Jimmy Kåla

VERKKO-OPINTOJAKSO MERENKULUN KYBERUHKIEN HALLINNAN ITSEOPISKELUUN

Merenkulun koulutusohjelma

2019

samk

Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VERKKO-OPINTOJAKSO MERENKULUN KYBERUHKIEN HALLINNAN ITSEOPISKELUUN

Kåla, Jimmy
Satakunnan ammattikorkeakoulu
Merenkulun insinöörin koulutusohjelma

Helmikuu 2019
Ohjaaja: Ahvenjärvi, Sauli
Sivumäärä: 18
Liitteet: 11
Avainsanat: merenkulku, koulutus, verkko-opinto, kyberturvallisuus

TIIVISTELMÄ

Tämän opinnäytetyön tarkoitus oli luoda verkko-opintoina toteutettava opintojakso merenkulun kyberuhkien hallitsemisesta. Opinnäytetyö toteutettiin Satakunnan Ammattikorkeakoululle yksilötyönä.

Luodun opintojakson lähteenä käytettiin mahdollisimman uusia, alan eri organisaatioiden julkaisuja, uutisartikkeleita, sekä videoita. Koska aihe käsittelee hyvin nopeasti kehittyvää teknologista ympäristöä, kirjoja ei käytetty lähteinä.

Opintojakson valmistuttua ryhmälle opiskelijoita annettiin tehtäväksi suorittaa opintojakso, ja antaa siitä palautetta mahdollisia parannuksia varten.

Palautteesta ei kuitenkaan ilmennyt selvää yhtenäistä viestiä mistään muutosta kaipaavasta tekijästä, joten opintojaksoa ei muutettu alkuperäisestä muodostaan.

MAKING OF AN ONLINE COURSE FOR HANDLING OF CYBER THREATS IN SEAFARING MANAGEMENT

Kåla, Jimmy
Satakunta University of Applied Sciences
Degree Programme in Marine Engineering

February 2019
Supervisor: Ahvenjärvi, Sauli
Number of pages: 18
Appendices: 11
Keywords: seafaring, education, online course, cyber security

ABSTRACT

The purpose of this thesis was to create an online unit about controlling the cyber threats that seafaring is facing. The thesis was produced for Satakunta University of Applied Sciences as an individual piece of work.

The sources used for the thesis consist of different publications from organizations within the field, as well as news articles and videos, all as contemporary as possible. Because of the rapidly changing nature of this topic, books were not used as a source of information for this thesis.

Upon completion of the online unit, it was given to a group of students to complete, and they were asked to give feedback after completing the unit in order to facilitate pedagogical improvements.

The feedback did not yield any clear unanimous message regarding need for change of the content of the unit, and therefore no change was made to the unit content.

SISÄLLYS

TERMIT JA LYHENTEET

Moodle	verkko-oppimisympäristö
SAMK	Satakunnan ammattikorkeakoulu
DDoS	Distributed Denial of Service (verkkohyökkäys)
DoS	Denial of Service (verkkohyökkäys)
BBC	British Broadcasting Corporation
Maersk/Maersk Line	monialayritys, muun muassa varustamo
Petya/Notpetya	haittaohjelma
CNBC	Consumer News and Business Channel
IAMU	International Association of Maritime Universities
IMO	International Maritime Organization
YK	Yhdistyneet Kansakunnat
Quiz	visailu/koe
Assignment	tehtävä/toimeksianto
Questionnaire	kyselylomake

1. JOHDANTO

Tämä opinnäytetyö tehtiin Satakunnan ammattikorkeakoululle, osana kansainvälistä projektia kyberturvallisuuden huomioimisesta merenkulun koulutuksessa. Satakunnan ammattikorkeakoulu toimii satakunnan alueella, ja yksi sen opintotarjonnan vaihtoehdoista on merenkulun opiskeleminen. Kyberturvallisuuden merkitys merenkulussa on viime vuosina kasvanut voimakkaasti. Merenkulun koulutusohjelmissa kyseistä asiaa ei kuitenkaan ole tähän mennessä käsitelty juuri lainkaan.

Opinnäytetyön tarkoituksena oli laatia opintojakso merenkulun kyberuhkien hallitsemisesta Satakunnan ammattikorkeakoulun tulevia merenkulun opiskelijoita varten. Opintojakso toteutettiin Satakunnan ammattikorkeakoulun käyttämällä Moodle -verkko-oppimisalustalla. Opintojakso suunniteltiin suoritettavaksi täysin verkossa, ilman kontaktitunteja.

Opintojaksoon kuuluu materiaalia teksti-, kuva-, ja videomuodossa, jonka omaksuminen arvioidaan monivalintakysymyksillä sekä lyhyen esseen kirjoittamisella.

2. SATAKUNNAN AMMATTIKORKEAKOULU

Satakunnan ammattikorkeakoulu (SAMK) on ammattikorkeakoulu joka toimii Satakunnan alueella. SAMK toimii Porissa, Raumalla, Kankaanpäässä ja Kuninkaisissa. Opiskelijoita on noin 6000 ja työntekijöitä noin 400. SAMK:n koulutus- ja tutkimustoiminta jakaantuu neljään osaamisalueeseen: hyvinvointi ja terveys, logistiikka ja meriteknologia, palveluliiketoiminta sekä teknologia. Merenkulun koulutusyksikkö sijaitsee Raumalla, ja koulutusohjelmiin kuuluu sekä kansipäällystön että konepäällystön koulutusohjelmat. Kansipäällystön koulutusohjelma on suomen kielen lisäksi suoritettavissa myös englanniksi. (SAMK:n www-sivut 2017.)

3. KYBERTURVALLISUUS

3.1 Kyberturvallisuuden määritelmä

Termi kyberturvallisuus voidaan määrittää seuraavasti: se tarkoittaa kootusti kaikkia työkaluja, käytäntöjä, tietoturvan konsepteja ja suojia, suuntaviivoja, riskienhallinnan lähestymistapoja, toimenpiteitä, suositeltuja toimintatapoja, sekä teknologiaa ja koulutusta joilla voidaan suojella kyberympäristöä, sekä jonkun organisaation tai henkilön digitaalisessa muodossa olevaa tietoa. (Boyes, H & Isbell, R. 2017, 15.)

Kyberympäristöllä tarkoitetaan toisiinsa yhteen kytkettyjä, tietoliikenne- sekä operatiivisia laitteita jotka hyödyntävät elektronisia, tietokoneisiin ja tietokonejärjestelmiin sekä langattomiin järjestelmiin perustuvia ratkaisuja joiden tehtävä on lähinnä tiedonsiirron tehostaminen. Tiedonsiirron tehostaminen säästää yksityishenkilöltä aikaa, sekä parantaa epäsuoraan yrityksen kannattavuutta, ja voi joissakin tapauksissa mahdollistaa asiakkaalle matalamman hinnan. Laivaympäristössä kyberympäristö koostuu esimerkiksi kannettavista- sekä pöytätietokoneista, erilaisista tietoverkkolaitteista, sekä tietoverkkoihin kytketyistä operatiivisista laitteista kuten esimerkiksi ohjauslaitteista, antureista ja tutkasta. (Boyes, H & Isbell, R. 2017, 15.)

3.2 Merenkulkuun kohdistuvat kyberuhat

Tavallisimmat merenkulkuun kohdistuvat kyberuhat voidaan jakaa kahteen pääkategoriaan, nimittäin ei-kohdennettuihin ja kohdennettuihin. Ei-kohdennetut hyökkäykset ovat usein suunniteltuja aiheuttamaan harmia mahdollisimman monelle organisaatiolle ja henkilölle, kun taas kohdennetut hyökkäykset pyrkivät häiritsemään yhden valitun organisaation tai henkilön toimintaa. (BIMCO. 2016, 3.)

Ei-kohdennetut hyökkäykset ovat usein suhteellisen alkeellisia rakenteeltaan, ja käyttävät suhteellisen yksinkertaisia työkaluja murtaakseen kohteen tietoturvasuojat. Tavallisimmat ei-kohdennetun hyökkäyksen uhat ovat:

- **Social Engineering.** Tämä toimintatapa koostuu kyberhyökkääjien yrityksistä ylipuhua organisaatiolle työskenteleviä henkilöitä rikkomaan tietoturvakäytäntöjään, jotta hyökkäyksen toteuttaminen helpottuisi. Sosiaalinen media toimii usein hyökkääjien työkaluna tässä toimintatavassa.
- **Phishing.** Hyökkääjät lähettävät suuria määriä sähköposteja satunnaisille vastaanottajille, joilta yritetään huijata esimerkiksi käyttäjätunnuksia ja salasanoja, luottokorttitietoja tai muuta vastaavaa. Sähköpostit noudattavat monesti tiettyä kaavaa. Viestissä voi esimerkiksi lukea että sen on lähettänyt henkilön esimies, siinä esitetään erilaisia uhkakuvia siitä, mitä kaikkea negatiivista voi tapahtua mikäli tietoja ei luovuteta. Usein viestissä myös vedotaan siihen että asia on kiireellinen, jotta vastaanottaja ei lähtisi selvittämään viestin alkuperää tarkemmin.
- **Water holing.** Perustuu olemassa olevan verkkosivun ulkonäön muuttamiseen, tai kokonaan uuden sivun luomiseen, joka kuitenkin näyttää alkuperäiseltä sivulta. Kun esimerkiksi yrityksen työntekijä menee sivulle ja luulee täyttävänsä käyttäjänimensä ja salasanansa niille tarkoitettuihin kenttiin kirjautumista varten, hän antaakin tiedot hyökkääjille.
- **Ransomware.** Tietokoneohjelma joka tunkeutuu käyttäjän tietokoneeseen ja estää käyttäjältä pääsyn tiedon luo, kunnes hän on maksanut lunnasrahan. Lunnaitten maksamista ei suositella, sillä se lisää tämän kaltaisen rikollisuuden houkuttelevuutta. Lisäksi ei ole mitään taetta siitä, että tiedot vapautetaan lunnaitten maksun jälkeen.
- **Scanning.** Menetelmä joka satunnaisesti ohjaa hyökkäyksiä kohti laajoja osia internetistä. (BIMCO. 2016, 4.)

Kohdennetut hyökkäykset ovat usein monimutkaisempia ja paremmin suunniteltuja kuin ei-kohdennetut. Koska ne ovat suunniteltuja vahingoittamaan tiettyä henkilöä tai organisaatiota, tai merenkulusta puheen ollen mahdollisesti tiettyä alusta, ne saattavat käyttää hyväkseen varta vasten kohteilleen suunniteltuja menetelmiä saavuttaakseen päämääränsä. Esimerkkejä kohdennetuista hyökkäyksistä ovat:

- **Spear-phishing.** Hienostuneempi versio phishing-menetelmästä, jossa vastaanottajille lähetetään yksilöllisiä sähköposteja. Tämäntyyppiset sähköpostit sisältävät usein haittaohjelmia joko suoraan, tai linkkien takana jotka automaattisesti lataavat haittaohjelmat tietokoneelle mikäli käyttäjä klikkaa linkkiä. (BIMCO. 2016, 4.)

- **Botnettien käyttö.** Botnetti on ryhmä laitteita jotka ovat internetin kautta yhteen kytkettyjä, ja jotka ohjataan hyökkäämään samanaikaisesti tiettyä verkkosivustoa kohti, jonka seurauksena kyseinen sivusto ylikuormittuu ja lakkaa toimimasta normaalisti. Mikäli laitteet kohdistetaan hyökkäämään palvelimeen, ne voivat aiheuttaa kymmenien verkkosivujen samanaikaisen kaatumisen. Tämäntyyppisistä hyökkäyksistä käytetään nimitystä ”Distributed Denial of Service” (DDoS) -hyökkäys. DDoS-hyökkäystä ei tule sekoittaa vähemmän tehokkaaseen ”Denial of Service” (DoS) -hyökkäykseen, jossa yksi tietty tietokone hyökkää yhdelle tietylle verkkosivulle. (IoT Business News-sivuston www-sivut 2019.)
- **Toimitusketjun horjuuttaminen.** Tämä tarkoittaa kohteelle toimitettavan ohjelmiston, ohjelmistopäivityksen, tai laitteiston tartuttamista haittaohjelmalla. (BIMCO. 2016, 4).

3.3 Uhkien takana olevat henkilöt ja ryhmät

Kyberhyökkäysten takaa voi löytyä monenlaisia eri henkilöitä tai ryhmiä, joilla kaikilla saattaa olla erilaiset intressit. Tavallisimmat kyberhyökkääjät ja heidän motiivinsa ovat:

- **Kyberympäristön väärinkäyttö.** Tällaiset hyökkäykset ovat usein suhteellisen alkeellisten hakkereiden, tai jopa organisaation omien tyytymättömien työntekijöiden aikaansaannoksia. Joitakin hakkereita motivoi pelkkä tietoturvasuojan murtamisen haaste.
- **Aktivistiryhmät.** Ryhmät saattavat hakkeroimalla esimerkiksi hakea huomiota ajamalleen asialle. He voivat esimerkiksi vastustaa tiettyjen lastien kuljettamista tietyillä merialueilla. Tavallisimpia kohteita ovat laivat, laivan omistajat ja operaattorit, lastin vastaanottajat, tai joku muu toimitusketjun toimija.

- **Vakoilijat.** Vakoilijat pyrkivät pääsemään käsiksi salattuihin tietoihin joko nationalististen intressien takia, tai luodakseen kilpailuetua itselleen tai jollekin taholle joka on maksanut vakoilijalle tietojen hankkimisesta.
- **Järjestäytynyt rikollisuus.** Esimerkkinä hakkerit jotka tekevät yhteistyötä merirosvojen kanssa. Mikäli hakkerit voivat murtautua jonkun varustamon logistiikanhallinnan ohjelmaan, he saattavat pystyä päättelemään missä jokin laiva tulee sijaitsemaan tiettynä aikana, ja täten helpottaa laivaan kohdistuvan fyysisen hyökkäyksen toteuttamista. Fyysisen hyökkäyksen tarkoitus voi olla esimerkiksi arvokkaan lastin varastaminen, tai miehistön kidnappaus jota seuraa lunnasvaatimus.
- **Terrorismi.** Esimerkkinä modernin aluksen ”etä-kaappaaminen”, eli aluksen ohjaus- ja propulsiojärjestelmien hallinnan kaappaaminen maista käsin. Aluksen hallinnan menettäminen levittää pelkoa ihmisissä. Tämä menetelmä toimii parhaiten mikäli kohteena on matkustaja-alus.
- **Sodankäynti.** Kansallisvaltio voi ollessaan aseellisessa konfliktissa muun valtion kanssa haluta suorittaa jonkin sortin vakoilua, tai vahingoittaa vihollisen alusten operatiivista tekniikkaa, päämääränään vihollisen logistiikan häirintä. (Boyes, H & Isbell, R. 2017, 16.)

3.4 Kyberturvallisuus arjessa ja tarve koulutuksen lisäämiselle aiheesta

Kyberturvallisuus on ollut osa miltei kaikkien yritysten arkipäivää jo monen vuoden ajan. Jostain syystä monet varustamot ovat kuitenkin vasta hiljattain heränneet kyberuhkien vakavuuteen, jotkut niistä vasta kun kyber-isku on jo toteutunut. (BBC:n www-sivut 2017.)

Esimerkiksi vuonna 2017, maailman suurimpiin varustamoihin kuuluva Maersk Line joutui kyberhyökkäyksen kohteeksi. Hyökkäyksen aiheutti haittaohjelma josta myöhemmin uutisoinnissa käytettiin nimeä NotPetya, ja se aiheutti Maerskille arviolta noin 200-300 miljoonan yhdysvaltain dollarin taloudellisen vahingon menetetyissä tuloissa mitattuna (CNBC:n www-sivut 2017.)

Tästä huolimatta kyberturvallisuutta ei ole merenkulun koulutusohjelmissa käsitelty juuri lainkaan. Tästä syntyi tarve opintojakson luomiseen, joka käsittelisi kyberturvallisuutta, ja antaisi opiskelijoille tarvittavat valmiudet toimia tulevissa ammateissaan turvallisesti ja osaavasti, myös kyberturvallisuuden näkökulmasta.

4. OPINTOJAKSO

4.1 Opintojakson taustaa

Opintojaksosta tehtiin täysin englanninkielinen. Tähän oli kolme keskeistä syytä:

1. Koska Samk:ssa voi opiskella kansipäällystön opetusohjelman myös englanniksi.
2. Kyberturvallisuudesta puhuttaessa on olemassa useita englanninkielisiä termejä.
3. Opintojakson luominen oli osa suurempaa kansainvälistä International Association of Maritime Universities (IAMU) -järjestön rahoittamaa CYMET-projektia, jossa käsitellään kyberturvallisuutta merenkulun koulutuksessa (SAMK:n www-sivut 2017.)

Laatimalla opintojakso täysin englanniksi taattiin että opintojaksoa voidaan käyttää myös englanninkielisessä kansipäällystön opetusohjelmassa. Opetusohjelman laajuus on 270 opintopistettä, eli sama kuin vastaavan suomenkielisen.

Kaikille englanninkielisille kyberturvallisuudessa ja myös laajemmin tietotekniikassa käytetyille termeille ei välttämättä löydy suomenkielistä käännöstä. Täten täysin englanninkielisellä opintojaksolla säästyttiin liialliselta termien selittelyltä.

Samk kuuluu kansainväliseen järjestöön nimeltä International Association of Maritime Universities (IAMU). Tämän järjestön perustivat vuonna 1999 seitsemän eri merenkulun korkeakoulua eri puolilta maailmaa. Järjestön tarkoituksena on yhteistyön kautta tuoda esille merenkulun koulutuksen tärkeyttä nopeasti muuttuvassa ja globalisoituvassa maailmassa. Nykyään järjestöön kuuluu yli 60 merenkulun korkeakoulua. (IAMU:n www-sivut 2018.)

IAMU toimii myös koulutuksen edustajana International Maritime Organization (IMO) järjestössä, joka on YK:n alainen merenkulun kattojärjestö. (SAMK:n www-sivut 2017).

Tämä opinnäytetyöprosessi sai alkunsa lokakuussa 2017, kun IAMU piti vuosikokouksen Varnassa, Bulgariassa. Vuosikokous hyväksyi projektiohjelmaan vuodeksi 2019 SAMK:n hakemuksen tehdä tutkimus aiheesta “Addressing Cyber Security in Maritime Education and Training”. Projektin vetovastuu on SAMK:lla, mutta projektiin osallistuvat myös muun muassa Puolalainen Gdynia Maritime University, sekä Tanskalainen Svendborg International Maritime Academy. (SAMK:n www-sivut 2017.)

4.2 Opintojakson rakenne

Kun opintojaksoa ryhdyttiin suunnittelemaan, pohdittiin ensin *mitä opiskelijoiden tarvitsisi osata.*

Opintojaksoon käytettiin lähteinä lähinnä eri merenkulun organisaatioiden aiheesta kertovia, mahdollisimman ajankohtaisia julkaisuja, ja niistä saatua tietoa suodatettiin niin, että opintojaksoon päätyvä tieto vastaisi mahdollisimman hyvin nimenomaan merenkulun opiskelijoiden oppimistarpeita.

Seuraavaksi mietittiin *miten opiskelijoiden olisi helpointa oppia tarvittavat asiat.* Tekstiä muokattiin loogisemmin eteneväksi, sekä elävämmäksi kuin mitä se oli lähteinä käytettävissä julkaisuissa, ja joukkoon lisättiin kuvia, tilastografiikkaa, sekä linkkejä uutisartikkeleihin ja videoihin. Tällä haettiin pedagogisesti paremmin toimivaa kokonaisuutta.

Lopulta mietittiin, miten ja missä järjestyksessä tarvittavat tiedot tulisi esittää. Opintojaksoon tehtiin kuusi eri lukua:

1. **Unit Introduction / Opintojakson esittely.** Ensimmäisessä luvussa opintojaksoa esitellään opiskelijalle yleisellä tasolla, ja annetaan ohjeita opintojakson suorittamiseksi.
2. **Understanding the Cyber Threats and Getting to Terms With the Terminology / Kyberuhkien ymmärtäminen ja terminologian sisäistäminen.** Toisessa luvussa opiskelijalle esitellään keskeisimmät kyberuhat, ja keskeisimmät kyberturvallisuuteen liittyvät termit. Tässä luvussa selittämättä jätettyjä, vähemmän keskeisiä termejä esitellään myös muissa luvuissa, sitä myöten kun ne tulevat esille asiatekstin edetessä. Tällä pyrittiin siihen, että asiatekstin eteneminen pysyisi mahdollisimman loogisena.
3. **Cyber Awareness Across the Organization and Supply Chain / Kybertietoisuus halki organisaation ja toimitusketjun.** Kolmannessa luvussa opiskelijalle kerrotaan yleisellä tasolla, miten rakentaa kyberturvallinen organisaatio sekä sisäisesti, että organisaation ulkopuoliset toiminnot huomioon ottaen.
4. **Cyber Security Onboard / Kyberturvallisuus laivalla.** Neljännessä luvussa opiskelijalle kuvataan käytännönläheisemmin ja tarkemmin kuin kolmannessa luvussa, miten hänen tulisi toimia laivalla, jotta laivan kyberturvallisuuden hallinta olisi asianmukaisella tasolla.
5. **Maersk Case Study / Maersk tapaustutkimus.** Viidennessä luvussa opiskelijalle annetaan julkaisupäivämäärän mukaan kronologisessa järjestyksessä olevat linkit viiteen eri uutisartikkeliin, jotka käsittelivät vuoden 2017 NotPetya kyberhyökkäystä, joka iski muun muassa Maersk-yhtiöön.
6. **Videos + Essay / Videoita + Essee.** Viimeisessä luvussa opiskelijalle annetaan linkki kolmeen videoon, jotka kertoivat yritysten kyberturvallisuudesta. Videot sisälsivät myös kaksi tapaustutkimusta.

4.3 Opintojakson arviointi

Opintojakson arviointi/opitun testaus toteutettiin seuraavasti: Ensimmäinen luku ei sisällä arviointia lainkaan, sillä se toimii lähinnä opintojakson esittelynä. Luvut 2-5 sisältävät monivalintatehtäviä, yksi monivalintatehtävä jokaisen luvun lopussa. Tehtävät on toteutettu siten, että opiskelijoiden tulee vastata kokeen kysymyksiin 30 minuutin aikarajan sisällä. Jotta kokeesta pääsisi läpi, on saatava 100% koevastauksista oikein. Yrityskertoja on rajattomasti. Jokaisella kysymyksellä on kolme vastausvaihtoehtoa, joista vain yksi on oikein, ja tästä tiedotettiin opiskelijoille kokeen alussa olevassa ohje-tekstissä. Viimeinen luku arvioidaan pyytämällä opiskelijoita kirjoittamaan lyhyt essee liittyen heidän katsomaansa videoihin. Heille annetaan myös lupa käyttää muita lähteitä kuin katsomansa videot, sekä ilmaista esseessä omia mietteitä ja näkökulmia.

4.4 Opintojakson hyväksyttäminen ja laatiminen Moodleen

Opintojakson materiaali palautettiin ohjaajalle, joka esitti vaatimuksensa muutettavista asioista. Tarvittavien muutosten tekemisen jälkeen muutokset hyväksytettiin ohjaajalla, jonka jälkeen opintojakso ladattiin verkko-oppimisympäristö Moodleen. Moodle on maailmanlaajuinen, monien organisaatioiden käyttämä oppimisympäristö, jota on mahdollista muokata persoonalliseksi tarpeiden mukaan. (Moodlen www-sivut 2019.)

Opintojakson tekstiluvut ja monivalintatehtävät olivat aiemmin olleet Google Docs-/Microsoft Word-dokumentteja, ja tässä vaiheessa luvut ladattiin Moodleen pdf-muodossa, ja lukujen 2-5 monivalintatehtävät upotettiin Moodleen käyttämällä ohjelman “Quiz” toimintoa. Viimeisen luvun esseetehtävän arviointia varten Moodleen tehtiin niin sanottu palautuslaatikko, käyttämällä ohjelman “Assignment” tomintoa.

4.5 Opintojakson pilotointi

Opinnäytetyön 1 seminaarissa heräsi ajatus opintojakson pilotoinnista. Pilotoinnissa opintojakso annettaisiin testimielessä suoritettavaksi joukolle opiskelijoita, jotka voisivat sitten antaa opintojaksosta palautetta. Palautetta voitaisiin käyttää mahdollisten muutosten tekemiseen, joilla opintojaksoa voitaisiin mahdollisesti parantaa. Moodleen upotettiin opintojakson loppuun palautekyselylomake käyttämällä ohjelman “Questionnaire” toimintoa, ja opiskelijoita pyydettiin opintojakson etusivulla vastaamaan siihen. Palautekyselylomake koostui 11 eri kohdasta. Lomakkeessa esitettiin 7 väittämää ja 3 kysymystä, eli yhteensä 10 kohtaa, joissa opiskelijoita pyydettiin vastaamaan väittämään/kysymykseen skaalalla 1-5. Lisäksi kohdassa 11 opiskelijoille annettiin mahdollisuus antaa avointa palautetta opintojaksosta. Alla on yhteenveto palautekyselyn kohdista 1-10. Listassa näkyy numeroinnin jälkeen ensin väittämä/kysymys, sen alapuolella suluissa skaala ja sen merkitys, ja oikealla suluissa opiskelijoiden antamien vastausten keskiarvo.

1. Työmäärä oli sopiva 1 op:n kurssiksi.
   (1 = eri mieltä, 5 = samaa mieltä.) (3.7)

2. Kurssi oli mielenkiintoinen.
   (1 = eri mieltä, 5 = samaa mieltä.) (3.4)

3. Kurssi oli itselleni hyödyllinen.
   (1 = eri mieltä, 5 = samaa mieltä.) (3.1)

4. Kurssi oli itseopiskeluun sopiva.
   (1 = eri mieltä, 5 = samaa mieltä.) (3.7)

5. Kurssin vaikeusaste?
   (1 = liian helppo, 5 liian vaikea.) (3.4)

6. Kurssin englannin kieli oli ymmärrettävää.
   (1 = eri mieltä, 5 = samaa mieltä.) (3.1)

7. Kuinka laajasti kurssi käsitteli aihetta?
   (1 = liian suppeasti, 5 = liian laajasti.) (3.4)

8. Millaisessa suhteessa kurssi käsitteli merenkulkuun suoraan liittyvää kyberturvallisuutta, vs. yleistä kyberturvallisuutta?
   (1 = liikaa merenkulusta, 5 = liikaa yleisestä.) (3.3)

9. Kurssin ohjeistus oli riittävää.
   (1 = eri mieltä, 5 = samaa mieltä.) (3.6)

10. Kurssin ohjeistus oli selkeää.
    (1 = eri mieltä, 5 = samaa mieltä.) (3.6)

Nähdään, että vastausten keskiarvon ero skaalan keskiarvoon 3, on keskimäärin 0.43 yksikköä, ja enimmillään kahdessa kohdassa 0.7 yksikköä. Vastauksia analysoitaessa eroja ei pidetty merkittävinä, jonka vuoksi opintojaksoon ei niistä johtuen tehty muutoksia.

Seuraavaksi esimerkkejä kohdassa 11 annetuista palautteista. Palautteita ei ole muokattu kirjoitusvirheiden korjausta lukuun ottamatta.

“Liikaa saman toistoa ja liikaa yrityksen rakennetta kyberturvallisuudessa ja sen kertaamista.”

“Kurssina tehtävä voisi käsitellä enemmän myös jokapäiväistä kyberturvallisuutta, toki sisällyttäen merenkulkuun liittyvät riskit.”

Avoimeen palautteeseen tulleet vastaukset antoivat kaikki suhteellisen erilaisia vastauksia ja kehitysehdotuksia. Koska avoimeen palautteeseen tulleista vastauksista ei löytynyt selvää, yhtenäistä viestiä siitä miten opintojaksoa olisi kuulunut kehittää, opintojaksoon ei tehty muutoksia avoimen palautteen perusteella.

5. YHTEENVETO

Opinnäytetyö luotiin vastaamaan koulutuslaitosten ja työelämän tarpeita merenkulkijoiden osaamisen kehittämisestä kyberuhkien hallinnan alueella. Ajankohtaisista julkaisuista kerätty tieto muotoiltiin pedagogisesti toimivaksi, loogisesti eteneväksi kokonaisuudeksi joka hyväksyttämisen jälkeen ladattiin verkkoon. Opintojakso annettiin opiskelijoille testattavaksi, ja heiltä kerättiin palautetta opintojakson mahdollisia parannuksia varten.

Opinnäytetyö oli kokonaisuudessaan tekijälleen opettavainen. Toivottavasti laadittu opintojakso tulee olemaan myös tuleville opiskelijoille opettavainen tiedon lähde, joka myös inspiroi heitä opiskelemaan aihetta enemmän tulevaisuudessa.

Haluan tässä kohtaa lausua kiitokseni Werner Hacklinin säätiölle opinnäytetyöhön myönnetystä apurahasta.

LÄHTEET

SAMK:n www-sivut 2017. Viitattu 28.01.2019. https://www.samk.fi/uutiset/samk-merenkulkualan-korkeakoulujen-jarjeston-hallitukseen/

Boyes, H & Isbell, R. 2017. Code of Practice Cyber Security for Ships. London. Institution of Engineering and Technology.

BIMCO. 2016. The Guidelines on Cyber Security onboard Ships. Bagsværd. BIMCO.

IoT Business News-sivuston www-sivut 2019. Viitattu 05.02.2019. https://iotbusinessnews.com/

BBC:n www-sivut 2017. Viitattu 28.01.2019. https://www.bbc.com/news/technology-40685821

CNBC:n www-sivut 2017. Viitattu 28.01.2019. https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

IAMU:n www-sivut 2018. Viitattu 28.01.2019. http://iamu-edu.org/?page_id=22

Moodlen www-sivut 2019. Viitattu 28.01.2019. https://docs.moodle.org/36/en/About_Moodle

LIITTEET

Seuraavissa liitteissä on Moodle-alustalle luodun opintojakson sisältö.

LIITE 1

Chapter 1 - Introduction

Introduction to the Unit

Welcome to this online unit on how to handle cyber threats posed to the shipping industry. This unit is completed totally online, with no need to attend class. Just read the chapters and watch the videos behind the links, and answer the multiple choice questions afterwards. The unit consists of 6 chapters:

1. Introduction
2. Understanding the Cyber Threats and Getting to Terms With the Terminology
3. Cyber Awareness Across the Organization and Supply Chain
4. Cyber Security Onboard
5. Maersk Case Study
6. Videos + Essay

Chapter 1 will not be assessed. Chapters 2-5 will be assessed with multiple choice question tests. Chapter 6 will be assessed by writing a short essay based on 3 videos watched. Chapters 1-5 consist mostly of reading, but also of videos, so please make sure to have some kind of audio available. **The unit is not a “check-list” for things to be done to make shipping cyber secure, but rather a guide that will teach you the basic principles and hopefully encourage you to undertake further studies about the matter in order to widen your knowledge and sharpen your skills. Hope you enjoy it!**

Introduction to Cyber Security

Across the globe, and across all fields of of business, doing business with sufficient efficiency to stay competitive, often means utilizing the latest available technologies. However, using the newest technologies, almost inevitably leads to sooner or later becoming increasingly depending on them, sometimes to the degree that doing business without them becomes practically unthinkable. This doesn’t come without challenges. Wherever there is dependence, forces that seek to exploit them might occur.

Like in virtually all industries, modern **IT, or “Information Technology”** has been an important part of seafaring and the maritime cluster for quite some time already. The term IT is usually used for describing computer-based technologies and telecommunications used to create, store, exchange and process information in a digital way. Although held back by satellite internet connections that, depending on the location of the ship and a few other variables, can have been considerably slower and less dependable than those ashore in the same period in time, it has still been there in some form. Emails and satellite phone calls, have been around for a while.

In recent years however, the shipping industry has found new ways to implement IT, and more specifically data transmission to enhance its operations. The **IoT, or “Internet of Things”** concept has made a strong entry into seafaring. This means that when it used to be that only ships’ IT systems were connected to the shore via the internet, this is now also the case for an increasing number of ships’ **OT or “Operational Technology”** systems.

For example, a maintenance provider can get real time data streams about a main engines running hours, as well as about bearing temperatures, among many other data points, making it easier to pinpoint when and where the next maintenance should take place. This supports an effective execution of **“Condition Based Maintenance”,** a concept that builds on the idea of performing adequate, but no unnecessary maintenance, and that is widely considered to be the most cost-effective approach to maintenance.

The benefits of utilizing these IoT based methods are evident. Besides cost-effectiveness, they provide improvements in crew and passenger safety, decrease environmental impact and enhance supply chain reliability. The downside is, that the increased interconnectivity of both IT and OT systems to the shore as well as to other ships, leaves them vulnerable to a number of possibilities for exploitation by cyber attackers. The benefits are still more significant than the drawbacks, and significant investments have been made by multiple parties to ensure the smooth operation of these kind of systems, and therefore there's no going back. The IoT is here to stay, and the best thing we can do is to educate ourselves on the risks, in order to avoid damage. On top of the IoT related ship-to-shore threat, the more traditional approach of directing a cyber attack against a shipping company's shore-based activities is also ever present, and shouldn't be underestimated.

Related material:

A New York Times article on a new kind of cyber threat:
https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html

A ~6 minute video with examples of cyber attacks against shipping companies:
https://www.youtube.com/watch?v=DfEiMj7wAi4

LIITE 2

Chapter 2 - Understanding the Cyber Threats and Getting to Terms With the Terminology

Read the text and the linked news article, and watch the linked video. After that, answer the multiple choice questions for this chapter.

When hearing the word cyber attack, we often tend to think about a piece of software somehow infiltrating our computer, severely compromising its operation. While this can be the case, the big picture is a bit more complicated than that.

First of all, cyber attacks can be categorized as either **untargeted, or targeted.** Untargeted attacks are designed to cause damage to as many organizations as possible. Targeted attacks on the other hand, are aimed at a specific target organization.

Untargeted attacks are usually quite basic in design, that use relatively simple tools in order to breach a company's IT systems. Some of the most common methods for this are:

- **Social engineering.** This method consists of the potential cyber attackers trying to convince individuals working for the targeted organization to break their security procedures, in order to make the breaching easier. A common way for attackers of doing this is through social media channels, although that's not always the case.
- **Phishing.** Sending out a big number of emails to potential targets, with content that aims to convince individuals to give away sensitive information. This is often done by claiming the email comes from the individuals own employer, and requesting the individual to click on a link in the mail that takes them to a staged website, where they are for example asked to give away their passwords and credentials. Other tricks that are often used to enhance the effectiveness of these emails is to claim that the matter is urgent, and that ignoring, or even postponing the requested action might lead to severe damage for the individual's employer. Whenever an email sender motivates their requests with authority, and/or urgency, and/or threats, the receiver should act with caution and criticism, verifying the request with the claimed sender or relative authorities, before proceeding.
- **Water holing.** Consists of either altering an existing website, or creating an entirely new one, designed to look like the original, in an attempt to take advantage of site visitors. For example, an employee trying to log in to an "employees' area" on what they believe to be the organization's website, might end up unknowingly giving away their username and password.
- **Ransomware.** A piece of software that infiltrates the targets' computers and encrypts data, until the creator/distributor of the software decrypts the data. Usually the decryption isn't done before a **ransom fee** has been paid to the creator/distributor, **if even then.**
- **Scanning.** A method that randomly targets attacks against vast portions of the internet.

Targeted attacks are often more complex and thought through than untargeted attacks. Since they are purpose built to attack a specific company, or even a specific ship in the scope and space of the shipping industry, they might be using custom made techniques and tools to fulfill their purpose. Examples of these are:

- **Spear-phishing.** A more sophisticated version of phishing, where the receivers get personalized emails. It’s common for these emails to contain malicious software either directly, or behind links that automatically download it when clicked upon.
- **Deploying botnets.** Botnets are a group of internet-connected computers/devices commanded to simultaneously attack a website and thereby overload the site, compromising its functions. Even worse, the attack can target a **DNS, or “Domain Name Server”,** taking down dozens of websites at once. This is known as a **DDoS, or “Distributed Denial of Service”** attack, not to be confused with a **DoS, or “Denial of Service”** attack. A DoS attack is caused by a single attacker targeting a single website and making it temporarily useless, sometimes for up to several days, making it lose **revenue and consumer trust.** The rise of the IoT has provided DDoS attackers with a very **large number of often very poorly protected devices that can be hijacked and used to deliver a DDoS.** There are even so called **“botnet for hire”** services, from where attackers can rent a botnet to launch the attack from. It is also common to send the targeted website a **“DDoS ransom note”**, asking them to pay a ransom fee in exchange of not getting attacked. The DDoS threat is real: according to iotbusinessnews.com, the 2016 “Dyn DNS” attack made **Twitter, Netflix** and other online giants unusable. They also say big websites could lose up to **40 000 US dollars/hour** during an unmitigated DDoS attack.
- **Subverting the supply chain.** This method consists of delivering the attack to the target organization by compromising either software or hardware, that are going to be delivered to the target organization.

Threat Actors

Cyber attacks can be launched by many different kinds of interest groups, each with their own specific goals. The motives and people behind the attacks and their interests are usually as follows:

- **Cyber misuse.** This form of attack is usually conducted by rather unsophisticated hackers, or even by dissatisfied employees of the organization itself. Sometimes classified data is accessed for research purposes only, and while it may be that no direct damage is done, it’s still illegal in most instances, if done without the data owner’s permission. Some hackers are pure opportunists, individuals that want to **show off their hacking skills.** They would for example hack a system, and then post the passwords and credentials of that system on public forums or social media, just for the sake of **gaining recognition.**
- **Activist groups.** The groups might be seeking publicity, in order to convince the public to support their case of for example resisting the shipping of

specific cargoes in specific areas. Targets include ships, ship owners/operators, cargo receivers, or some other actor in the supply chain of the cargo. This is sometimes called **"hacktivism".**

- **Espionage.** Unauthorized access of the target's computer systems, in order to extract classified information. This may for example be done by hackers either for state purposes, or to seek financial gain either for themselves or a competitor to the target (if paid by the competitor to do it), the later sometimes referred to as **"industrial espionage".**
- **Organized crime.** Examples include hackers working together with **pirates** in order to facilitate a physical attack on a ship. If the hackers can break into a shipping company's or cargo handler's logistics management system, they can possibly find out which ship is going to be loaded with what cargo, and passing through what area at a given point in time. This makes it easier for them to commit **theft of valuable cargo, or kidnapping** in order to receive **ransom payments.** Another example is to alter the cargo data, in order to facilitate **smuggling of illegal cargo.**
- **Terrorism.** Includes for example **"remotely hijacking"** a ship by compromising its navigation and propulsion/steering systems, forcing the ship to switch from a "business as usual operational mode" to something closer to a **"survival mode"**. This method plants fear in the public, and is most effective when done to a ship that's either in close proximity to a passenger ship, seaside hotel etc., or even directly to a passenger ship.
- **Warfare.** A nation state in an armed conflict with another one, might try to perform some sort of espionage or direct disruption of ship OT, with the purpose of disrupting the operations of the enemy state's ships on a general level, in order to halt their transports of **weapons, fuel, and food.**

Desired attack outcomes for the attacker that haven't been described earlier are for example destruction of cargo, ships, and shipping facilities. Influencing where in the world the ship is willing to do business by for example altering relevant data. **Distracting** the ship's crew by for example altering the readout of a sensor, as a **smokescreen** in order to facilitate a **data extraction** operation.

Attack Symptoms - Data Compromise

As there are different methods of delivering an attack, there are different ways in which the attacks can cause trouble. Here are three examples of common data compromise:

- **Loss of confidentiality.** This means that sensitive data has been obtained and understood by the attacker, in such a way that it is possible to **exploit the target.**
- **Loss of integrity.** In this situation the target cannot be sure that any data hasn’t been, at least partially, altered by the attacker, which will probably lead to at least some level of **complications of everyday business.**
- **Loss of availability.** A case where the data is being made unavailable to the target, causing **disruptions to doing business.**

These three **(Confidentiality, Integrity, Availability),** form the basis for the so-called **CIA model**, which is a common method used as a part of cyber risk assessment.

For example, if a no backup USB drive containing encrypted data but no data decryption software, is lost/stolen, there is no loss of confidentiality, due to the data being encrypted, but a loss of availability, since the data is unavailable to the user.

When using the CIA method, the one of the three that yields the highest risk, should determine the overall risk for that specific procedure or technical entity.

Stages of a Cyber Attack

A cyber attack is done in multiple stages. It can usually be described as a 4-stage process:

1. **Survey/Reconnaissance.** The time spent on this stage can vary greatly, depending on the strength of the motivation of the attacker, the strength of the organization’s defenses, and the time available (in case the attacker’s motivation for the attack is to stop a specific thing from happening, like for example making a ship unable to navigate and thereby stopping it from carrying a dangerous cargo into a specific geographical region before it reaches it). A popular way of gathering information preceding a cyber attack is the so-called **OSINT method.** OSINT stands for **“Open Source Intelligence”,** and means gathering bits and pieces of information from social media, news, the organization’s website, interviews with the senior management etc., that are not classified, and that are not sensitive one by one, but when combined they can allow a potential attacker to build a good road map for an attack.
2. **Delivery**. The attacker commences the attack.
3. **Breach.** The method chosen for the attack and the severity of the exploited vulnerability will decide the extent of the breach. It’s important to keep in

mind that not all attacks make systems crash. **Some attacks are not even designed to make systems crash, but rather to infiltrate the system, and extract data in a stealthy way, making them harder to spot.** This way, the attackers can extract data over a long period of time, which might be effective in case of for example national espionage. Examples include interrupting or disrupting the operation of the **ECDIS or "Electronic Chart Display",** gaining access to data that is sensitive from a point of view of commerce and safety, like crew/passenger lists or cargo manifests, or even **gain full control of a machinery management system.** An ECDIS is a computer-based navigation system, that combines information from **GPS, radar and AIS** among others, and projects this combined information onto a screen with an electronic navigational chart. GPS stands for **Global Positioning System,** and AIS for **Automatic Identification System.** The GPS shows the ship's position on the sea, and the AIS makes it possible to track other ships' movements, in case they are giving out AIS data. The radar also provides information on the position of other objects in relation to the ship, but in a more direct, accurate, and reliable way than the AIS, because the radar's function is based on direct bouncing of radio waves, rather than transmitting and receiving data packages.

4. **Affect.** What affect a breach will have for the organization is determined by the motivations and goals set out by the attacker. Once inside the system, the hacker might be able to not only monitor, destroy, or extract data, but also expand the attack onwards, or perform necessary actions in order to be able to return to the system at a later stage. An example of destruction of data would be to destroy important pre-arrival data from the ship's cargo handling database, in order to postpone and severely complicate a ship's upcoming port operations, causing financial loss to the organization.

Related material:

BBC news article, "How hackers are targeting the shipping industry": https://www.bbc.com/news/technology-40685821

Professor Kevin Jones from the University of Plymouth, UK, talks about a few basic aspects of maritime cyber security: https://www.youtube.com/watch?v=U-xjiD9ZYM0

LIITE 3

Chapter 2 Questions

Pick the right answer to the questions, recalling what you learned from chapter 2. Each question has only 1 correct answer.

What does the abbreviation “OSINT” stand for?

A. Overly Secure Intranet
B. Operational Signal Intrusion
C. Open Source Intelligence

What are botnets?

A. Computers designed to monitor information exchange between Operational Technology devices in an industrial or maritime environment
B. A group of internet connected devices commanded to simultaneously attack a website.
C. A group of robotic devices that have been networked together for optimization purposes

What are the three keywords of the CIA model?

A. Confidentiality, Integrity, Availability
B. Confrontation, Independency, Assertiveness
C. Centralized, Intellectual, Ambitious

How common is it for ECDIS systems to have anti-virus?

A. ECDIS systems pretty much always have anti-virus
B. ECDIS systems pretty much never have anti-virus
C. ECDIS systems automatically obtain the anti-virus via a USB cable from the bridge PCs needed to regulate the ECDIS.

LIITE 4

Chapter 3 - Cyber Awareness Across the Organization and Supply Chain

Read the text and the linked article, and watch the linked video. After that, answer the multiple choice questions for this chapter.

When building and maintaining a cyber secure organization, it is crucial to keep in mind that **"a chain is only as strong as its weakest link",** meaning that every person involved with the organization should be equipped with sufficient knowledge about cyber security related issues.

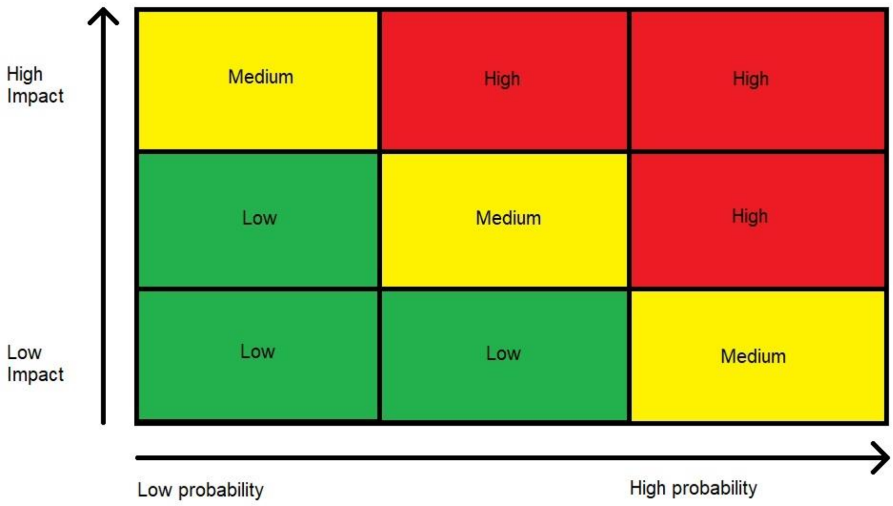
Because each organization is different, they are also vulnerable to different security threats. Therefore, the first actual step in the building process is to do a **risk assessment** for the specific organization. Before the assessment is done however, it is recommended that it is being made sure that cyber security as a whole should start, and be managed from, the organization's senior management, and appropriately involve everyone in the organization. **Cyber security issues should not by default be delegated to the IT department.** Why not? This is due to a few different factors that we are going to have a look at next.

First of all, a more robust policy on cyber security in general might result in many of the everyday tasks and procedures performed within the organization to become more expensive and time-consuming to see through.

Also, it is important to remember that **cyber security is not only about IT.** As a matter of fact, one way of viewing cyber security is as a the sum of **3 different parts or pillars: People, processes, and technology.** The people need to be adequately trained in order to be able to act in secure ways. The processes need to be such, that they minimize the risk of cyber intrusion. Finally, the technology needs to be on point and up to date, in order to withstand the latest threats.

Heightened cyber security measures might also affect interactions with customers, suppliers, and even authorities. For all of these reasons the senior management should be involved in outlining the cyber security guidelines of the organization, and deciding on a risk versus reward basis what should and what shouldn't be implemented. Following this general outline, it is possible to do a risk assessment. Once the risk assessment is done, it can be decided what the role of the IT department will be for future operations.

The risk assessment could be done in a classical way, like illustrated in the matrix below, where **“the risk = potential impact + probability of it happening”.**



High Impact	Medium	High	High
	Low	Medium	High
Low Impact	Low	Low	Medium
	Low probability		High probability

Risk assessment matrix

Developing Contingency Plans

Although all precautions would have been taken, the possibility of becoming the victim of a breach is real for any organization. Therefore, it is important to make contingency plans for the actions that should be taken immediately after the incident, and further, in order to minimize damage and to be able to go back to “business as usual” in the shortest possible window of time. **An important detail to keep in mind, is that copies of these plans should be kept in paper form and within close proximity, in case the electronic ones become unreachable after a breach.** Responding to a cyber attack can be a task that is beyond what the organization’s employees are capable of, since it can be quite complex. In case bad decisions are made immediately after the attack, it might cause the following repairing actions to be severely complicated. Because of this, seeking professional external help is recommended, and there should be a clear procedure in place in the contingency plan for how to do it, to ensure that the help is sought for, and hopefully also received, without wasting any time. Also, everyone should know what their role is in terms of action, in case a breach is found.

Contingency plans should undergo periodical tests, by for example running scenario exercises including all relevant personnel. Exercises can be held either as simulated "meeting room exercises" or, by doing a full-scale so-called **penetration test.** A penetration test is a test of the organization's cyber security, where a specialized company is hired to try to breach their system. You can find an example of a penetration test in the video linked at the end of this chapter, and the topic will be more widely covered in chapter 4.

It should also be pointed out in the contingency plan, how to verify if data has been altered or not, in cases where a breach is suspected, but not proven. Another thing to address is how to deal with **ransomware attacks.**

Response Plan

An effective response can be seen as having four main stages:

1. **Identification of the incident.**
2. **Defining the response objectives as well as investigating the situation.**
3. **Taking action as needed.**
4. **Recovering systems, connectivity and data.**

Questions that the response plan should be able to address are for example to which systems it is most applicable, and if the systems should be kept running or if it would be better to shut them down immediately? Should ship-to-shore links or other links be shut down in order to contain the damage to a smaller area? Would it be wise to use some kind of pre-installed security software, and if yes, in what situation and when? Who is the person within the IT department that could be immediately contacted in case of a breach? And also, how to proceed in case communication links are compromised?

Recovery plans

Recovery plans should be available to relevant personnel, in accordance to their roles in case of a breach, and it should be made sure the relevant personnel, as well as external IT helpers, understand the aim and scope of the plans.

Software and data backups should first of all **exist,** and be quickly accessible in order for the organization to make a quick recovery after a cyber incident.

Investigation

After the organization has recovered from the incident, it could be a good idea to hold a **debriefing** with the personnel, and look into what really happened and the reasons behind it. **This can help in avoiding, and dealing with, future incidents.** Further, if the incident was considered severe, it could be good to call in external experts to complete **research about the incident.** The findings could be used to make appropriate changes to reduce the risk of **similar incidents occurring in the future,** both to the organization/supply chain, and to the **maritime community as a whole.**

Related material:

When a device reaches the end of its life cycle, it is important that it is **disposed off correctly,** for several reasons. In this article, you can get familiar with the basics of disposing off an old device:
https://www.getsafeonline.org/protecting-your-computer/safe-computer-disposal/

A link to a ~20 minute video on the DNV GL website, that demonstrates a penetration test, and some best practices:
https://www.dnvgl.com/maritime/webinars-and-videos/videos/cyber-security-awareness.html

DNV GL is one of the most widely known classification societies in the world. They also work with quality assurance and risk management, in both seafaring and in other fields.

LIITE 5

Chapter 3 Questions

Pick the right answer to the questions, recalling what you learned from chapter 3. Each question has only 1 correct answer.

What are the 3 pillars of cyber security?

A. People, processes, technology
B. Pinpointing, proportions, tenacity
C. Proactiveness, precision, topology

Who should be involved when outlining the structure of cyber security within an organization, keeping in mind that it might be a time consuming task?

A. The IT department
B. The senior management
C. Both of the aforementioned as well as the rest of the organization

Contingency plans should -

A. Never be printed due to security reasons
B. Undergo periodical tests
C. Always be written in both English and French

For security reasons USB sticks should -

A. Never be bought from online shops
B. Always be tested on an offline computer before entered into a network device
C. Never be used to transfer files smaller than 1 megabyte

LIITE 6

Chapter 4 - Cyber Security Onboard

Read the text. After that, answer the multiple choice questions for this chapter.

There is a lot of material available for making environments like IT companies and land based industrial control systems cyber secure. However, these guidelines and recommendations cannot always be directly applied to a maritime environment. Some of them might, if directly applied, come in conflict with the ship's safety critical systems. **Safety should not be compromised for the sake of security.**

Something that has increasingly led to problems within maritime cyber security is the fact that the safety critical ship systems that handle alarms and control, become ever more merged with the more traditional IT systems.

When every individual working for the organization have been given enough training, with respect to their frame of work and position within the organization, about cyber awareness, it's time to focus on the more specific things.

The **IMO or "International Maritime Organization"** which is a part of the **UN or "United Nations",** an international organization dedicated to international collaboration, has pushed forward that cyber security should be incorporated into the **ISM or "International Safety Management"** code. The motivation for this is the fact that an increasing number of ships have been found to have **malware infected systems.** Malware is short for **"malicious software",** which is a type of software that installs itself onto the user's device, without the user's consent. Malware usually changes settings, deletes software, causes errors, monitors browsing habits or opens up the device for an attack.

From a **seafarer's** point of view, the most important part is the onboard cyber security, which is what we will be talking about next.

CSA

All onboard security should build upon the **ISPS or "International Ship and Port Facility Security" code,** which is an IMO framework for enhancing the security of ships and ports. It should also be made sure that all guidelines are aligned with the ship's flag state's legal requirements. Onboard cyber security should then be specified through a **CSP or "Cyber Security Plan".** The CSP should be based on a **CSA or "Cyber Security Assessment".** When finished, the CSP should build upon, and be an annex of the **SSP or "Ship Security Plan".** Due to the rapidly changing nature of the cyber threats, **the CSA and CSP should be reviewed and amended if needed, at least once every 2 years,** instead of once in 5 years for the **SSA or "Ship Security Assessment",** and the SSP.

When the creation of the CSA and CSP are commenced, it is recommended that professional help is sought, since this is a task that requires a wide and deep knowledge about cyber issues. If left to the ship's crew alone, there is a high probability that important details might be missed.

The CSA should be put together like a traditional risk assessment, where "the risk = potential impact + probability of it happening".

The greatest benefit of this kind of risk assessment approach is that the organization can get a better understanding of where to spend their **resources** when it comes to risk avoidance and mitigation.

When developing a CSA, there are various things to consider. The first step is to make a list of all the sensitive assets (may it be data, systems, or facilities) that are being considered vital, not forgetting those outside the ship. Next the processes surrounding those critical assets should be identified. Then, the risks from potential threats can be assessed. After the assessment, it should be decided what the priorities should be. The **residual risk** should then be evaluated, and a decision should be made whether or not to implement further changes.

Some good procedures to execute when performing a CSA are a **vulnerability test,** and a penetration test. A vulnerability test is a method for assessing how vulnerable a computer system is to cyber attacks. The assessment covers a number of topics such as verifying the strength of passwords, and checking if system configuration files are protected. We saw an example of a penetration test in the video linked at the end of chapter 3. A penetration test is a service that can be bought from companies specializing in cyber security. The test consists of having a team of cyber security professionals attempting to breach an organization's computer systems, in order to reveal weaknesses in their defenses, that can then be mitigated.

Onboard cyber security in practice

A CSA should be ship specific, and should take things like the ship's purpose, routes and operation routines into consideration. When applying the theories of preparing a CSA, it should be kept in mind that a ship has some characteristics that make it a somewhat unique entity when it comes to cyber security. The ships are linked to the shore, meaning that they are affected by cyber security measures that have **(hopefully)** already been set up by the company. A ship is also moving, oftentimes between different nation states, and is often involved with more than one stakeholder, which sometimes might leave it in a kind of grey zone when it comes to IT infrastructure accountability. Sometimes business-critical information is shared with providers of shore-based services. Also, an increasing number of the ships' safety systems are getting computer controlled.

Vulnerable Onboard Systems

The onboard systems that should be kept in mind when preparing a CSA should be:

- **Cargo management systems.** Digital cargo management systems are often linked to the shore, and include systems for ship tracking, in order to make business easier for shippers. **It is good to keep in mind, that this includes dangerous cargo.**
- **Bridge systems.** Networked navigation systems that are linked to shoreside networks, are often set to receive **streamed updates from ashore,** which make them **vulnerable to network intervention by hackers.** Non-networked systems aren't safe from cyber attacks either, since the **connected hardware** used to update them, can be infected with malicious software. A typical attack would involve DoS, or for example manipulations of the ECDIS. Other navigational targets could be the Radar/**ARPA, VDR,** AIS, and **GNSS.** ARPA stands for **"Automatic Radar Plotting Aid",** and is an add-on to radar that plots other moving objects like ships, thereby helping to avoid collisions. The VDR or **"Voyage Data Recorder"** is for ships kind of like what a "black box" is for airplanes. It records and stores voyage data, to make it easier for investigators to find out what led to an accident in case one was to

occur. GNSS or **“Global Navigation Satellite System”** is a general term for various kinds of satellite navigation systems.

- **Propulsion and machinery management and power control systems.** Linking these systems to the shore provides a good way for shippers and shipboard machinery maintenance providers to follow up on things like fuel consumption and engine bearing temperatures. However, like with the navigation systems, these systems too can be **intervened by hackers.** In case these systems are not directly linked to the shore, but are connected to shore-linked navigation systems, they could still be **penetrated via the navigation systems.**
- **Access control systems.** These are digital systems that are there for the purpose of enhancing the safety and security of the ship, its cargo and passengers. They usually encompass electronic “personnel on board systems”, shipboard security alarms and surveillance.
- **Passenger servicing and management systems.** These are the digital systems used for management of property, access control, and boarding and disembarkation. They may contain **sensitive data** about passengers.
- **Passenger facing public networks.** These are networks that should be considered as uncontrolled. They may be either wireless or fixed, and are there mainly for the purpose of entertaining the passengers and keeping them comfortable. **These networks should not be connected to any system that’s critical for the ship’s safety.**
- **Administrative and crew welfare systems.** Since these systems can be accessed through internet and email, they are **especially vulnerable** to attacks. If connected to the ship’s **safety critical systems,** they might be used by hackers as a **“gateway”** into the onboard systems.
- **Communication systems.** All wireless communication of data increases the cyber vulnerability of a ship, be it with or without satellites involved. It is a good idea to check with the service providers of these systems, what kind of cyber security measures they have taken on their end. However, even if they seem to be in order, **it’s never a good idea to rely exclusively on them.**

CSP

After the CSA is done, it’s time to use the results to create the CSP. The CSP should build upon the SSP wherever appropriate, and upon completion, the CSP **should become an annex of the SSP. Through this, the physical security already created by the SSP could extend to the aspect of cyber security. The main purpose of a CSP is to meet the challenges found when doing the CSA.** When a CSP is being developed, it is important to approach things in a holistic manner. The aspects of people, process, physical and technological security should be considered. Examples include that personnel who are to be granted **privileged** access to systems should undergo **periodic background checks as well as pre-employment screenings.** Another thing to look out for is USB sticks carrying software updates, and connected laptops used for diagnostics, that have been infected with malware. Procedures should be set up to ensure that these devices are **proven clean** before connected. The CSP should also **state who is responsible** for the maintenance of the security matters both inside the organization and in the supply chain.

Individuals that are granted with authorized access to systems should be given regular training to ensure good cyber hygiene. When complete, the CSP, as an annex to the SSP, should be kept **confidential.**

Review, Monitoring and Auditing of the CSP

In order to keep the CSP up-to-date with the latest technical developments, a procedure for carrying out **at least annual reviews** of it should be found in it, as well as a procedure for carrying out reviews **extempore,** after an incident or a change. Examples of possible changes include changes of legislation, the ship's operations, and/or -ownership.

Appropriate monitoring and auditing should be carried out by appropriate individuals and organizations, during the **entire lifespan** of the systems. Care should also be given to the upholding of monitoring, even in the case of setbacks like for example extreme weather, if it is reasonably possible. Although a part of the monitoring and auditing can be delegated to relevant companies and authorities, the main responsibility should remain with the organization. Like with any rapidly developing field, a risk assessment is essentially just a **snapshot** of an ever-changing living picture, and should therefore be **viewed with criticism even if the results are good.**

The CYSO/CSP

After the CSA and CSP are completed, it is time to appoint a **CYSO or "Cyber Security Officer".** The CYSO is an individual that is responsible for the cyber security of the ship. Depending on the ship, it's operations and owner, the CYSO can be located either on the ship or ashore. The CYSO should cooperate with the organization's **CSO or "Cyber Security Officer",** and act as a link between the ship's crew and cyber security professionals from inside of or outside of the organization. Part of the CYSO's role is also to **stay updated** on changes in legal and regulatory matters, and if needed, make alterations to procedures and policies. It is important that **responsibility is distributed** in a clear way between the CSP/CYSO/ship's crew/shore employees. For example, it could be the CSO's responsibility to manage background checks of contract personnel.

SOC

An **SOC or "Security Operations Centre"** is a centralized unit that handles cyber security issues affecting the fleet or systems connected to it. It could be a part of the organization's operations center from which the fleet is generally supervised, but this could vary based on the size of the organization. The main tasks of an SOC include monitoring of operations, and detection of abnormal, suspicious, or threatening activities, all while maintaining **situational awareness.** The SOC should stay updated with changes affecting the risks toward operations, and conclude whether any mitigating actions should be taken, and if yes, proceed to take them. On top of this, the SOC should also follow the **general public's as well as the experts'** discussion about security matters, in order to stay informed on a **general level.** It could also be a good idea to look into official reports from cyber incidents that have happened to other organizations with similar operating profiles, studying both cases that have had generally negative as well as generally positive outcomes. In other words, **the organization should learn from the mistakes of others, but also from their successes.**

Regulation of Information Spreading

Whenever an organization holds a presentation, posts on its website or social media, or adds content to conference papers among other things, there is a possibility of leaking sensitive information. The information might be either directly sensitive, or become sensitive in case a potential attacker is using the OSINT method to gather information. **The information might be leaked from both inside the organization, or from the supply chain.** It should therefore be made sure that all people affiliated with the organization are given sufficient and proportionate training on how to handle these kinds of matters, depending on their role within the organization. For example, while public relations and sales people should undergo more advanced training, it may be enough for the ship’s crew to have basic restrictions regarding personal social media posts as well as how to answer to media in case contacted by them, especially after a major incident. The guidelines necessary to meet these requirements should be found in the CSP.

Shipboard Networks

Logically thinking, the best timing for constructing a cyber secure and well-functioning shipboard network would be when the ship itself is being built. This is not always possible, due to for example the ship being bought second hand, or that the shipowner has realized the potential dangers of neglecting cyber security at a later stage, when the ship is already in operation. Whatever the case, the second best timing would probably be at a dry docking. In any of these two scenarios, the fact that the ship is not conducting its day to day, “business as usual” operations, makes it easier to create a network with good physical security. **It is important to keep in mind, that physical security is an important part of cyber security,** and as it is a part which is costly and time consuming to alter at a later stage, it should be the first part to be addressed.

The physical layout will define how different workstations aboard are connected to each other, and also how they are connected to the internet and thereby, to the shore-based organization, partners in the supply chain, and also various business affiliated third parties. **It is of high importance that the physical locations of cables and access points like USB ports are considered from a physical security perspective.** Locations that enable physical intrusion of the network by, for example performing an unauthorized inserting of a malicious laptop computer or USB drive, should be kept to a **minimum,** and have **restricted** access. Third party individuals, like maintenance workers, should not be left to work **unsupervised** in these spaces. It’s a good idea to keep a **list** (for example as an annex of the CSP) of the individuals having access to these spaces, and possibly also a **logbook** about who visited a specific space, and when.

There should be a policy set out by the organization, determining which networks should be uncontrolled, and which should be controlled. Direct interaction with uncontrolled networks should be avoided, especially if the ship's network infrastructure is a bit more advanced. There could also be an **application server** in place to restrict access time and protect passwords. An application server could be described as a framework of software that allows the creation of web applications, as well as a server environment to run them. They sit between the primary web-based server **tier**, and a database server's back end tier. A tier can be loosely described as a "level" within a computer network.

So if for example a password is given to a maintenance worker from outside of the ship's crew in order to access the ship's networks, it should be made sure that the passwords should be **valid only for a limited time, not much longer than what is needed to complete the tasks.** In case this kind of time limiting systems are not available, the passwords should be **changed immediately** after the outside individual has completed their service work. **When establishing onboard networks, a good rule of thumb is, that two pieces of equipment that don't need to communicate with each other, shouldn't be able to do it.** And again, external people should not be left working with systems unsupervised.

Some consideration should be given as to how the **switches** themselves should be protected. A switch is a hardware device with the ability to forward or filter away information packets, or pieces of data. It is capable of more than a **hub,** but less than a **router.** A router/gateway is a hardware device that receives, analyzes, and moves incoming data packages to another network. A hub is the most basic kind of network device, that connects computers or other network devices together.

It should not be made possible to jump from a less sensitive **VLAN** to a more sensitive one. A **LAN or "Local Area Network"** is a network where several computers in close physical proximity to each other are connected and can share data and resources. A VLAN or **"Virtual Local Area Network"** is like a LAN without cables, which also allows the administrator of the network to filter and organize data by dividing the network. **In order to reach the highest level of security, no more than one VLAN should be configured for each switch.** By doing this, the possibility of an attacker jumping from one VLAN to another is minimized. It also reduces the risk of misconfiguration. Whether or not to combine multiple VLANs on a single switch is a case by case decision, that has to be made depending on a **cost versus risk base.**

Before commencing use of the network, an important detail to remember is to check the **default security settings** of all the systems to make sure that none of them are taken into use without altering **generic factory passwords like "user" or "1234",** into safer ones. It should also be made sure, that it is not possible to without **proper authorization** add new devices to the network.

An infrastructure for managing the network is needed. Depending on the type of ship, there might be a need for one or more **management workstations,** that have multiple servers with various levels of security. **Because these servers are basically the cornerstones of network management and security issues, the recommendation is that a separate management VLAN would be used.** The management VLAN should be separated from the rest of the network using an access list and a **firewall**. A firewall can be either a software utility or a hardware device that filters data that enters or leaves a network or a computer. The ideal situation would be, if all of the traffic going into the management network would be from the managed devices, or alternatively be encrypted. One of the goals in network design should be to keep management traffic from entering the production network, in order to remove the possibility of interception. It would be best if each device would be configured with a physical port on the management VLAN. If this is not reasonably possible, because of for example heavy physical restrictions, then the management part of the system should be encrypted. The controls for controlled networks should be easy to monitor and measure.

Networks that fulfill different purposes, like for example the management net, the navigation equipment, and the **CAMS or "Control And Management Systems",** should be kept separated by a router/gateway. Each net should possess its own selection of **IP addresses/subnet masks** in order to not have issues with interconnection without a router/gateway. An IP address is kind of like a registration number for identifying a specific computer/device on the internet. Subnet mask is short for **"subnetwork mask".** The term **subnetting** stands for the process of dividing an IP network into blocks of logical addresses in order to improve security.

By default, uncontrolled networks should not be allowed to have any direct connections. Whenever the controlled LAN is to be accessed from an uncontrolled LAN, certain procedures should be followed. It should be managed by registration of connections, as well as registrations of activations, and it should comprise **automatic deactivation after a pre-set period of time.** These kinds of operations should only be performed by authorized personnel, and only after receiving permission to do so from an administrator. The only way direct connections should be accepted, is if they go through a firewall, or if they are initiated from the controlled side of the network.

A security measure to consider when bridging between uncontrolled and controlled networks is for example how to prevent unauthorized access managing traffic and separating networks. One way of implementing this is through the use of firewalls and VLANs. Another issue to be avoided is malicious software. **The main idea is to keep anti-virus, anti-spyware and anti-adware software up-to-date.** The same goes for the operating system patch management on all computers that access the LAN. Accessing the internet from hybrid LAN computers should also be prevented. **Only computers that do not access onboard operational systems should be able to access the internet.** Encryption protocols should be managed to ensure commercial connections and privacy. Certificates for verifying the origin of digitally signed software should be properly managed.

It is also essential to continuously manage and monitor the systems to make sure that the IT department, together with both the shoreside and onboard personnel, have up-to-date knowledge about the networks current status at any given time. This is where an **IDS or "Intrusion Detection System"** could come in handy. An IDS monitors the traffic and generates an alert to the system administrator when it senses something suspicious, in real time.

IDSs can be set to react to violations, or clear threats of violations of computer-security policies, violations of policies for acceptable-use, or violations of standard practices of security. An **IPS or "Intrusion Prevention System",** has a primary focus on identification of possible cyber incidents, but may also recognize reconnaissance that precedes a cyber attack. In the latter case, there is a chance that the IPS can block the reconnaissance activity and inform the cyber security administrators, which might then be able to change security controls in order to prevent further cyber incidents.

A network IDS/IPS can be a regular piece of computer software, or it could be an appliance-type device, or even a built-in card inside a switch. Usually a firewall is an application or a device that enforces security policy through specific elements like for example source-destination addresses and ports. An IPS on the other hand, is an enhanced application or device, which **analyses the traffic in itself,** and that is looking for familiar threats, while it can also reject what is incompatible with security policies. Another recommendation is **proactive log-monitoring software and host-based intrusion detection.** A host, also known as an **"internet node",** in this case refers to a computer/device on a network that delegates to the other **nodes.** A node is an active, physical, electronic device that is attached to a network (like a computer in a network). The IDS/IPS sensors should be placed within the network topology in a logical manner.

Examples of other tasks that the IPSs can fulfill are identification of problems related to security policies, documentation of an existing threat, and discouraging the organization's employees from violating policies regarding security. When selecting an IPS, the organization should make sure that they select one that is up-to-date in order to be able to handle the newest threats. IPSs use a number of different methods for detecting threats, like for example these:

- **Signature-based detection.** The IPS compares a known threat against events that it observes in order to decide what could be a cyber attack.
- **Abnormality-based detection.** Sometimes called **"anomality-based detection",** this method works by following "normal" traffic for a set period of time, to give itself an idea of what is normal, and it then makes an alert whenever it finds something that's out of the ordinary.
- **Stateful protocol analysis.** This method monitors traffic and compares it against a database of generally accepted traffic patterns that indicate either friendly or hostile activities.

A sensor should be mounted on the **internet facing** segment of the network, due to the visibility of the public servers to attackers. A good idea is to place another one **behind the firewall,** monitoring the traffic between the internet and the internal LAN. An

IDS/IPS sensor placed by a remote access segment, like for example a dial-up server or **VPN**. A VPN or **“Virtual Private Network”,** is a network allowing a user to connect to a network through a tunneling **“protocol”,** and thereby access internal internet, intranet websites as well as email. A “protocol”, is essentially an access method into a specific network.

Defence in Depth

The fact that cyber threats are persistent and complex, makes it ideal to try to adapt a so called **“defence in depth”** approach. This means that adequate security and resilience should be ensured by protecting data and equipment with multiple layers of defence. These layers could consist of **trained users, “best practice”-procedures, up-to-date defensive software, and strong physical security.**

Resilience of Ship Systems/Infrastructure

It should not be forgotten that IoT-based OT causes more threats to ships than simply those posed by cyber attackers. Ships increasingly dependent on IoT to be able to operate safely, are also vulnerable to for example **storms, and even geomagnetic solar storms,** which have the ability to disrupt the ship-to-shore link.

Onboard Contingency Plans

A contingency plan should state **who has the authority to make decisions, which experts should be called in and in which situations, and how communications should be handled.** Some critical parts of a contingency plan are knowing what to do in case the electronic navigation systems, or propulsion and power management systems, or other critical systems are compromised. Another thing to address is contingency for ships whose shore-based data has been lost.

Where a ship’s OT systems have been affected by a cyber incident, recovering them might need shore-based assistance. Therefore, it should be stated in the recovery plan how to safely proceed to port, or whatever is needed, in order to make the OT systems work again.

LIITE 7

Chapter 4 Questions

Pick the right answer to the questions, recalling what you learned from chapter 4. Each question has only 1 correct answer.

The CSA and CSP should be reviewed and amended if needed at least once every -

A. 6 months
B. 2 years
C. 5 years

When the CSP is complete it should be -

A. Displayed on a visible place on the ship's bridge
B. Handed over to the flag state authorities
C. Kept confidential as an annex to the SSP

The physical layout of the ship's network -

A. Is irrelevant in terms of cyber security
B. Is easiest to alter once the ship is in operation
C. Is an important part of cyber security

External maintenance people should be -

A. Left alone so they can do their job effectively
B. Always be supervised by a crew member
C. Allowed to only plug in devices running Apple software, since it's the securest software available

An IPS's threat detection method that compares a known threat against events that it observes is called -

A. Signature-based detection

B. Abnormality-based detection
C. Stateful protocol analysis

LIITE 8

Chapter 5 - Maersk Case Study

Here are links to 5 news articles about the 2017 NotPetya attack that hit Maersk among others. The articles are in chronological order by the date of publishing, so you can follow how the events unfolded. Read all of the articles and after that answer the multiple choice questions for this chapter.

A New York Times news article headlined: “Cyber Attack Hits Ukraine Then Spreads Internationally”.
Published on June 27, 2017
https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

A New York Times news article headlined: “Mystery of Motive for a Ransomware Attack: Money, Mayhem or a Message?”.
Published on June 28, 2017
https://www.nytimes.com/2017/06/28/business/ramsonware-hackers-cybersecurity-petya-impact.html

A BBC news article headlined: “Petya cyber-attack still disrupting firms weeks later”.
Published on July 18, 2017
https://www.bbc.com/news/technology-40645569

A CNBC news article headlined: “Shipping company Maersk says June cyberattack could cost it up to $300 million”.
Published on August 16, 2017
https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

A CSO news article headlined: “Maersk took just 10 days to replace 45,000 PCs wiped by NoyPetya attack”.
Published on January 26, 2018
https://www.cso.com.au/article/632622/maersk-took-just-10-days-install-4k-servers-45k-pcs-after-notpetya-attack/

LIITE 9

Chapter 5 Questions

Pick the right answer to the questions, recalling what you learned from chapter 5. Each question has only 1 correct answer.

What was a main difference between Wannacry and NotPetya/Petya?

A. NotPetya locked entire hard drives, where Wannacry only locked individual files
B. NotPetya did not use the Eternal Blue hacking tool used by Wannacry
C. There was no real difference between the two attacks

What appeared to have been the main focus in the design of NotPetya?

A. Acquiring large amounts of money
B. Targeting shipping companies
C. To have it spread quickly

What was the immediate cause of harm to Maersk from NotPetya?

A. Some port terminals had to be shut down
B. One of its ships rammed a dock
C. The salaries of some of the employees were stolen

In what way have Maersk improved their cyber security measures after the NotPetya attack?

A. They have swapped all their PCs for Macs

B. They have implemented different and further protective measures on top of continuing system reviews
C. They have significantly reduced outsourcing to be able to manage their cyber security more effectively in-house

Looking back after the incident, what was the main pitfall for Maersk that led to the Notpetya breach?

A. They employed the wrong people
B. They focused their core business in very unstable parts of the world
C. Their management was being too "naive" about cyber security

LIITE 10

Chapter 6 - Videos + Essay

Here is a link to a website with 3 videos talking about cyber security for a company, including 2 case studies:

https://maritimecybersecurity.org/maritime-cybersecurity-awareness/

Watch all the videos and write a short essay based on what you saw in them, and using one of the two following headlines:

- Maritime Cyber Security and Me
- Principals of a Cyber Secure Organization

You can use external sources if you like, as well as your own ideas and points of view. Return the completed essay to the Moodle dropbox.

LIITE 11

Sources used for the texts in the chapters.

These sources do not include the links to the news articles and videos that are already visible within the chapters.

IoT Business News' www-pages 2019. Referred to on January 28, 2019. https://iot-businessnews.com/

Computer Hope's www-pages 2019. Referred to on January 28, 2019. https://www.computerhope.com/

BIMCO. 2016. The Guidelines on Cyber Security onboard Ships. Bagsværd. BIMCO.

Boyes, H & Isbell, R. 2017. Code of Practice Cyber Security for Ships. London. Institution of Engineering and Technology.

Blomhoff, J C & Csorba, M J & Haugehåtveit, O & Springer D. 2018. Cyber Security Threats for the Maritime Industry – Are you prepared?. DNV GL.

The Facilitation Committee & Maritime Safety Committee. 2017. IMO Guidelines on Maritime Cyber Risk Management. London. IMO.