμή να αποδείξει την ύπαρξη τεκμηριωμένης πολιτικής σε σχέση με αυτές τις διαδικασίες. Τέλος, εφαρμόζονται ανά τακτά χρονικά διαστήματα αξιολόγηση και διαχείριση κινδύνων.

Ερευνητικός στόχος 2: Εξέταση παραγόντων ενδυνάμωσης συστήματος Cyber Security της εταιρείας.

Σχολιασμός: Οι εταιρείες φροντίζουν να ενδυναμώνουν τα συστήματά τους εφαρμόζοντας ενημερωμένες νέες τεχνολογίες καθώς και τοίχοι προστασίας Firewall και το θεωρούν πολύ σημαντικό ώστε να διασφαλίζουν με αυτόν τον τρόπο την ασφάλεια της εταιρείας στον κυβερνοχώρο με ποσοστό 66.67%. Επίσης, η εκπαίδευση προσωπικού αποτελεί ακόμη έναν παράγοντα ενδυνάμωσης των συστημάτων τους με 14 άτομα να έχουν απαντήσει ότι το

βρίσκουν σημαντικό και 18 πολύ σημαντικό. Τέλος, εφαρμόζουν αξιολόγηση και διαχείριση κινδύνων ώστε να αποφευχθούν τυχόν επιθέσεις με ποσοστό 71.8% (21 άτομα).

Ερευνητικός στόχος 3: Διερεύνηση επιθέσεων.

Σχολιασμός: Οι εταιρίες τα τελευταία τρία χρόνια έχουν παρατηρήσει κυβερνο-επιθέσεις σε ποσοστό 38,5%. Οι απειλές αφορούσαν κυρίως τα email του πλοίου και του γραφείου, λιγότερο το οικονομικό τμήμα της εταιρείας και ελάχιστα τα συστήματα διαχείρισης του πλοίου. Οι αλλαγές που έχουν παρατηρήσει στον τρόπο λειτουργίας της εταιρείας είναι σημαντικές με ποσοστό 51,28% έως μέτρια σημαντικές με ποσοστό 43,59%.

5.2 Τελικά συμπεράσματα

Η ανάπτυξη της τεχνολογίας συνετέλεσε στη δημιουργία ενός ασφαλούς κυβερνοχώρου. Αυτό επιτυγχάνεται με την εκπαίδευση του προσωπικού (Krzysztof Cabaj, Dulce Domingos, Zbigniew Kotulski, Ana Respicio, 2017) και την ενδυνάμωση των συστημάτων σε πλοίο και γραφείο (Hugh Boyes, 2014). Επίσης, οι εταιρείες εφαρμόζουν κανονισμούς οι οποίοι αφορούν τα συστήματα αυτά και ακολουθούν τις κατευθυντήριες οδηγίες της BIMCO ώστε να καλύπτονται ασφαλιστικά και όχι μόνο.

Άλλος ένας σημαντικός παράγοντας σχετικά με την ασφάλεια των πληροφοριών σε μια εταιρεία είναι ο κανονισμός γενικής προστασίας προσωπικών δεδομένων (GDPR). Ο κανονισμός αυτός αφορά, την προστασία της ιδιωτικής ζωής και την ασφάλεια προσωπικών δεδομένων και εφαρμόζεται υποχρεωτικά σε όλα τα κράτη μέλη της ΕΕ από τις 25 Μαΐου 2018 (GDPR, 2018).

Η εποχή των Big Data επιβάλλει ακόμη μεγαλύτερη προστασία σχετικά με το Cyber Security στη ναυτιλία. Αυτό γίνεται για την αποφυγή των περιστατικών πειρατείας στον κυβερνοχώρο και κλοπής σημαντικών δεδομένων για την εταιρεία. Τα συστήματα στα πλοία, χρήζουν προσοχής καθώς είναι ιδιαίτερα ευάλωτα (B. Svilicic – David BrCiC, 2019). Επιπρόσθετα εφαρμόζεται διαχωρισμός των συστημάτων στα πλοία σε IT και OT καθώς το πρώτο αφορά τα συστήματα πληροφορικής και το OT αφορά το υλικό και το λογισμικό που άμεσα παρακολουθεί και ελέγχει φυσικές συσκευές και διαδικασίες.

Το Cyber Security στη ναυτιλία αποτελεί πλέον μέρος του κώδικα ISM και θα εφαρμόζεται υποχρεωτικά από τον Ιανουάριο του 2021. Οι εταιρείες ήδη προετοιμάζονται για αυτό,

δίνοντας μεγάλη προσοχή σε διαδικασίες, κανονισμούς, εκπαιδεύοντας το προσωπικό τους και πραγματοποιώντας δοκιμές διείσδυσης στα συστήματά τους είτε με τη βοήθεια συμβουλευτικών εταιρειών είτε με δικό τους εξειδικευμένο προσωπικό. Οι κανονισμοί που υποχρεωτικά ακολουθούν είναι:

- GDPR
- IMO-MSC
- TMSA 3
- VIQ 7
- IACS
- ISO 27000 προαιρετικά

Από την άλλη πλευρά οι ασφαλιστικές εταιρείες έχουν προχωρήσει αρκετά στο κομμάτι της ασφάλειας του κυβερνοχώρου. Αυτό έχει συμβεί λόγω αύξησης του ενδιαφέροντος από τις ναυτιλιακές εταιρείες. Από την πλευρά των εταιρειών, εάν και εφόσον ακολουθούν τις οδηγίες και τους κανονισμούς, είναι απόλυτα καλυμμένες ασφαλιστικά σε περίπτωση περιστατικού στον κυβερνοχώρο.

Επιπρόσθετα, οι νηογνώμονες, εκτός από την πλευρά των επιθεωρήσεων παίζουν πλέον συμβουλευτικό ρόλο για τις εταιρείες. Αυτό πραγματοποιείται, παρέχοντας υπηρεσίες από εξειδικευμένο προσωπικό ώστε να στήσουν τα συστήματά τους, να εκπαιδεύσουν το προσωπικό τους, να εφαρμόσουν δοκιμές διείσδυσης των συστημάτων τους και τέλος τις αξιολογούν. Από την άλλη, οι εταιρείες εφαρμόζουν κάποιες «άτυπες» διαδικασίες οι οποίες βασίζονται στους κανονισμούς και κοινοποιούνται σε όλους τους εργαζομένους της εταιρείας, σε γραφείο και πλοίο.

Τέλος, το ερευνητικό μέρος αυτής της εργασίας, έθεσε τρείς ερευνητικούς στόχους

1. Διαδικασίες που ακολουθούνται σε σχέση με την οργάνωση των ναυτιλιακών εταιρειών με το Cyber Security.
2. Εξέταση παραγόντων ενδυνάμωσης των συστημάτων τους.
3. Διερεύνηση ευπαθειών.

οι στόχοι αυτοί, αποτελούνταν από κάποια ερευνητικά ερωτήματα. Τα ερωτήματα αυτά απαντήθηκαν με τη χρήση ερωτηματολογίου στα πλαίσια ποσοτικής έρευνας, το οποίο εστάλη ηλεκτρονικά σε στελέχη ναυτιλιακών εταιρειών. Οι απαντήσεις ήταν 39 από τα 80 ερωτηματολόγια του συνόλου. Αναφορικά με το θέμα, οι απαντήσεις ήταν θετικές διότι το μεγαλύτερο ποσοστό των ερωτηθέντων έδειξε ότι εκτός από γνώση του αντικειμένου

έχει και τη θέληση να γίνεται ολοένα και καλύτερο δίνοντας μεγάλη σημασία σε οτιδήποτε σχετίζεται με την κυβερνοασφάλεια. Αυτό συνεπάγεται ότι το Cyber Security έχει μπει για τα καλά στη ναυτιλία και ότι η εξέλιξή του είναι δεδομένη.

5.3 Μελλοντική έρευνα

Η παρούσα έρευνα μπορεί να χαρακτηριστεί σημαντική λόγω της θέσης των ερωτηθέντων και των αποτελεσμάτων των απαντήσεων τα οποία απαντούν στα αρχικά ερωτήματα με θετικά για το θέμα αποτελέσματα. Ωστόσο, φαίνεται η ανάγκη του ναυτιλιακού κλάδου για συνεχή αναζήτηση και ενημέρωση πάνω στο θέμα της ασφάλειας του κυβερνοχώρου. Πιο συγκεκριμένα, οι εταιρείες παρόλο που είναι πολύ καλά ενημερωμένες σχετικά με τις διαδικασίες και τους κανονισμούς, δεν είναι 100% προετοιμασμένες και δεν συμμορφώνονται απόλυτα με τους κανονισμούς οι οποίοι σε λίγο καιρό θα είναι υποχρεωτικοί. Παρόλα αυτά, έχουν διάθεση να το κάνουν σχετικά σύντομα.

Σε μια μελλοντική έρευνα θα ήταν καλό να απευθυνθούμε ξανά σε ναυτιλιακά στελέχη πραγματοποιώντας ποσοτική έρευνα ώστε να δούμε την ετοιμότητά τους σε σχέση με τους κανονισμούς όταν αυτοί τεθούν υποχρεωτικοί και παράλληλα να πραγματοποιηθεί μια ποιοτική έρευνα με τη χρήση συνεντεύξεων ή ομαδικών συνεντεύξεων τύπου group. Στη συνέχεια, θα γίνει τριγωνοποίηση των αποτελεσμάτων και θα δούμε εάν αυτά τα δύο αποτελέσματα συμφωνούν μεταξύ τους. Με τον τρόπο αυτό η άποψη θα είναι πιο συγκεκριμένη σχετικά με την κυβερνοασφάλεια στη ναυτιλία, θα καταγραφούν οι απαντήσεις και οι συμπεριφορές των ανθρώπων ως προς την ετοιμότητα και θα κατανοήσουμε τις ανάγκες τους.

6. Βιβλιογραφία

Βιβλία:

[1] Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, "*Cyber Security Policy Guidebook*", 2012.

[2] Kenneth J. Knapp, "*Cyber security and Information Assurance*", 2009.

[3] James Graham – Richard Howard – Ryan Olson, "*Cyber Security Essentials*", 2011.

[4] Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts. "*Issues in Maritime Cyber Security*", 2017.

[5] John G.Voeller, "*Cyber Security*", 2014.

[6] Cohen L., Manion L., (1994). "*Μεθοδολογία εκπαιδευτικής έρευνας*". Αθήνα: Μεταίχμιο.

[7] Δημητρόπουλος Ε., (2004). "*Εισαγωγή στη μεθοδολογία της επιστημονικής έρευνας*". Αθήνα: ΕΛΛΗΝ.

[8] Κυριαζόπουλος Π. και Σαμαντά Ε. (2011). "*Μεθοδολογία έρευνας εκπόνησης διπλωματικών εργασιών*" Αθήνα: Σύγχρονη Εκδοτική.

[9] Νόβα–Καλτσούνη, Χ. (2006). "*Μεθοδολογία εμπειρικής έρευνας στις κοινωνικές επιστήμες: ανάλυση δεδομένων με τη χρήση του SPSS 13*". Αθήνα: Gutenberg.

Επιστημονικά Άρθρα:

[1] Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg , Jon Shamah , Sławomir Górniak "*Definition of Cybersecurity – Gaps and overlaps in standardisation*" – ENISA, December 2015.

[2] Dan Cimpean, Johan Meire, Vincent Bouckaert, Stijn Vande Casteele, Aurore Pelle, Luc Hellebooge "*ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR"* ENISA, November 2011

[3] DNVGL AS, "*Cyber security resilience management for ships and mobile offshore units in operation*", September 2016.

[4] DLA Piper "*GDPR Data Breach Survey*" A report by DLA Piper's cybersecurity team, February 2019.

[5] *Cyber Security Culture in organizations*, ENISA November 2017. www.enisa.europa.eu

[6] B. Svilicic, David BrCiC, "*Raising Awareness on Cyber Security Of ECDIS*", March 2019.

[7] Huge Boyes, "*Maritime Cyber Security- Securing the Digital Seaways*". January 2014.

[8] Krzysztof Cabaj, Dulce Domingos, Zbigniew Kotulski, Ana Respicio, "*Cybersecurity education: Evolution of the discipline and analysis of master programs*", January 2018.

[9] Kimberly Tam, Kevin Jones, Maria Papadaki, "*Threats and Impacts in Maritime Cyber Security*", January 2012.

[10] Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, "*Improving cyber security awareness in maritime transport: A way forward*", October 2017.

[11] Thiago Alves, Rishabh Das, Aaron Werth, Thomas Morris " *Virtualization of SCADA testbeds for cybersecurity research: A modular approach*" , May 2018.

[12] Ivo Friedberg, Kieran McLaughlin, Paul Smith, David Laverty, Sakir Sezer "*STPA-SafeSec: Safety and security analysis for cyber-physical systems*", June 2016.

[13] Nick Ridle, Stephen Wares, "*The Risk of Cyber Attack to the Maritime Sector"*, July 2014.

[14] Kimberly Tam, Kevin Jones, " *Factors Affecting Cyber Risk in Maritime*", June 2019.

[15] Kimberly Tam, Kevin Jones, "*Forensic Readiness within Maritime Sector*". June 2019.

Κανονισμοί:

[1] IMO - ANNEX 10: RESOLUTION MSC.428(98), "*MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS*", 16 June 2017. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf

[2] IMO – "*ISM Code and Guidelines on Implementation of the ISM Code"* http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx

[3] IMO – "*Maritime cyber risk"* - MSC-FAL.1/Circ.3, 5 July 2017 http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

[4] INTERNATIONAL STANDARD ISO/IEC 27001:2016 4th edition 2016-02-15 http://mahdi.hashemitabar.com/cms/images/Download/ISO/iso-iec-27000-2016-english.pdf

[5] IACS- "*Recommendations on Cyber Safety Mark Step change of Cyber Security resilient"*, http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-change-in-delivery-of-cyber-resilient-ships/

[6] TMSA 3 - TMSA 3- "*MARITIME SECURITY – ELEMENT 13"* VERSION 2017

[7] VIQ version 7.0.05, 2019

[8] BIMCO - ICS CS ON BOARD SHIPS

"*The guideline on cyber security on board ships v.3*" (Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL) http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

[9] GDPR - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 https://gdpr-info.eu/

[10] GDPR - Communication from the Commission to the European Parliament and the Council Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018 - https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf

[11] IMO No:9288447 Cyber Security Management Plan. DNVGL

[12] CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES – ABS

[13] CYBER SECURITY SOLUTIONS FOR INDUSTRY – BUREAU VERITAS

[14] Cyber security resilience management for ships and mobile offshore units in operation – DNVGL, September 2016

[15] Cyber security Advanced Solution – ABS.

Ιστός:

[1] Ευρωπαϊκή Ένωση
https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf

[2] Lexico powered by oxford
http://www.oxforddictionaries.com/definition/english/cybersecurity?q=cyber+security

[3] http://www.merriam-webster.com/dictionary/cybersecurity

[4] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[5] https://www.iso.org/isoiec-jtc-1.html

[6]Institute Cyber Attack Exclusion Clause – CL. 380, 2003
https://www.modernaforsakringar.se/siteassets/documents/foretag--industri/villkorsbanken/foretagsforsakring/allmanna-villkor/transport/institute-cyber-attack-exclusion-clause---cl-380-vst-24-1-.pdf

[7] European Union -Μεταρρύθμιση των κανόνων της ΕΕ για την προστασία των δεδομένων το 2018 https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_el

[8] IBM, X-Force Threat Intelligence Index, 2017.
https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf

[9] Singapore's Operational Technology Cybersecurity Masterplan 2019 https://www.csa.gov.sg/~/media/csa/documents/publications/ot_masterplan/otcybersecuritymasterplan.pdf

[10] Maersk shipping Reports $300M Loss Stemming from NotPetya Attack https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/ , 10 July 2017.

[11] Allianz - Q&A: Cyber risk on the rise in shipping
https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-risk-on-the-rise-in-shipping.html

[12] Marsh - The Risk of Cyber Attack to the Maritime Sector
https://www.marsh.com/uk/insights/research/the-risk-of-cyber-attack-to-the-maritime-sector.html

[13] Beazley Launches Affirmative Marine Cyber Cover
https://www.insurancejournal.com/news/international/2019/05/15/526480.htm

[14] Plymouth University
https://www.plymouth.ac.uk/research/maritime-cyber-threats-research-group/publications-news-and-talks

[15] Pen Ten Partners
https://www.pentestpartners.com/penetration-testing-services/maritime-cyber-security-testing/

[16] LR
https://www.lr.org/en/bimco-guidelines/

[17] LR
https://www.lr.org/en/cyber-security/