CHALMERS

IT-säkerhetsomkostnader i samband med implementering av IMO:s lagkrav om Cyber Risk Management

Examensarbete inom sjökaptensprogrammet

ANDREAS MEYER
TOBIAS ÖJBRO

INSTITUTIONEN FÖR MEKANIK OCH MARITIMA VETENSKAPER
CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige, 2021

.

IT-säkerhetomkostnader i samband med implementering av IMO:s lagkrav om Cyber Risk Management

Examensarbete inom sjökaptensprogrammet

ANDREAS MEYER
TOBIAS ÖJBRO

Institutionen för mekanik och maritima vetenskaper
Avdelningen för maritima studier
CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige, 2021

.

IT-säkerhetomkostnader i samband med implementering av IMO:s lagkrav om Cyber Risk Management

ANDREAS MEYER
TOBIAS ÖJBRO

Institutionen för mekanik och maritima vetenskaper
Chalmers tekniska högskola
SE-412 96 Göteborg
Sverige
Telefon: + 46 (0)31-772 1000

Omslag:
Fartyg till hamn med assistans av bogserbåt. (Public domain)

Institutionen för mekanik och maritima vetenskaper
Chalmers tekniska högskola
Göteborg, Sverige 2021

.

FÖRORD

Detta examensarbete har utförts av Tobias Öjbro & Andreas Meyer på Chalmers tekniska högskolas fyraåriga sjökaptensprogram. Iden till arbetets omfattning tillkom under sommaren 2020 vid praktik ombord på Stena Danica.
Ombord arbetade IT-tekniker från Stena Lines egna IT-avdelning med att undersöka sårbarheter i IT-systemen såväl som sårbarheter i satellit och navigationsutrustningen. Personalen utbildades i att upptäcka IT-säkerhetshot och ett riskhanterings avsnitt i fartygets SMS arbetades fram som omfattade IT-säkerhet.
Arbetet hade pågått under en längre period för att förbereda sig inför den nya lagen som trädde i kraft den första januari 2021 och omfattar IT-säkerhet ombord på fartyg.
Efter en närmare undersökning fann vi att det hade skrivits flera arbeten om hur implementeringen av IT-säkerhetshantering och åtgärder för att stävja attacker går till ombord. Vi fördjupade oss vidare i ämnet och snubblade över en videokonferens där det samtalades om eventuella framtida kostnader kopplat till de nya åtgärderna som behöver finnas ombord för att kunna stävja IT-attacker.
Detta resulterade i ett intresse kring vad kostnaderna har varit sedan resolutionen kom 2017 till att den blir lag 2021 och vad rederierna själva spår att utgifterna kring IT-säkerhet kommer att landa på i framtiden. Vidare utvecklades ämnet efter tips och ideer från klasskamrater såväl som lärare och vi är därav väldigt tacksamma till samtliga, utan er hade inte arbetet kommit till.
Vi vill även uttrycka ett stort tack och en stor tacksamhet till de rederier som valde att delta i vår undersökning.
Ett speciellt tack till intervjuobjekten för att dom tog sig tid att ställa upp på intervjuer och för att dom lade ner energi på att ta fram material för att utförligt kunna svara på våra frågor.
Ett tack riktas även mot vår handledare Martin Larsson som kontinuerligt ställde upp med tips ideer och möten. Martins stöd var ovärderligt och avgörande för att arbetet kunde tas i hamn.

.

IT-säkerhetomkostnader i samband med implementering av IMO:s lagkrav om Cyber Risk Management

ANDREAS MEYER
TOBIAS ÖJBRO

Institutionen för mekanik och maritima vetenskaper
Chalmers tekniska högskola

SAMMANDRAG

IT-attacker mot fartyg och den maritima industrin har ökar kraftig världen över. Mot den bakgrunden kom IMO med en resolution 2017 som behandlar IT-säkerhet hanteringen globalt ombord på fartyg. Resolutionen ämnar till att utveckla IT-skydd ombord på fartyg i såväl system, handlingsplaner vid incidenter och att öka kunskapsnivån för sjömän inom ämnet. 2021 den första januari träder resolutionen i kraft som lag och alla fartyg förväntas ha implementerat en IT-säkerhets hanteringsplan i deras SMS. Arbetet har undersökt kostnader inom tankfartygs branschen i samband med arbetet kring IT-satsningar för att nå IMOs nya krav på IT-säkerhet. Prislappen på implementeringen av IT-skydd och utbildning har inte förändrats sedan resolutionen kom 2017. Den största kostnaden för rederier är vid studiens utförande inom licens, service och underhåll och majoriteten av åtgärder för att skydda fartygens system återfinns inom kategorin användare i form av policy ändringar, förbud av flyttbar teknologi, begränsade rättigheter och e-postfiltrering. Studien presenterar också sårbarheter funna i AIS, GNSS och satellitkommunikationssystem som finns ombord på fartyg. Dessa system är nödvändiga för fartygs sjöduglighet och drift och studiens resultat indikerar att rederier brister i satsningar på att skydda dessa system. Vidare pekar studiens resultat på att det existerar en obalans mellan vad försäkringsbolagen anser att rederierna ska uppnå i IT-säkerhetsnivå och vad rederierna faktiskt uppnår.

Nyckelord: IMO, IT-säkerhet, Cyber Risk Management, IT-attack, tankfartyg

.

IT-säkerhetomkostnader i samband med implementering av IMO:s lagkrav om Cyber Risk Management

ANDREAS MEYER
TOBIAS ÖJBRO

Department of Mechanics and Maritime Sciences
Chalmers University of Technology

ABSTRACT

IT attacks on ships and the maritime industry have increased rapidly worldwide. Against this background, IMO produced a resolution in 2017 that deals with IT security management on board ships. The resolution aims to develop IT protection in ship systems, action plans in the event of incidents and to increase the level of knowledge for seafarers within the subject. 2021, the first of January, the resolution enters into force as law and all vessels are expected to have implemented an IT security management plan in their SMS. This study has examined costs in connection with IT investments to meet the IMO's new requirements for IT security. The price tag on the implementation of IT protection and training has not changed since the resolution came in 2017. The largest cost for shipping companies is in the conduct of the study in licensing, service and maintenance and the majority of measures to protect the ships' systems are found in the category of users in the form of policy changes, bans of mobile technology, restricted rights and email filtering. The study also presents vulnerabilities found in AIS, GNSS and satellite communications systems found on board ships. These systems are necessary for the seaworthiness and operation of ships and the results of the study indicate that shipping companies are lacking in efforts to protect these systems. Furthermore, the results of the study indicate that there is an imbalance between what the insurance companies believe the shipping companies should achieve in the IT security level and what the shipping companies actually achieve..

Keywords: IMO, IT-security, Cyber Risk Management, IT-attack, tanker

.

INNEHÅLLSFÖRTECKNING

.

.

TABELLFÖRTECKNING

.

FÖRKORTNINGAR OCH BEGREPP

IMO - International maritime organisation.

AIS - Automatiskt identifikationssystem.

GPS - Global positioning system.

Eternal Blue/Eternal romance - IT-säkerhetsluckor.

Notpetya - Utpressningsvirus.

NSA - Amerikanska nationella säkerhetsmyndighet.

ISM - Internationella säkerhets hanteringskod.

SMS - Säkerhetshanteringssystem.

Spam - Skräppost.

DDOS - Denial of service. Hindrar normal användning av system.

Spoofing - Förfalskad eller lånad identitet.

SATCOM - En grupp geostationära kommunikationssatelliter.

VSAT - Very small aperture terminal. Tvåvägs satellit jordstation med antenn.

NOC - Network operations center.

GMDSS - Global maritime distress and safety system.

INMARSAT - Företag som ansvarar för kommunikation via satellit till fartyg.

Flaggstat - Fartygets nationalitet.

MMSI - Nummer som identifierar fartyg eller kuststationer.

GNSS - Satellitnavigation.

Iridium - Motorolas satellitbaserade kommunikationssystem .

HTTP - Kommunikationsprotokoll för att överföra webbsidor på world wide webb.

.

CyRim - Ett projekt med en hypotetisk utförd It-attack.

P&I - En skydds och skadeförsäkring. Inkluderar kollision, egendomsskador, föroreningar, miljöskador och borttagning av vrak.

Confidentiality - information som inte ska lämnas ut till allmänheten.

Authentication - En kontroll av given identitet vid ex inloggning.

Availability - att informationen är tillgänglig enbart för auktoriserade användare.

Loyds - Ledande internationellt klassningssällskap

.

1. INLEDNING

CyRim är ett samarbete lett av Nanyang tekniska universitet i Singapore tillsammans med centrum för försäkringsrisk i Singapore och finans. Dessa parter genomförde ett projektet på beställning av Loyds som bestod av en hypotetisk IT-attack mot 15 stora hamnar i Asiatiska stillahavsområdet.

CyRiM valde att sprida sitt hypotetiska IT-virus genom att infektera fartyg som sedan infekterade de hamnar som fartygen anlöper till. I rapporten kan man utvinna att kostnaderna för den hypotetiska IT-attacken om den skulle lyckas, skulle komma att kosta så mycket som 110 miljarder amerikanska dollar (CyRiM report 2019.)

IT-attacker har stadigt ökat och utvecklats i sin sofistikering sedan mätningen påbörjades 2017. Det rapporterades 50 stycken operativa teknikhackningar i världen 2017. Det rapporterades 120 stycken år 2018 och år 2019 var det 310 stycken som rapporterades. Detta är en ökning på 900 % på tre år (Hellenic Shipping News 2020).

Safety At Sea & BIMCO (2019) utförde en undersökning där drygt tre av fyra deltagare svarade att de anser att IT-attack är en hög eller mellanstor risk gentemot deras organisation. Undersökningen visade även att en tredjedel av deltagarna hade varit med om en malware-attack, cirka 41% en spear-phising attack och 68% hade upplevt en phising-attack.

Trots detta visade undersökningen att bara drygt en tredjedel av deltagarna hade investerat i någon form av IT-säkerhet (BIMCO & Safety at Sea, 2019).

2017 adopterade IMO en resolution med nya riktlinjer som behandlar IT-säkerhet. Vidare utvecklade IMO en guide för att hjälpa rederier att hantera potentiella hot. Den 1:a Januari 2021 blir resolutionen internationell lag och IMO:s nya krav om IT-säkerhetshantering förväntas ha implementerats runt om i världen på samtliga handelsfartyg.

I denna studie vill vi ta reda på hur den ekonomiska kostnaden har sett ut, om resursbehovet har ökat eller varit oförändrat för att möta kraven i den nya lagen. Studien vill undersöka kostnaderna mellan 2017 när resolutionen släpptes tills att den träder i kraft som lag 2021. Studien undersöker även vad rederierna anser kan behövas i framtiden i form av satsningar och resurser.

.

1.1 Syfte

Syftet med studien är att undersöka hur svenska tankrederiers kostnader har utvecklats i och med implementeringen av IT-säkerhet ombord på fartygen. Från att IMO:s Resolution MSC.428(98) adopterades 2017 till resolutionen blir lag den 1 januari 2021.

Vidare ämnar studien undersöka vilka framtidssatsningar rederierna gör på IT-säkerhet i nuläget och vilka kostnader det medför. Samt vilken syn rederierna har på eventuella framtida IT-säkerhetslagar ur ett kostnadsperspektiv.

För att studien ska kunna leverera ett förståeligt resultat kommer en bakgrund redovisas som bygger på redogörelse för hotbilden inom IT-säkerhet, visa utsatta teknologiska områden samt de vanligaste typerna av IT-attacker.

1.2 Frågeställning

- Hur har kostnaderna ändrats från 2017-2021
- Vilka system för IT-säkerhet har installerats på fartygen?
- Vad har IT-säkerheten kostat att implementera ombord på fartygen?
- Sker framtida satsningar inom IT-säkerhet i nuläget och vad kostar det?

1.3 Avgränsningar

Studien kommer redovisa kostnader kopplat till IT-säkerhet för tankrederier och dess fartyg samt organisationskostnader med den valda frågeställningen som grund till kostnadsundersökningarna. Avgränsning gällande typ av rederi gjordes på grund av den geografiska närheten till tankrederier som återfinns i Sverige. Antalet tankrederier i Sverige, ca 32st är relativt stort i relation till andra typer av rederier enligt trafikanalysrapport. (Svensk sjöfarts konkurrenssituation 2012).
Studien påbörjas från att IMO:s Resolution MSC.428(98) antogs 2017. Studien kommer inte ta upp kostnader för rederierna innan 2017 utan fokusera på kostnader och kostnadsutveckling från 2017 till och med första januari 2021 samt en förväntad kostnadsutveckling i framtiden efter första januari 2021. Studien kommer inte fördjupa sig djupt i den teknologiska aspekten av IT-säkerhet eller IT-säkerhetshot. Dock kommer studien tydliggöra vad malware-attack, spear-phising, operational attack och phising-attack är då dessa utgör de mest vanliga attackerna mot fartyg enligt Ayala (2016). Även de största tekniska sårbarheter som har identifierats kommer att redogöras för vilka är AIS, GNSS och satellitkommunikation. Även de tekniska aspekter som redogörs i IMO:s resolution från 2017 samt dess tillhörande guide som innehåller rekommendationer för att kunna skapa en effektiv riskhantering i ett IT-säkerhets syfte. Undersökningen kommer utreda vad rederier anser är de största IT-säkerhetshoten.

.

2. TEORI

2.1 Tidigare incidenter

I sin artikel skriver Caprolu et al (2020) att fartyg är troligtvis det äldsta långdistans transportmedlet som människor använder för att nå geografiska platser långt bort. Den maritima logistik industrin står idag för ca 90% av världens bytes varutransport. Ihop med kryssningsindustrin utgör den maritima industrin ett organ som transporterar tusentals människor ihop med tusentals ton gods. Varav det går att anse att industrin är av en kritisk sort som behöver pålitlig utrustning i form av kommunikation, navigation, lastoperativa såväl som administrativa datasystem. Dock har industrin historiskt fått minimalt med uppmärksamhet från rederier och maritima organisationer angående IT-säkerhet.
Flera anledningar går att hitta så som den sena digitaliseringen av den marina industrin och den långsamma utvecklingen av digitala system samt den släpiga uppdateringen av utrustningen ombord. Vidare har fokus legat på att utveckla andra aspekter inom industrin såsom lätttillgängliga tjänster. Därtill övertron om att fartyg tekniskt sett är svåra att utföra IT-attacker mot.

I sin IT-säkerhetsguide presenterar Mission secure (2020) en av det mest lyckade IT-Attackerna hittills. I juni 2017 drabbades Maersk av en av det hittills mest högprofilerade IT-attackerna. Maersk som opererar i 130 länder med över 80 000 anställda är världens största container och supply rederi. Maersk blev utsatt för en attack med ett utpressnings liknande virus vid namn NotPetya. NotPetya har förmågan att sprida sig utan hjälp av spamemails eller socialteknik.

Viruset använder sig av att exploatera Eternal Blue och Eternal Romance vilka är IT-säkerhetsluckor utvecklade av amerikanska nationella säkerhets byrån (NSA). NotPetya krypterar allt i sin väg och skadar data utan möjligheten till återställning och utan möjlighet till återhämtning av data. Viruset utveckling påstås vara statligt sponsrad av ryssland för användning mot ukrainska företag. NotPetya spred sig utanför de ukrainska gränserna och orsakade uppskattningsvis ekonomisk skada för ca 10 miljarder dollar totalt över hela världen.

Maersk är inte ensamma om att falla offer för IT-attacker. I november 2019 rapporterade Reuters (2019, 5/11) att James Fisher and Sons vilket är ett företag som erbjuder marina tjänster föll offer för en hacker attack. Rapporten av incidenten resulterade i att företagets aktievärde föll 5.7%.

I BBC rapporterade Tom Bateman (2013, 16/10) om en IT-attack 2013 där den Belgiska hamnen Antwerpen blev utsatt. Mjukvara mailades till personal som arbetade i hamnen varav gärningspersonerna kunde skaffa sig åtkomst till det logistiska container systemet. Man kunde därmed kontrollera rörelsemönster och platser man ville att containrar skulle befinna sig på. Det lyckade IT-attacken möjliggjorde narkotikasmuggling och det misstänks ha pågått sedan 2011.

.

I en artikel av Wall street journal (2018) rapporterades det om en IT-attack mot Cosco Shipping Holdings Co. Attacken inaktiverade det kinesiska statliga företagets amerikanska webbplats och e-postsystem. Det rapporterades att företaget lyckades behålla sin normala operationella nivå utan större påverkan av attacken.

Mission secure (2020) beskriver i sin IT-säkerhetsguide att en ökning med 400% av utförda försök till IT-attacker riktade mot den maritima industrin har skett från juni till februari 2020. Den globala Covid-19 pandemin har bidragit till en ökning av IT-säkerhetsincidenter såsom nätfiskeförsök, ransomware och ligger förmodligen till grund för den lavinartade sammanlagda utvecklingen av incidenter världen över. Anställda som arbetar på distans skapar flera utmaningar när det gäller att skydda organisationens IT infrastruktur genom nätverksåtkomst problematik.

IMO 2017 (b) Beskriver hur IT system har blivit en viktigt kärna i driften av flera kritiska system ombord fartyg såsom den operationella driften, säkerheten ombord och möjligheten att förhindra miljöutsläpp. I flera fall möter standarden på dessa system kraven som ställs av flaggstater. Dock har det skapats flera sårbarheter bland annat genom sammankoppling av nätverk samt åtkomstmöjligheter. Dessa system kan alltså leda till IT-säkerhetsrisker och riskerna dessa system medför bör hanteras.

Mot ovanstående IT-säkerhets attacker och ökningen av IT-attacker antog IMO 2017, resolution MSC.428(98) för IT-säkerhetshantering (Caprolu et al 2020). Resolutionen ämnar till att en riskhanterings förmåga ska omfatta IT-säkerhet och ska existera i rederiers SMS. Projektet med att integrera IT-säkerhet som en del av fartygets SMS ska vara klart till den första januari 2021 då det sker en årlig revidering av rederiers säkerhetsorganisation (Transport Styrelsen).

2.2 IMO Resolution MSC.428(98)

“Internationella sjöfartsorganisationen - är FN: s special byrå med ansvar för sjöfarts säkerheten och förhindrandet av marina och atmosfäriska föroreningar från fartyg”. (IMO egen översättning)

IMO adopterade en Resolution MSC.428(98) - Maritim IT-säkerhetshantering i SMS vid den 98:de sessionen i juni 2017. Denna resolution är inkorporerad i ISM koden.
Resolutionen ämnar till att uppmuntra maritima administrationer att IT-säkerhet ska implementeras i SMS systemet som definieras vidare i ISM koden. Detta ska ha skett senast den första januari 2021 vid den första årliga verifieringen av rederiernas efterlevnad dokument (IMO 2017 a). Resolutionens beståndsdelar är följande.

.

- Resolutionen MSC.428(98) erkänner de brådskande behovet av att öka medvetenheten kring IT-säkerhetshot samt IT-systemets sårbarheten. För att kunna säkra en säker frakt industri som är motståndskraftig mot IT-säkerhetshot.

- Vidare att administrationer, klassningssällskap, fartygsägare, fartyg operatörer, fartygsagenter, utrustningstillverkare, service leverantörer, hamn och hamnanläggningar samt all maritim industri ska arbeta mot att säkra industrin mot IT-säkerhetshot och IT-sårbarheter.

- MSC-FAL.1/Circ.3 riktlinjer för marin cyber riskhantering godkändes av den underlättande kommitten vid dess fyrtioförsta session mellan 4-7 april 2017 samt av den maritima säkerhetskommitten vid dess nittio åttonde session mellan 7-16 juni 2017. Denna guide tillhandahåller rekommendationer för maritim IT-säkerhets riskhantering vilka kan implementeras in i en redan existerande riskhanteringsprocessen och är kompletterande till etablerad säkerhetshantering inom organisationen.

- Erinra om resolution A.741(18) där sällskapet adopterade den internationella management koden för säker drift av fartyg och för förorenings prevention (ISM koden) som bland annat erkänner behovet av lämplig förvaltnings organisation så att ledning kan tillfredsställa behoven av dem ombord på fartyg som krävs för att uppnå och upprätthålla höga krav på säkerhet och miljöskydd.

- Noterar ISM kodens behov vilka bland annat inkluderar tillhandahållandet av säker praxis för fartygs drift samt tillhandahålla praxis för säker arbetsmiljö, bedömning av alla identifierade risker för fartyg, personal och miljö, etableringen av lämpliga förebyggande åtgärder mot risker och den kontinuerliga förbättringen av säkerhets hanterings kompetens av personal ombord samt iland.

Vidare beskriver resolutionen fyra punkter med rekommendationer och riktlinjer.

1. Bekräftar att ett godkänts säkerhets hanterings system skall inehåll IT-säkerhets hantering i enlighet med mål samt de funktionella kraven ISM koden ställer.

2. Uppmuntrar administrationer till att försäkra att IT-säkerhetsrisker är lämpligt adresserad i säkerhetshantering systemet senast den första januari 2021 vid den årliga verifieringen av företagets dokument av efterlevnad.

3. Erkänner nödvändiga försiktighetsåtgärder som skulle kunna bli aktuella för att bevara konfidiallitet kring vissa aspekter av riskhantering inom IT-säkerhets.

4. Uppmanar alla medlemsstater att föra vidare resolutionen till samtliga intressenter. (IMO 2017 a. *egen översättning)*

.

2.3 Riktlinjer för IT-säkerhets risk hantering IMO (MSC-FAL.1/Circ.3)

I IMO:S (2017 b) riktlinjer för marin IT-säkerhets riskhantering delges rekommendationer för riskhantering inom IT-Säkerhet samt förebyggande åtgärder för att förhindra lyckade attacker ihop med rekommendationer för skademinimering.

IMO (2017 b) identifierar flera grundläggande system som återfinns på fartyg som bör fokuseras på i ett IT-säkerhetshanteringssystem. Dessa inkluderar följande men utesluter inte att det finns fler.

- Bryggsystem och navigationsutrustning.
- Lastoperativa system
- Maskin, framdrivning och ström hanteringssystem
- Passagerar administrativa och passagerarservice system
- Publika nätverk
- Administrative system för besättning
- Kommunikationssystem
- Åtkomstsystem

Ovanstående system utgör en nödvändighet i fartygets drift såväl som gynnar fartygs effektivitet inom flera områden, exempelvis som effektiv framdrift, effektiva och säkra lastoperationer etc. Trots nödvändigheten och gynnsamheten av att ha moderna system innebär existensen av dessa system att det finns risker. Riskerna uppstår på flera ställen bland annat i kritiska system och processer kopplat till integrerade system. Dessa kan vara ett resultat från otillräckligt underhåll, integration, avsiktliga samt oavsiktliga IT-hot och designen av system som är IT relaterade kan vara bristfälliga och ha sårbarheter.

Hot kan uppstå i form av skadliga intentioner, i detta sammanhang är det hot som avsiktlig hackning eller införande av skadlig systemkod. Men hot kan även uppstå via oavsiktliga handlingar av operatörer såsom dåligt underhåll av mjukvara eller negligerade hantering av användar åtkomster. Det senare kan i regel leda till att sårbarheter exponeras såsom ej uppdaterad mjukvara eller ineffektivt IT-skydd i form av brandväggar såväl som andra mjukvaruskydd.
Konsekvensen kan bli att möjligheten att kunna exploatera sårbarheter inom operationella system och informationssystem presenterar sig. Enligt IMO (2017 b) ska en effektiv riskhantering bejaka båda möjligheterna till hot.

Vidare beskriver (IMO 2017 b) att sårbarheter kan uppstå via brister i designen av system, integrationen eller underhållet såväl som brister i IT-säkerhetstänk vid användning av system. Vid sårbarheter som är exponerade inom operationella eller informationstekniska områden där åtkomsten sker direkt via brister i lösenordsstyrka eller indirekt via nätverk som inte är segregerade kan det ha konsekvenser för integriteten, säkerheten och konfidentialitet. Speciellt där kritiska system exponeras för sårbarhet eller åtkomst så som navigationsutrustning eller framdrivnings utrustning.

.

Enligt IMO (2017 b) ska en effektiv IT-risk säkerhetshantering även beakta säkerhets konsekvenser som kan uppstå från exponering eller exploatering av sårbarheter inom det informationstekniska området. Ett sådant scenario där exploatering eller exponering av informationstekniska områden kan upstå genom olämplig abslutning till ett operativt system eller genom en tredjeparts användning av flyttbar media såsom USB-sticka. Vidare beskrivs det i guiden hur ett lämpligt säkerhetstänk är viktigt för att förhindra dessa situationer. En kultur med högt säkerhetstänk bör börja utvecklas på ledningsnivå för att vidare implementeras in i alla nivåer av organisationen. Målet är att nå en kultur där ett helhetsgrepp är säkerställt och ett system för att kunna utvärdera IT-säkerhetshantering är i kontinuerlig drift.

Guiden IMO (2017 b) menar att ett acceptabelt sätt att uppnå ovanstående är att heltäckande jämföra och bedöma organisationens nuvarande IT-säkerhetshantering med den önskvärda ställningen. En sådan kontinuerlig jämförelse kan leda till luckor tydliggörs och upptäcks lätt. Dessa kan då adresseras och det blir tydligare vad som behöver prioriteras för att uppnå önskvärda mål. Vidare leder det till att organisationer kan använda sina resurser med effektivt.

Guiden presenterar fem stycken element till stöd för en verksam IT-riskhantering. Det är inte sekventiella utan de ska anses implementeras på ett lämpligt sätt i säkerhetsorganisationen och utföras praktisk på ett lämpligt sätt inom ett riskhanterings ramverk. Dessa fyra element är följande.

1. Identifiera: Definiera personal roller och ansvar för IT-säkerhetshantering. Identifiera systemen, tillgångar, datan och konsekvenser samt risker som uppstår för fartyget när system störs ut.

2. Skydda: Implementera riskkontroll ihop med processer och förebyggande åtgärder för att skydda system mot IT-attacker och säkra drift.

3. Upptäck: Utveckla och implementera aktiviteter som är nödvändiga för att upptäcka IT-säkerhetshot i god tid.

4. Reagera: Utveckla och implementera aktiviteter samt planer som ska kunna ge motstånd samt kunna återställa system eller tjänster nödvändiga för operationell drift under en exponering av en IT-säkerhetsincident.

5. Återställa: Identifiera åtgärder för att kunna återställa system nödvändiga för operationell drift samt implementerade åtgärder för att ha ett fungerande back-up system.

.

2.4 Typer av IT-attacker

2.4.1 Malware

Ayala (2016) beskriver malware som skadlig programvara som är utformad för att komma åt eller skada en dator utan ägarens vetskap. Det finns olika typer av skadlig programvara, inklusive trojaner, ransomware, spionprogram, virus och maskar. Ransomware krypterar data på ett system tills en lösen har betalats. Skadlig programvara kan också utnyttja kända brister och problem i föråldrad programvara. Termen "utnyttja" avser vanligtvis användningen av en programvara eller kod, som är utformad för att dra nytta av och manipulera ett problem i en annan programvara eller hårdvara.

Detta problem kan till exempel vara ett kodfel, felaktig design, maskinvarufel och/eller fel i implementeringen av protokollet. Dessa sårbarheter kan utnyttjas på distans eller utlösas lokalt. Lokalt kan en del av skadlig kod ofta köras av användaren, ibland via länkar distribuerade i e-postbilagor eller via skadliga webbplatser.

2.4.2 Phising

Phising utförs genom att skicka e-post till ett stort antal potentiella mål som ber om vissa känsliga eller konfidentiella uppgifter. Ett sådant e-postmeddelande kan också begära att en person besöker en falsk webbplats med hjälp av en hyperlänk som ingår i e-postmeddelandet. Detta e-postmeddelandet skickas ut till många individer ihop om att någon trycker på länken. Här är det kvantitet över kvalitet (Ayala 2016).

2.4.3 Spear-Phising

Spear-phising fungerar som phising men individuellt riktat med personliga e-postmeddelanden, som ofta innehåller skadlig programvara eller länkar som automatiskt hämtar skadlig programvara. Man försöker alltså skicka e-postmeddelanden som man vet att individen är intresserad utav för att öka chansen att individen aktiverar viruset genom att klicka en länk (Ayala 2016).

2.4.4 Operational Technologies Hack

I BIMCOs (et al 2020) guide förklarar att operations teknologiska system påverkar den fysiska världen. OT-system skiljer sig från traditionella IT-system. Operationstekniska system är hårdvara och programvara som direkt övervakar och kontrollerar fysiska enheter och processer.
IT täcker spektrumet av teknik för informationsbehandling, inklusive programvara, hårdvara och kommunikationsteknik. Traditionellt har OT och IT separerats, men med internets framfart har OT och IT närmat sig varandra och historiskt fristående system har integrerats.

.

Vidare beskriver Guiden att en OT-Hack försöker störa driften av OT-system vilket kan medföra en betydande risk för säkerheten ombord och både personal och last kan utsättas för allvarlig risk. Detta kan även medföra skada på den marina miljön och hindra fartygets verksamheter.

2.4.5 Tredje part, OEMS & Luftgap

Safety at seas & BIMCO (2020) beskriver i sin guide de komplikationer som uppstår med tredje part och OEMs. Med tredje part menas kopplingarna som fartygen har genom rederiets relationer med leverantörer av maritima produkter så som utrustning och system.

Tillverkarna av produkterna och systemen samlar kontinuerligt data från systemen som används ombord på fartyget. Tillverkarna lagrar information från systemets operativa driftstatus i syfte att förbättra produkten genom att analysera eventuella upptäckta fel. Detta är en av OEMs (Maritima tillverkare av originalutrustning) lösningar för att kontinuerligt arbeta för att upptäcka sårbarheter. Tillverkarnas produktion av produkter och system har sämre förmåga att upptäcka sårbarheter då dom tillverkar markant färre i antal än vad en större biltillverkare skulle tillverka.

Den mindre mängden produkter som serietillverkas innebär att de finns mindre resurser för att kunna erbjuda säkerhetslösningar, riskhantering tidigt och att i produktionsfasen kunna upptäcka eventuella sårbarheter. Organisationer och företag som erbjuder tjänster för att upptäcka sårbarheter och fel i en tillverkares system eller produkt har vid ett flertal tillfällen upptäckt brister i OEMs produkter. Man har kunnat bryta sig in i systemet genom att använda ett så kallat standardlösenord vilket är ett ursprungligt lösenord som följer med systemet, denna typ av intrång blir en sorts spoofing attack. Man lånar helt enkelt en existerande identitet för att få åtkomst till ett nätverk eller system.

Dessa lösenord följer med produkt dokumenten och hamnar ibland öppet tillgängligt på internet. Fartygsindustrin har flera olika leverantörer av OEM produkter vilket skapar en svårighet att hantera alla olika system. Safety at sea och BIMCOS (2020) undersökning visade att 83% av tillfrågade rederierna hade upphört att göra affärer med OEMs om det hade uppdagats att deras system eller produkter är sårbara inför IT-attacker. Man menar att ett fokus har legat på kostnadsminimering istället för att skapa system med tekniska förmågor och egenskaper för att motverka sårbarheter eller risker.

Undersökningen ger en klar fingervisning åt leverantörer att försäkra sig om att deras produkter innehåller en förmåga att motstå IT-attacker och att deras produkter och system används på ett avsett sätt för att minimera risken för icke auktoriserad åtkomst till deras system. Vidare utvecklar Safety at sea & BIMCOs guide (2020) myten som så kallat isolerat system eller luftgap. Det har ansetts att mellan system som är isolerade från varandra gällande

.

kommunikation kan det inte uppstå scenarier där systemen blir utsatta för IT-attacker eller skadliga mjukvaror.

Denna myt har motbevisats genom incidenter där USB-stickor har introducerat skadlig programvara till skyddade system. Mobiltelefoner är också en teknik som lätt kan brygga gapet mellan isolerade system genom att man kopplar upp sig till samma WiFi nätverk som de isolerade systemen är uppkopplade till. Idag är flera produkter uppkopplade till flera olika nätverk. Ett exempel är hur internet of things, vilka är vardagsprodukter uppkopplade till nätverk såsom skrivare. Dessa kan vara uppkopplade till samma nätverk som ett skyddat system samt till ett sekundärt nätverk för att där producera utskrifts loggar.

Ett sådant nätverk av grenade uppkopplingar skulle kunna riskera hela OT nätverket. Safety at sea & BIMCO (2020) beskriver i en rapport där ett nätverk av hackare länkade till ryska underrättelseorganisationer har använt just internet of things för att bryta sig in i företagsnätverk. Gruppen använde sig av just skrivare uppkopplade till flera nätverk för att skapa sig åtkomst till det skyddade företagsnätverket. Den vidspridda iden om att primärt skydda den bärbara eller stationära datorn har lämnat flera säkerhetsluckor. Främst i internet of things som i allt större utsträckning har en uppkoppling till internet för att skicka och ta emot information om driftstatusen.

2.5 Tre känsliga system

I sin artikel menar (Caprolu et al 2020) att GNSS (Global Navigation Satellite System) har identifierats som ett system med sårbarheter. GNSS system förlitar sig på civila signaler. Med behovet av att förstärka meddelande mottagnings möjligheten blev tekniken utan någon form av auktorisering eller konfidillitets mekanism. GNSS tjänster används av civila system där de bidrar med tidssynkronisering till flera teknologier och tjänster. Detta innebär att satelliternas bana kring jorden är tillgängliga publikt. Med relativt enkel teknika kan man därmed stämma in sig på samma operativa signal som GNSS tekniken använder och sända konfigurerade meddelanden som är väldigt lika den riktiga GNSS signalen. Ett sätt att skilja på vilken signal som är legitim och vilken som inte är legitim är att legitima signaler är relativt svaga vid marknivå medans dom illegitima signalerna är märkbart starkare.

Den stora sårbarheten inom systemet har varit vida känt länge utan att den har fått större uppmärksamhet. 2017 inträffade en incident i svarta havet där omkring 20 st fartyg rapporterade anomalier i deras GNSS system. Deras GNSS system signalerade en instabil position där platsen man såg ut att befinna sig på var nära en flygplats. I själva verket befann sig inga fartyg på eller i närheten av en flygplats. Samtliga fartyg tvingas återgå till äldre mindre pålitliga navigations system för att kunna säkra sin rutt samt säkra sin navigering. Vidare nämner artikeln att GNSS system även är väldigt sårbara för utstörning. Detta kan ske genom att man mobilt närmar sig ett fartyg eller att ett fartyg är nära en stationär station som sänder ut en signal på samma frekvens som GNSS systemets kommunikationsfrekvens.

.

Vidare beskriver (Caprolu et al 2020) AIS som ett system med sårbarheter. AIS är ett system som ämnar till att sända fartygets position, fart, rörelse samt fartygets rutt. Denna information används av fartygen för att säkra trafik navigering och undvika kollision. AIS använder två frekvenser för kommunikation 161.975 för fartyg till fartyg kommunikation samt 162.025 för fartyg till land kommunikation. AIS är begränsad i sin räckvidd när det gäller att ta emot och skicka information.
För att förbättra täckningsområdet har man börjat använda AIS mottagare på satelliter som kretsar i en låg omloppsbana runt jorden, informationen reläas till jordytan och man uppnår en räckvidd om ca 400 km.
AIS är ett system som utvecklades på 80-talet när det primära syftet var att vara ett verktyg i att undvika kollision. Idag har AIS fler användningsområden där sök- och räddningsinsatser, olycksutredning, fjärr spårning, uppskattning av havsströmmar, och skydd av marinkritisk infrastruktur är flera exempel. AIS är ett system som inte stödjer någon form av autentisering eller konfidentiella säkerhetsegenskaper.
Verktyget är sårbart på många olika sätt. Spoofing, data manipulation samt DoS är flera där det senare är ett sätt att neka åtkomst möjlighet AIS vilket omöjliggör möjligheten att skicka och ta emot information. Med dessa tillvägagångssätt skulle man kunna skapa falsk data såsom falskt mål, position, fart samt MMSI nummer. Man kan alltså skapa ett trovärdigt falskt mål för att sända illegitim datan.

Caprolu et al (2020) förklarar vidare hur satellitnätverk kan vara ett utsatt system. Satellitkommunikation används i flera olika syften ombord ett fartyg däribland kommunikation och säkerhet. Ett sattelit kommunikationssystem förkortas SATCOM och består av satelliter i omloppsbana, landstationer med inkörsport på marknivå, VSAT (Very small aperture terminal) vilket är en tvåvägs satellitstation på marknivå utrustad med antenn samt ett NOC vilket är ett nätverkoperations center med övervakning, styrning samt hantering av sattelit nätverket. Satelliterna i ett sattelit kommunikationsnätverk är utrustade med ett flertal olika kommunikationstekniker för att kunna skicka och ta emot information genom andra satelliter såväl som landstationer.
På ett fartyg existerar VSAT samt land stationerna med inkörsport på fartyget tillsammans. Satelliterna kommunicerar direkt med mottagar/sändnings utrustningen på fartyget genom att siktlinjen mellan satelliterna och sändnings/mottagar utrustningen på fartygen görs möjlig vilken är nödvändig för kommunikation.
Antennerna monteras ute på fartyget så att vinkeln mellan satelliterna och fartygets mottagare/sändare bibehåller en siktlinje. Utrustning som små motorer möjliggör antennes förmågan att kunna arbeta mot att bibehålla en siktlinje så att kommunikation kan upprätthållas. Vidare underhålls NOC av en satellit operatör som skickar koordination och underhållsuppgifter till nätverket som vidare skickas till mottagaren.
Varje fartyg utgör därmed en sorts nod i ett nätverk som inkluderar fartygen i samma flotta samt dem som använder samma satellitoperatör. Några maritima satellit tjänster är INMARSAT,IRIDIUM samt globalsat där INMARSAT utgör den största tjänsten och är den enda som tillhandahåller den globala maritima nödmeddelanden och säkerhetssystemet tekniken vilken förkortas GMDSS. GMDSS tekniken erbjuder en rad olika tjänster, fartyg till land kommunikation via olika kommunikationstekniker och frekvenser, att kunna ta emot

.

kommunikation från landstationer till fartyg, sända och ta emot säkerhetsinformation, navigations information samt platsinformation. Säkerheten kring dessa tjänster är beroende av vilken operatör det är som sköter satelliterna.

Dessa aktörer är privata och deras säkerhetsstruktur som omger tjänsterna är därmed skyddat av regler som omfatta intellektuell egendom, vilken grad av säkerhet man upprätthåller blir därmed svårt att utvärdera. Krypterade anslutningar har upptäckts mellan VSAT antenner och inkörsportar till SATCOM nätverken vilket skapar problem med privat och skyddad användning av tjänster som är relativt osäkra så som e-mail eller HTTP internet sökning.

En rapport publicerad av säkerhets firman IOActive upptäckte att tjänster som erbjuds eller distribueras av INMARSAT är påverkade av svagheter inom säkerhet och skydd. Bakdörrar har upptäckts där det finns möjligheter att installera skadlig tredjeparts programvara. Via en bakdörr blir därmed inte brandväggar och säkerhetsmjukvara effektivt då man redan har gett INMARSAT åtkomst till sitt system.

Ytterligare svagheter upptäcktes i INMARSAT-C terminalen där luckor i säkerheten möjliggjorde ett scenario där man kunde stänga av fartygets säkerhets larmsystem. Detta system används av fartyg för att signalera om det är under attack av pirater eller terrorister, Vidare svagheter möjliggjorde attacker genom att man helt enkelt kunde ta kontroll över de motorer som styr VSAT antennens riktning och därmed dirigera om antennen så att sattelit uppkoppling inte kunde bibehållas. Satellituppkoppling används av system avgörande för navigation, kommunikation, räddnings koordination och säkerhet.
Nedan är olika system som använder INMARSATS satellituppkoppling.

- Telefon
- Internet
- Email-filöverföring
- Multi voice
- Videokonferens
- Säkerhet 505/Red button (Nödmeddelande vi pirat eller terrorist attack
- Notice to mariners
- Maritima hamnföreskrifter
- ECDIS
- Fartygs ruttsystem
- Lasthantering System
- Underhållningssystem/mjukvara
- Radio över IP (RoIP) via Walkie talkie
- VHF/UHF
- Telemedicin
- Väderrapportering

.

IOActive beskriver i sin rapport det räcker i teorin med att ett av dessa system skulle äventyras och falla offer för en lyckad attack för att hela SATCOM infrastrukturen skulle riskeras. Till industrier som använder sig av detta nätverk och tekniker hör förutom fartygsindustrin även militära organisationer, flygindustrin, media industrin, industrikomplex som oljeriggar, gas pipelines, vattenbehandlings verk, vindturbin parker och akut tjänster. Se Tabell 1. Fartygs teknologier och dess säkerhetsaspekter.

Tabell 1. Fartygs teknologier och dess säkerhetsaspekter. (Carpolu et al 2020)

Technology	Confidentiality	Authentication	Availability
GNSS	✗	✗	✗
AIS	✗	✗	✗
SATCOM	✗	✓	✓

2.6 Försäkring

I sin rapport beskriver Safety at Sea & BIMCO (2020) hur försäkringsläget kring att skydda sig mot IT-attacker har kommit att se ut.
Man menar att med den stora prislappen som kommer med en lyckad IT-attack (se maersk incident) har försäkringsbolag blivit en av dom större rösterna när det kommer till att öka medvetenheten inom IT-säkerhet. Stora ekonomiska förluster från maritima industrin vid lyckade IT-attacker innebär även stora kostnader för försäkringsbolagen. Den maritima logistiska industrin har stadigt börjat agera för att skydda sig själv och kravet på försäkringsprodukter har ökat.

Försäkringsbolagen har kommit med riktlinjer som verkar för att skapa tekniska förebyggande åtgärder mot IT-attacker. Vidare har försäkringsbolag uppmärksammat vikten av att utveckla planer som ska vara på plats när en incident inträffar. Dessa planer verkar för att snabbt kunna agera i ett data återhämtnings syfte. 2018 utförde BIMCO en undersökning publicerad i guiden av Safety at sea & BIMCO (2020) där dom undersökte om IT-attacker rederier hade utsatts för täcks av organisationens försäkring. Där IT-attacker täcktes av försäkringen svarade ⅔ att begäran om ersättning hade gjorts genom en specifik IT policy medans ⅓ hade gjort begäran om ersättning genom den traditionella P&I försäkringen.

Av de begärda utbetalningarna accepterades 16% varav 84% nekades utbetalning. Utvecklingen av IT-attacker mot den maritima industrin har gjort försäkringsbolag mer medvetna och engagerade i vad som är kundens skyldighet när det kommer till nivå av säkerhet. Ansvaret att upprätthålla en standard som möter kraven på vad som är sjövärdigt fartyg kan enligt Safety at sea, BIMCO (2019) delas in i två stycken krav.

1. Fartyg, besättning samt utrustning ska kunna motstå vad som anses vara vanliga risker,
2. Fartyget måste vara lämpligt att transportera frakten. Detta omfattar det fysiska tillståndet av fartyget, att lämpliga system existerar så som kommunikationssystem, navigationssystem samt korrekt bemanning.

.

Underlåtenhet att skydda dessa system, och i förlängning underlåtenhet att skydda ett fartyg mot en IT-attack kan tolkas som underlåtenhet att utöva vederbörlig aktsamhet för att göra fartyget sjövärdig. Vidare kommer det vara mer regel än undantag att försäkringsbolag kommer att titta på vad för förebyggande åtgärder man har vidtagit för att skydda kritiska system. Även om korrekt utbildning av personal har skett så att dessa innehar kompetensen samt möjligheten att agera i händelse av en incident.

Försäkringsbolagen kommer kontrollera att systemen har genomgått simulerade IT-attacks tester, att en återhämtningsplan finns, en reaktionsplan finns samt att tekniska åtgärder är på plats för att skydda systemen.

BIMCO, Safety at sea (2020) fann i sin undersökning att det är troligt att dom organisationer med en specifik IT försäkring kommer söka ersättning i större utsträckning än organisationer med en traditionell P&I försäkring. Man ansåg att dom som skyddas av en traditionell försäkring kan dra slutsatsen att det inte är ett alternativ att söka ersättning för att risken för att behöva argumentera för sin rätt är stor och därav avstår man.

.

3. METOD

3.1 Fallstudie

Arbetet grundar sig på en fallstudie där fokus ligger på ett fall av ett visst fenomen i syfte att ge en djupgående redogörelse för händelser, relationer, upplevelser eller processer som inträffar i det specifika fallet. I detta sammanhang är det är att undersöka svenska tankrederiers kostnader för IT-säkerhet i och med att resolutionen MSC.428(98) kom 2017 och blir lag första januari 2021. Vad rederierna anser är dom största IT-hoten är, möjliga kostnader i framtiden samt kostnader för It-säkerhet ombord. Fallstudien kommer utgå ifrån frågeställningen i sin helhet. Data från intervjuer kommer vara den primära källan till insamlad data för resultatet.

3.1.1 Deltagare & datainsamling

Datan tillhörande resultatet har uteslutande samlats in via intervjuer. Intervjuerna skedde med nyckelaktörer inom varje rederi. Nyckelaktörer valdes ut just för att de är specialister, experter, mycket erfarna och deras vittnesbörd medför en hög grad av trovärdighet (Denscombe 2010).

Människor i studien som intervjuas deltar specifikt för att de har en position inom rederiet som behandlar IT-säkerhet och ekonomiska kostnader kopplat till It-säkerhet vilket är relevant för oss som undersökare och för studiens syfte. En dialog fördes med samtliga rederier där den person som av rederiet ansågs vara mest kvalificerad för att svara på frågorna valdes ut som intervjuobjekt.

Målgrupp för intervjuerna är svenska tankrederier oberoende av storlek. Kontakt med rederierna inleddes via mejl med en introduktion kring ämnet och vilka frågor som vi som författare ville ställa, samt en beskrivning av studiens syfte. Vidare skedde intervjuerna digitalt eller via telefon efter att sekretess avtalet var undertecknat av båda parter. Intervjuerna genomfördes med förutbestämda frågor och teman. Se bilaga .1 för intervjumall.

3.1.2 Semi-strukturerade Intervjuer

Undersökningens datainsamling utfördes i kvalitativt form med semi-strukturerade intervjuer. Rederierna intervjuades angående deras ekonomiska kostnader och satsningar kring IT-säkerhet.

Med denna metod hade vi som intervjuare en specifik lista över frågor som ska behandlas och frågor som ska besvaras. Metoden tillät oss i form av intervjuare att vara flexibel när det gäller den ordning som ämnena beaktas, och kanske än mer betydelsefullt, att låta intervjuaren utveckla idéer och tala bredare om de frågor som forskaren tar upp (Denscombe 2010). Detta passar med studiens frågeställning som behandlar ämnet framtida kostnader kopplat till IT-säkerhet då det ger svar på specifika frågor men ändå öppnar upp för eventuella

.

följdfrågor. Även vad rederierna anser är dom största IT-säkerhetshoten kan vara specifika svar men variera från rederi till rederi och öppna upp för följdfrågor. Se bilaga 1.

3.1.3 Litteraturöversikt

Delen av studien som utgör litteraturöversikt är menat att fånga in en stor del relevant information för att konstruera teorikapitlet. För studiens innehåll angående IT-säkerhet är det av intresse att en klar bild av utvecklingen, tekniken, hotbilden inom sjöfartsindustrin representeras på ett sant sätt. Vidare grundar sig teoriavsnittet till en del på existerande resolution från IMO samt tillhörande guide från IMO. IMO hänvisar i sin guide för IT-säkerhetshantering till guider så som BIMCO samt mission secure vilka används för att vidare konstruera teorikapitlet.

3.1.4 Sökning

Litteratur inhämtningen påbörjades med en pilotsökning för att kunna hitta relevanta sökord. Områdets terminologi undersöktes innan sökord valdes ut. Efter en pilotsökning valdes sökordet “NOT” bort då det kan resultera att relevant information exkluderas. Sökorden Data security; Security issues; Vessel; Cybersecurity; Data protection; Computer security; Cybersecurity valdes och användes i chalmers biblioteksökning.

Systematisk sökning utfördes i flera steg i enlighet med modellen som återfinns i Noblit & Hare, 1988; Hesser & Andersson, 2015. Dom menar att sökningar i databaser inte är heltäckande och behöver kompletteras, därav gjordes även en omfattande frisökning samt att inga databaser exkluderades i Chalmers biblioteks sökning. Målet var ett uttömmande resultat där all relevant information för studien skulle fångas in. Materialsökning gjordes i Chalmers library med kombinerade sökord som återfinns nedan, sökningen skedde i samtliga tillgängliga databaser. Se bilaga 2 för sökresultat.

- Data security; Security issues
- Vessel; CyberSecurity
- Data protection; Computer Security; Cybersecurity

Frisökning gjordes för att införskaffa IMO:s guide för IT-säkerhetshantering samt IMO:s resolution för IT-säkerhet. Resolutionen samt guiden inhämtas från IMO:s hemsida. Vidare hämtades material för att beskriva händelseutvecklingen av föregående IT-attacker inom den maritima industrin, den spådda utvecklingen av IT-attacker i framtiden samt möjliga konsekvenser vid en lyckad attack.

.

Frisökningen skedde på google med nedanstående sökord.

- Vessel Cyber security
- Risk management
- IMO cyber risk management
- Computer security
- Maritime cyber security
- Computer science,

Frisökningen genererade samtliga nyhetsartiklar som har använts samt rapporten av CyRim som beskriver ett hypotetiskt IT-attack scenario. Vidare har nätverkssökning utförts där de guider som har använts för att konstruera teorikapitlet är samma som IMO hänvisar till i sin egen guide för IT-säkerhetshantering.

Rapporten av IOActive var utöver guiderna den enda nätverkssökning som gjordes. Rapporten refereras till i Vessels Cybersecurity: Issues, Challenges, and the Road Ahead av Caproul et al (2020) och behandlar IT-säkerhets luckor inom den tekniska utrustning som existerar ombord på fartyg.

3.1.5 Inklusion & Exklusion

3.1.5.1 Vetenskapliga artiklar & Guider.

Urval av artiklar bedömdes utifrån bedömningsmetoden som presenteras i Joanna Briggs Critical Appraisal Checklist (2017). I checklistan bedöms hur syfte, metod och resultat sammanfaller med syftet. Litteraturen kvalitet granskades med avseende på tillförlitlighet, relevans för frågeställningen samt tillämpbarhet. Checklistan fungerar även som ett verktyg för att säkerställa opartiskhet i litteraturen.

Material publicerat före 2017 som behandlar IT-säkerhetshantering har exluderats då dom faller utanför resolutionens tillkomst. Undantag har gjort för material publicerat före 2017 som behandlar utförda IT-attacker samt avsnittet som behandlar dom vanligaste formerna av IT-attacker samt säkerhetsluckor.

Dessa har inkluderats då dom inte behandlar ämnet riskhantering, åtgärder eller resolutionen. Guider publicerade före 2017 som behandlar IT-säkerhetshantering har exkluderat då resolutionens krav uppkom efter 2017. Filtering har gjorts gällande språk där språk utanför engelska och svenska har valts bort. Patent har exluderats. Artiklar utan peer review valdes bort. Undantag har gjorts gällande peer review av de guider som har använts då dom refererades till av IMO.

3.1.5.2 Frisökning

Mindre mediehus som producerade artiklar om samma incidenter valdes bort till fördel för större. Mediehusen som inkluderades är Wall street journal, BBC och Reuters. Undantag gjordes för Hellenic shipping news som producerade material från en undersökning av Naval

.

Dome som behandlade ökningen av antal IT-attacker. Samma material refererade Safety4sea till.

Både Naval Dome och Safety4sea har ansetts ha kredibilitet efter att ha bedömts genom Joanna Briggs Critical Appraisal Checklist därav anses innehållet i artikeln tillförlitligt. Dessa artiklar har använts i avsnitten “Tidigare incidenter samt “Bakgrund”.

Nyhetsartiklarna beskriver lyckade IT-attacker mot den maritima industrin samt ökningen av IT-attacker. Kredibiliteten av artiklarna bedömdes genom Credder. Credder är ett journalistiskt verktyg där journalister bedömer trovärdigheten hos ett mediehus, författare eller artikel. Efter att alternativa undersökningar eller analyser uteblev valdes nyhetsartiklarna ut som grund för att beskriva IT-attackerna. Se bilaga 3 för bedömning av nyhetsartiklar.

3.1.6 Intervju Etik

Då viss information som inhämtas av intervjuobjekten är av känslig art såsom ekonomiska kostnader, ekonomiska kostnadsökningar över tid, teknisk utrustning för IT skydd ombord samt IT-säkerhets sårbarheter förblir parterna som deltog i intervjuerna anonyma. Information som kan komma att identifiera verksamhet, organisation, rederi eller personer har exkluderats i enlighet med ett undertecknat sekretessavtal av intervjuaren och intervjuobjektet. Dessa åtgärder har vidtagits för att få rederier att delta i undersökningen samt för att värna om deltagarnas integritet. Sekretessavtalet återfinns i bilagor, se bilaga 4.

Det etiska förhållningssättet studien grundar sig på återfinns i Descombes (2010) praktiska undervisningsprinciper.

• deltagarna ska vara anonyma;

• informationen är konfidentiell;

• deltagarna förstår forskningens karaktär och deras involvering;

• deltagande är frivilligt;

Denscombe (2010) menar även att i egenskap av undersökare förhåller sig intervjuaren till följande undersöknings och intervju etik. Som undersökare arbetade vi utifrån denna intervju etik. För att kunna presentera seriositet, få rederier att delta och därav kunna presentera ett resultat förhöll vi oss även till samtliga nedanstående punkter.

• Forskarna ska vara professionella och integritetsfull

• Forskarna ska hålla sig inom lagen

• När forskarna har med deltagarna att göra så ska de vara öppna och ärliga, och inte begå något bedrägeri

• När forskarna har med kollegor att göra så ska de uppehålla en god standard och inte mixtra med resultatet

• Forskarna förväntas ta personlig säkerhet på allvar och inte utsätta sig själva eller kollegor för oacceptabla faror i deras sökning av information.

.

4. RESULTAT

Detta kapitel kommer presentera det resultat som har tagits fram baserat på de utförda kvalitativa intervjuerna. Resultatdelen är uppdelad i de fyra teman som har använts under intervjuerna och kommer redovisas tema för tema. Tema ett, budget och kostnader vill svara på vår första fråga om hur kostnaderna har förändrats från 2017. Tema två framtidssatsningar, vill svara på vår fråga om vilka framtida satsningar som sker inom IT-säkerhet och vad de kostar. Tema tre, finansiering, vill undersöka vilka system som har installerats på fartygen. Tema fyra, strategi och säkerhetshot, vill också undersöka vilka system som har installerats. Alla frågor inom ett tema är inte enbart till för att söka svar för just en frågeställning, fokus har främst legat på att få ett bra flyt i intervjun.

En rubrik med övriga diskussioner kommer presenteras som innehåller utvecklade diskussioner på de frågor som ställts. Alla deltagare fick erbjudande om komplett anonymitet och har valt att vara anonyma, alltså kommer inga namn på rederier eller de anställda som intervjuades att redogöras. Det kommer inte heller redogöras för vilka positioner de intervjuade har inom rederierna då vi anser att det hade varit att bryta mot den fullständiga anonymiteten som har utlovats. På frågor där svaren har skiljts sig avsevärt mellan respondenterna kommer rederierna att tilltalas som rederi A, B, C, D, E och F.

4.1 Tema ett, budget och kostnader

Tema ett innehåller frågor som handlade om rederiernas budget och kostnader. Här har rederierna svarat att inga kostnader har ändrats efter 2017, förutom rederi A som svarade att det har ökat något.

På andra frågan inom tema ett om vilka kostnader de har just nu har rederierna A, B, D, E och F svarat med specifika siffror där snittet har blivit på 180 000 SEK per år. Rederi C valde att inte svara. Se Tabell 2. Rederiernas IT-kostnader nutid.

Tabell 2. Rederiernas IT-kostnader nutid.

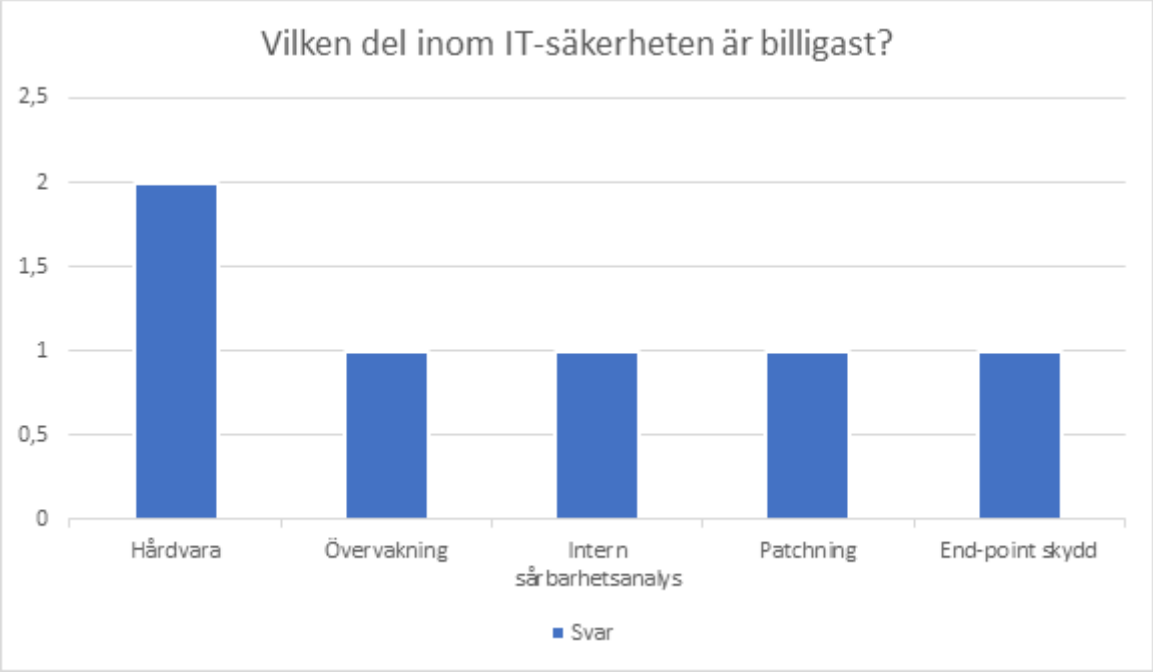
Respondenternas enskilda svar. Kostnad per månad.

.

När respondenterna fick fråga om vilken del inom IT-säkerhet som är dyrast har svarat unisont blivit personalutbildning. Rederi A utvecklade sitt svar genom att ange IT-avtalet som en stor kostnad, och specificerade att deras tre nybyggda fartyg kostade 500 000 SEK per år enligt IT-avtalet. IT-avtalet omfattar licenser, hårdvara, mjukvara och service. Rederi A gav inga siffror på personalutbildning men tyckte ändå att personalutbildning var en större kostnad om man räknade med kostnaden för utbildning och förlusten av arbetstimmar.

På frågan om vilken del inom IT-säkerheten som är billigast har svaren varierat. Svaren från de sex rederierna blev övervakning, intern sårbarhetsanalys, patchning, end-point skydd och hårdvara. Rederi C och F ansåg att hårdvara var den billigaste delen. Se Tabell 3. Billigaste delen inom IT-säkerhet.

Tabell 3. Billigaste delen inom IT-säkerhet.



Antal gånger ett svar angavs från de olika respondenterna.

Gällande frågan om respondenterna tror att kostnaderna kommer att öka efter 2021, har svaret blivit att det antagligen kommer att öka något men inte speciellt avsevärt från alla rederier.

.

4.2 Tema två, framtidssatsningar

Tema två innehåller frågor som har avsett att undersöka vilka framtidssatsningar rederierna har gjort inom IT-säkerheten. Första frågan i detta tema undrar om det finns några utbildningar angående IT-säkerhet i dagsläget och där har alla rederier unisont svarat att det finns.

När respondenterna blev tillfrågade om de tror att priset på utbildningarna kommer öka har de svarat att det troligen kommer att öka något, men inget rederi har givit en specifik siffra för ökningen de tror kan ske.

Fråga tre har sökt svar på om det är skillnad i kostnad på utbildningar som är riktade mot landsidan gentemot fartygssidan. Alla respondenterna svarade att utbildningarna är billigare på landsidan.

Om rederierna ser ett behov av att utöka resurserna ombord eller iland har svarat blivit ett simpelt nej från alla tillfrågade.

4.3 Tema tre, finansiering

Tema tre innehåller frågor som avser att undersöka mer specifikt vad olika byggdelar inom IT-säkerhet har kostat rederiet att bygga upp.

Första frågan söker svar på vad det har kostat att installera nytt system för IT-säkerheten och svaret har varierat grovt. Två rederier, (B och D) ansåg att frågan var omöjlig att svara på. Rederi E ansåg att det varierade för mycket mellan de olika fartygen för att ge ett bra svar.

Enligt det rederiet så beror variationen mellan fartygen på hur ofta man behöver tillkalla en tekniker till fartyget. Rederi F svarade också att det berodde på hur ofta man fick tillkalla en tekniker till de olika fartygen men nämnde inte att det varierade avsevärt mellan båtarna och gav siffran 300 000 SEK per fartyg. Rederi A, hade precis beställt tre hela system till tre nybyggen och svarade med siffran 375 000 SEK per fartyg. Rederi A utvecklade att hen ansåg att 10% av denna kostnad var specifikt för IT-säkerheten och resten var för att installera andra stöttande system som krävdes innan man kan installera systemet för IT-säkerhet. Det sista rederiet, rederi C, svarade följande;

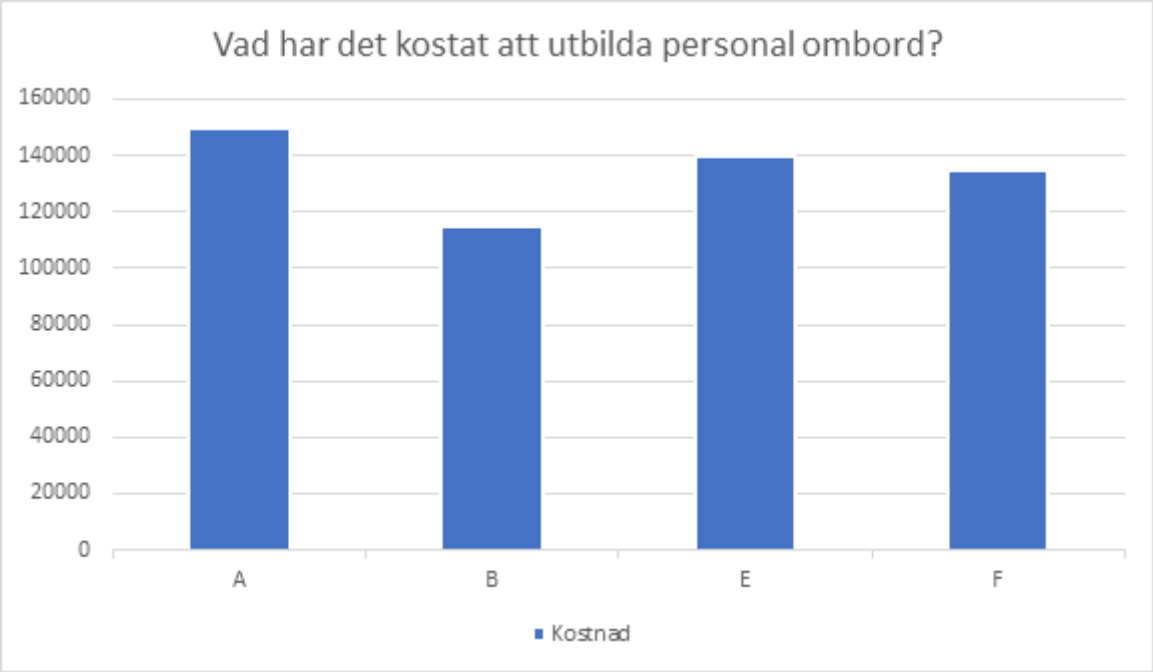
”Det beror på vilken produkt det handlar om samt om det är en mjukvara eller om det är hårdvara. Det är sällan eller aldrig det behöver komma ombord någon tekniker för dessa typer av produkter. Oftast är kostnaden inte mer än kostnaden för själva produkten och ev. frakt.” (Rederi C).

Andra frågan inom temat handlade om vad det har kostat rederierna att utbilda ombord personal. Rederi C och D sa sig inte veta vad utbildningar som har avsett IT-säkerhet har kostat. Rederi D utvecklade sitt svar med att det har varit många små utbildningar och att det därför är en svår kostnad att hålla koll på. Det fyra resterande respondenterna gav svar som tillsammans blev en medelkostnad på 135 000 SEK. Det ska nämnas att rederi A svarade

.

specifikt 150 000 SEK med siffror för år 2020, medan rederi B, E och F svarade med siffror som hade ursprung från rederiernas kostnader år 2019. Se Tabell 4. Kostnad personalutbildning.

Tabell 4. Kostnad personalutbildning.



Summa pengar de olika rederierna angav som svar. Kostnad per år.

När respondenterna blev frågade om vad det kostar på landsidan att installera nya system för IT-säkerhet svarade A, B, D och F att det kostade cirka 250 000. Rederi A utvecklade även här att hen ansåg att 10% av denna kostnad var specifikt för IT-säkerheten och att resten var för de stöttande systemen. Rederi C svarade att det berodde på vilken produkt det handlar om.

Temats fjärde fråga handlade om vad det har kostat att utbilda personal i land. Resultatet visar att det har varit avsevärt billigare att utbilda landpersonal, gentemot personalen ombord. Rederi A gav specifikt att kostnaderna för år 2020 var 25 000 SEK för utbildningarna. Resterande rederier svarade utan att ange siffror, men uttryckte att kostnaderna bara rörde internutbildning, intern introduktion och löpande information. Rederi F svarade;

”Inget mer än internutbildning, intern introduktion och löpande information.” (Rederi F).

.

När respondenterna tillfrågades om deras rederier kommer att ha de ekonomiska resurserna till att hålla jämn takt med vad lagar kan kräva i framtiden svarade alla rederier positivt. Rederi As representant uttryckte sig så här;

”Ja, det tror jag. Vi har inget val, så det måste ju bli ett ja på den frågan.” (Rederi A)

4.4 Tema fyra, strategi och säkerhetshot

Frågorna inom tema fyra hade avsikt att undersöka vad rederierna har för strategi kring IT-säkerheten, samt att undersöka vilka eller vilket hot som ansågs vara allvarligast. Tema fyra inleds med att fråga vad man har installerat på fartygen för att öka säkerhetsnivån. De olika svaren på den frågan redovisas Tabell 5. Åtgärder kring IT-säkerhet.

Tabell 5. Åtgärder kring IT-säkerhet.

Antal gånger ett svar angavs från de olika respondenterna.

När respondenterna blev tillfrågade om det fanns någon skillnad i strategi mellan land- och fartygssidan, svarade alla rederier att landsidan var mer affärs- och användarorienterad och att IT-säkerhet åtgärderna var avsedda för att underlätta för de anställda. Rederi B utvecklade;

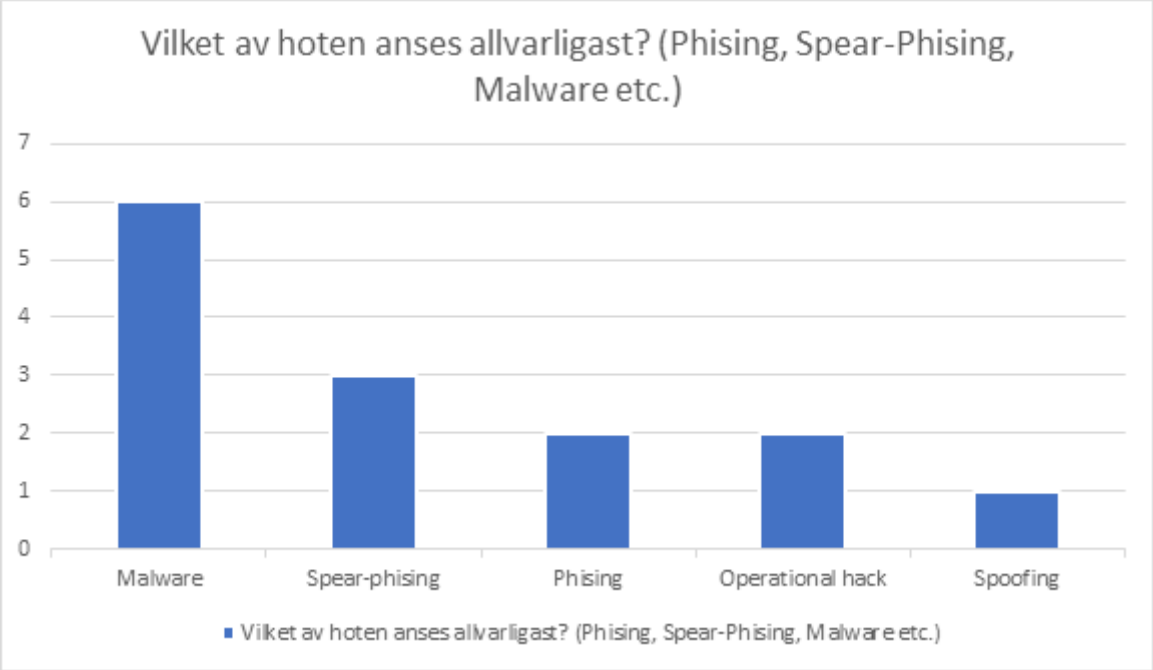
”Åtgärderna på landsidan handlar mer om att göra det svårare för våra anställda att, av misstag då, trycka på till exempel ett scam e-mail. Om man lyckas filtrera ut dessa risker blir det då lättare att arbeta för att man inte behöver hela tiden akta sig för olika fällor.” (Rederi B).

.

På fartygssidan var det mer säkerhets orienterat ansåg rederi A, B, D och F. Rederi C och E ansåg att fartygssidan var system fokuserad.

Tredje frågan sökte svar på vilket hot som ansågs vara störst mot fartygen. Här skiljde svaren något mellan respondenterna. Det hot som dock återfanns i alla rederiers svar var malware. Rederi A utvecklade sitt svar med att förklara att hen ansåg malware vara det troligaste hotet men att ett operational hack skulle kunna ha störst konsekvenser. Se Tabell 6. Allvarligaste hoten.

Tabell 6. Allvarligaste hoten.



Antal gånger ett svar angavs av de olika respondenterna.

Intervjun avslutades med att fråga om vilket hot som är störst mot organisationen. Rederi B, C, D, och F svarade att de ansåg att en lyckad spear-phising attack är det största hotet. Rederi E ansåg att den egna personalen utgjorde det största hotet. Rederi A svarade att hen tyckte att servicetekniker, anställda av andra företag, som kommer ombord är det största hotet.

”Skulle jag vara terrorist så skulle jag se till att bli anställd som servicetekniker för fartyg.” (Rederi A).

.

4.5 Övriga diskussioner

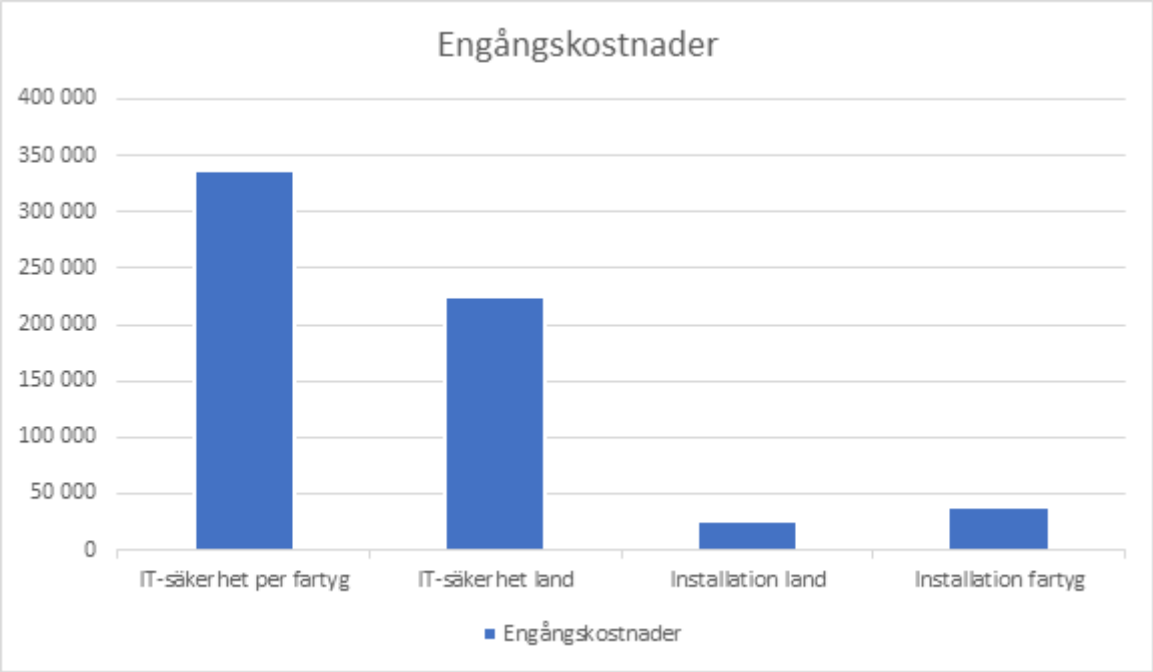
Vid diskussioner kring om huruvida rederierna anser att dom uppfyller resolutionen från IMO ansåg samtliga att dom har arbetat i enlighet med vad resolutionen kräver och uppfyller den. Rederierna anser inte att dom kommer att ha några ekonomiska problem att uppfylla eventuella hårdare krav på IT-säkerhet i framtiden samt att dom inte har något val ändå. Samtliga rederier har primärt använt sig av IMOs guide för att implementera IT-säkerhet ombord på fartyg samt på landsidan. Man anser sig ha goda möjligheter av värja sig mot eventuella försök att utföra IT-attacker. Vid diskussioner kring säkerhets svagheter inom AIS,GNSS och satellitutrustning ansåg man sig inte ligga till större risk för att utsättas för ett angrepp genom satellit utrustningen. På samma ämne ansåg en deltagare att dom flesta angreppen görs mot besättningsmedlemmar genom malware och risken för att ett angrepp skulle komma genom AIS,GNSS eller sattelit bedömdes som mindre. Försäkringar ansåg man täcker nuvarande troliga scenarier och är tillräckliga. Fyra av sex rederier hade en specifik IT-försäkring istället för en P&I då man ansåg att den inte var fullt lika täckande. Vid diskussioner kring varför priset på IT-säkerhet inte har ökat eller har ökat marginellt från 2017-2021 ansåg man att det är på grund av konkurrensen inom den marknaden. Rederierna menade att den industrin växer snabbt och aktörerna på marknaden som tillhandahåller IT-säkerhetstjänster är så pass många att priset trycks ner. Vid diskussioner kring om kostnaderna för IT-säkerhet är stora i ett sammanhang för utgifter överlag ansåg samtliga att kostnaderna är nödvändiga och att dom inte har något val än att spendera vad det kostar på IT-säkerhet.

4.6 Övriga tabeller

Resultatet sammanställdes även i de två följande tabellerna, Tabell 7. Engångskostnader och Tabell 8. Löpande kostnader. Detta gjordes för att lättare kunna jämföra de olika rederiernas kostnader, samt att i presentationssyfte enklare kunna visa kostnader.

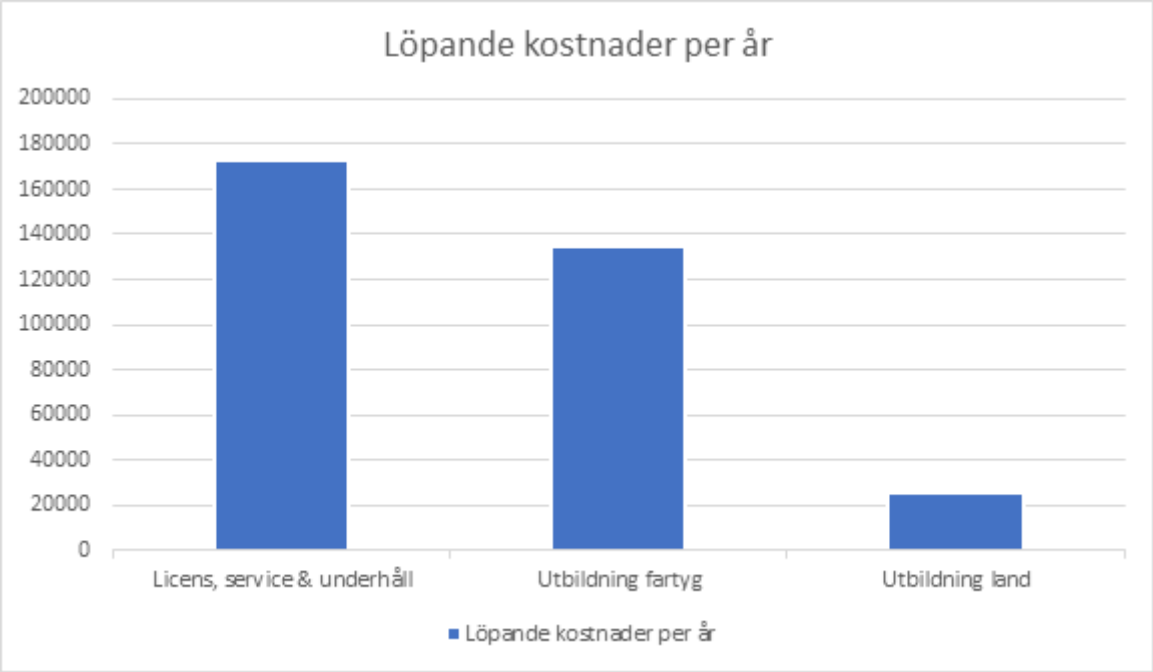
Tabell 7. Engångskostnader.

.



Engångskostnad för olika delar inom IT-säkerhet

Tabell 8. Löpande kostnader.



Löpande kostnader per år för olika delar inom IT-säkerhet. Kostnad per år.

.

5. DISKUSSION

5.1 Resolution & Guide

Resolutionens IMO 2017 (a) innehåll erbjuder inga konkreta åtgärder eller planer för att stävja IT-attacker. Den erkänner behovet av att IT-säkerhet behöver existera på en högre nivå idag än vad den historiskt har gjort. Att hela den maritima industrin ska gemensamt arbeta mot att säkra branschen mot hot och sårbarheter. Det ska finnas ett riskhanteringsplan på plats i fartygets SMS samt att rederier har försäkrat sig om att säkerhets hanteringen har blivit tillräckligt adresserad till den första januari 2021. Guiden IMO (2017, b) lanserades i samband med resolutionen och där nämns först dom system man anser vara kritiska och sårbara för IT-attacker. Dessa är bla bryggsystem, navigations utrustning, maskin, framdrivning med flera, se rubriken riktlinjer för IT-säkerhetshantering av IMO för flera punkter.
Här adresseras hur hot kan uppstå i olika former och hota dom kritiska systemen. Man definierar fem punkter för ett riskhanterings ramverk kan behöva att se ut. Punkterna behandlar implementering av riskkontroll, identifiering av åtgärder och aktiviteter som ska skydda fartygen system. De mest konkreta behandlar nödvändigheten av att ha ett back-up system. Vidare utvecklar guiden riskerna med sårbarheter inom det operationella området, informationstekniska området samt sårbarheter genererat av designen kring nätverk och system. Bristen på tydlighet kan ligga till grund för olika tolkningar av resolutionen. Vad som konkret behöver göras för att skydda dom operationella systemen och dom informationstekniska system beskrivs inte. Man hänvisar till sekundära guider. Detta kan i slutänden resultera i att vissa maritima organisationer inte uppnår den nivå av säkerhet som resolutionen kräver. Även att missa att implementera åtgärder för att skydda eventuella sårbarheter. En total genomgång av fartygs systemen skulle kunna göras för att mer tydligt och konkret identifiera sårbarheter. Därmed utveckla en guide som presenterar åtgärder och lösningar för att uppnå en tillräcklig nivån av skydd.

5.2 Känsliga system & attacker

Resultatet visar en satsning på att stävja attacker och täppa till sårbarheter som genereras genom tredjeparts åtkomst. Åtgärderna behandlar främst malware och phising. Ayala (2016) beskriver malware som skadlig programvara som är utformad för att komma åt eller skada en dator utan ägarens vetskap. Attacker kan komma via dator och mobiltelefon utrustning från land personal eller besättning. De intervjuade rederierna har satsat på att skapa policy, förbjuda flyttbar teknologi så som usb stickor, segregera nätverk, e post filter samt begränsade rättigheter. Alla dessa åtgärder är alltså i linje med att stävja hot som kan uppstå utifrån via mail, usb stickor eller datorer. Satsningen tyder på att man anser att malware och spear-phising är dom största hoten. Detta kan tolkas som att man även anser att dom flesta attacker sker mot användare och inte direkt mot systemen. Rederiernas satsningar lämnar en del frågor kring säkerheten av dom operationella systemen. Man skyddar delvis genom nämnda åtgärder men svagheterna som finns i AIS,GNSS och sattelit kommunikationen som beskrivs av

.

Caprolu et al (2020) talar för att det behöver göras åtgärder för att skydda dom operationella systemen ombord. Dessa system ingår i guiden av IMO som system som ska skyddas mot IT-säkerhetshot. IMO 2017 (b) beskriver att sårbarheter som är exponerade inom operationella eller informationstekniska områden där åtkomsten sker direkt via brister i lösenordsstyrka eller indirekt via nätverk som inte är segregerade kan det ha konsekvenser för integriteten, säkerheten och konfidentialitet. Speciellt där kritiska system exponeras för sårbarhet eller åtkomst så som navigations utrustning eller framdrivnings utrustning
Om åtkomsten till kritiska system kan ske genom AIS,GNSS och sattelit teknologin äventyras hela fartygets integritet.

5.3 Försäkring

Enligt BIMCO & Safety at seas (2020) är det främst försäkringsbolagen som har drivit på arbetet med att göra rederier medvetna om riskerna vilket kan ligga till grund för att det finns luckor i satsningarna som görs ombord på fartygen. Försäkringsbolagen har tolkat IT-säkerhetsåtgärder som att det ska spegla fartyget sjövärdighet. Fartyget måste vara lämpligt att transportera frakten. Detta omfattar det fysiska tillståndet av fartyget, att lämpliga system existerar så som kommunikationssystem, navigationssystem samt korrekt bemanning. Underlåtenhet att skydda dessa system, och i förlängning underlåtenhet att skydda ett fartyg, mot en IT-attack kan tolkas som underlåtenhet att utöva vederbörlig aktsamhet för att göra fartyget sjövärdig. Inom ämnet försäkring belyser vi vad försäkringsbolagen anser. Konsensus verkar vara att det kommer vara mer regel än undantag att försäkringsbolag kommer att titta på vad för förebyggande åtgärder man har vidtagit för att skydda kritiska system. Enligt BIMCO och Safety at seas (2020) undersökning 2018 nekades 84% av rederier utbetalningar för IT-attacker. Att inte se över sårbarheterna i system som AIS, GNSS och satellit kan vara en av anledningen till att många nekas. Det verkar finnas ett glapp mellan vad försäkringsbolagen anser att man ska göra ombord för att stävja IT-attacker och täppa till sårbarheter och vad man tolkar att IMOs resolution anser att man ska göra.
Försäkringsbolagen anser även att utbildning inte räcker om man inte har satsat tillräckligt på förebygganden åtgärder (BIMCO och Safety at seas 2020). Även om kompetensen finns för att upptäcka äventyrade system så måste det finnas andra förebyggande åtgärder på plats för att stävja en IT-attack.

5.4 Resultat

Resultatet visar att utbildning är bland det mest kostsamma för rederier vilket kan vara på grund av att det är bland det dyraste men kan även innebära en satsning i övervikt på just det området. Vad som även gör utbildning kostsamt är att det faller under löpande kostnader. Utbildning behöver kontinuerligt genomföras på grund av uppdateringar i innehållet samt personalomsättning. Dom tillfrågade rederierna ansåg att utbildning var den största kostnaden. Resultatet visar att den inte är den största kostnaden utan näst störst efter license,service och underhåll. Det kan finnas flera olika förklaringar till att man anser detta. Men det väcker

.

frågor kring hur bra koll man har på vad man lägger resurser på. Dom sammanlagda kostnaderna för IT-säkerhet ombord på fartyg har inte ökat mellan 2017-2021. Mot bakgrunden av att försäkringsbolagen nekar 84% ersättning för IT-attacker kan det anses intressant att omkostnaderna för IT-skydd inte har ökat. I kapitlet tidigare incidenter återgavs Mission secures (2020) IT-säkerhetsguide. Deras undersökning visar att en ökning med 400% av utförda försök till IT-attacker riktade mot den maritima industrin har skett från juni till februari 2020. Frågan väcks om rederierna som har undersökts verkligen gör tillräckligt för att stävja IT-attacker.

5.5 Tredjepart & OEMs

BIMCO och safety at seas (2020) menar att flera rederier inte skulle inhandla produkter eller system som visar sig ha kritiska sårbarheter. Ändå existerar dessa produkter och system som nödvändig utrustning och en kritisk del för att fartyg ska kunna upprätthålla sjöduglighet. Tidigare i arbetet under rubriken som behandlar OEMs nämndes problemen som finns med att identifiera sårbarheter inom OEM produkter. Den mindre mängden produkter som serietillverkas innebär att de finns mindre resurser för att kunna erbjuda säkerhetslösningar, riskhantering tidigt och att i produktionsfasen kunna upptäcka eventuella sårbarheter. Oavsett om man anser att ansvar för säkerheten ska ligga på tillverkaren eller hos fartygen så talar försäkringsbolagen kring vikten av tidiga åtgärder. Det kan anses att för att säkerställa att man behåller skyddet försäkringarna ger bör fartygen arbeta för att implementera säkerhetsåtgärder inom de områden man identifierar svagheter inom, även vara medveten om att OEMs kan ha svagheter och skapa åtgärder för dessa. Simuleringar ska kontinuerligt ske och resultatet speglar att man testar systemen ombord på fartygen för att kunna identifiera sårbarheter (BIMCO & Safety at seas 2020). Även om vi inte vet exakt vilka system som testas eller vilka sårbarheter som upptäcks kan det anses att de det verkar finnas en grad av medvetenhet baserat på resultatet kring sårbarheterna som behandlar AIS, GNSS och sattelit vilka Caprolu et al (2020) beskriver men inte tillräckligt med satsningar för att åtgärda svagheterna. Man anser att ansvaret inte helt är rederiets.

5.6 Metoddiskussion

Fallstudie valdes som metod för att undersöka kostnader, strategier, finansiering och framtidssatsningar kopplat till IT-säkerhet på ett fördjupat sätt och i relation till att resolutionen MSC.428(98) kom 2017 och blir lag första januari 2021. Fallstudie möjliggör en djupdykning i ett fenomen vilket passar studien då den undersöker dessa teman från 2017-2021. För studiens syfte lämpar sig även fallstudie då fallet har en utmärkande identitet och är studerat i ett isolerat sammanhang. Fallet i studien har en tydlig avgränsning och är en fristående enhet. Enligt Denscombe (2010) är nackdelen med att göra en fallstudie är att det kan vara svårt att dra slutsatser utifrån insamlad data. I och med att ett fördjupat sätt används och att ett specifikt fenomen studeras blir mängden data relativt liten. Datan som samlats in blir i sammanhanget svår att analysera och dra slutsatser ifrån. Exempel finns i studien

.

gällande just kostnader. En bild av vad IT-säkerhetskostnader utgör av de sammanlagda driftkostnader för rederier hade behövts att presenteras för att det skulle kunna gå att analysera om utgifterna är stora eller små i ett större sammanhang. Datan representerar inte ett bild av om kostnaderna är märkbara för rederierna eller försumbara i det större sammanhanget. Antalet deltagande tankrederier blev sex stycken vilket kan anses vara få i antal. Mot bakgrunden av antal tankrederier i Sverige är ca 32st enligt trafikanalys rapport (Svensk sjöfarts konkurrenssituation 2012) kan sex av 32 anses vara en svag representation av industrin. Det svaga deltagandet påverkar även vilka åtgärder som tillämpas för att skydda systemen ombord och iland mot IT-attacker. Det kan inte anses vara fullt representativt för vad rederier satsar på för åtgärder.

Initialt gjordes ett försök att undersöka bokslut i syfte att ta reda på kostnaderna. Iden var att fördjupa sig mer i IT-säkerhet, installerade system, hårdvara och framtida syn på utvecklingen av system via intervju samtidigt som kostnads frågorna skulle besvaras med bokslut. I bokslut redovisas inte uppgifter av denna art i en egen kolumn som specifikt märkt IT-säkerhet eller dylikt. Samtliga kostnader som hanterar IT-säkerhet, utbildning av personal inom ämnet, granskningar utifrån av tredje part och investeringar i IT-säkerhetssystem redovisas som övriga utgifter och blandas med utgifter som inte relaterar till IT-säkerhet. Detta innebär att resultatet inte kan valideras eller styrkas med andra uppgifter. Eftersom det inte gick att använda bokslut som grund valdes det att göra en semi strukturerad intervju där svar kunde fås på specifika frågor gällande kostnader och även diskussioner kring framtida kostnader, regelverk etc.

Material sökningen gav flera resultat som användes för att bygga ett teorikapitel. Främst inom olika typer av IT-attacker, känsliga system samt tredje part & OEMs. Sämre resultat genererades gällande försäkring, dess kostnad, täckning samt nuvarande IT-säkerhets utgifter som rederierna kan tänkas ha. Inga alternativa källor genererades utanför intervjuerna ang kostnader och utgifter. Materialet som behandlar försäkring genererades via BIMCO & Safety at seas undersökning men inga alternativa källor hittades. Således kan det inte styrkas att försäkrings situationen är representativ.

Ämnets aktualitet gav oss generella svårigheter att hitta vetenskapliga artiklar som behandlar frågeställningens kostnadsaspekt. Då undersökningen primärt lutar sig på intervjuer när det kommer till att generera svar på frågeställningen som behandlar kostnader kan det anses tunt när resultatet som presenteras inte styrks av några vetenskapliga källor. Resultatet ger därmed en indikation och kan inte anses vara fullt representativt.

5.1.1 Intervjudiskussion

Intervjuerna som vi genomförde med de sex rederi representanterna tog alla plats över telefon. Eftersom det var första gången som vi har varit intervjuare kan detta ha lett till ett antal problem. Exempelvis ledande frågor och dåligt formulerade frågor. Enligt Denscombe (2010) finns det åtta punkter man ska följa för att få ett bra resultat när man har en intervju. Dessa punkter behandlar intervjuteknik.

.

Vi var medvetna om dessa punkter innan första intervjun gjordes då en pilotintervju utfördes men vi fann problem med att följa dom intervju tekniska punkterna. Det ska nämnas att även ifall man följer dessa åtta punkter perfekt betyder inte det att en intervju genast blir bra. Vissa intervjuer gick avsevärt mycket smidigare och bättre än andra intervjuer. Detta kan självklart berott på oss och våran ovana vid att hålla intervjuer, vilket i sin tur kan ha påverkat resultatet vi har fått.

Även vissa av våra frågor kan i efterhand varit ledande, till exempel löd tredje frågan i tema fyra; *Vilket av hoten anses allvarligast? (Phising, Spear-phising, Malware etc)*, vilket kan påverkat svaret vi har fått. Alla sex rederier svarade att malware var ett av de största hoten och det kan ha varit för att vi precis hade nämnt malware som ett exempel i frågeställningen.

Ett annat problem som uppstod under intervjuerna var att respondenterna nekade att svara på vissa frågor. Detta hände inte ofta men på ett par frågor valde de att säga att de inte visste eller rakt nekade att ge ett svar. Detta kan ha berott på vissa frågors känsliga natur, främst frågor om ekonomiska uppgifter. Då vi visserligen fick svar som angav exakta siffror för kostnader så hände det också att några respondenter inte ville svara med siffror utan gav mer övergripande svar istället vilket innebar att vi fick tolka informationen. Vi valde att inte pressa dessa frågor hårdare under intervjuerna då det kändes som att det hade varit opassande även om det hade kunnat ge ett bättre resultat. Överlag var dock de flesta öppna med sina ekonomiska kostnader.

.

6. SLUTSATSER

Resultatet ger en fingervisning om vad som utgör den största kostnaden för rederierna. Även vart den strategiska fokusen ligger för att stävja IT-attacker. Resultatet ger även en fingervisning kring att det existerar ett glapp mellan vad försäkringsbolagen anser att man ska uppnå i IT-säkerhet samt vad rederierna faktiskt uppnår. Ämnet behöver undersökas mer då resultatet enbart bygger på BIMCOs undersökning samt att fyra av sex rederier inte hade en P&I försäkring. P&I ansågs inte vara lika täckande, i vilken utsträckning eller vart försäkringen skulle ha brustit har inte undersökts vidare. Undersökningen ger en indikation och kan inte tolkas som representativ i full utsträckning.

6.1 Kostnadernas förändring

Enligt resultatet har kostnader för IT-säkerhet inte ökat från 2017-2021. Löpande kostnader har förblivit ungefär samma per år. Vad som påverkar sammanlagda kostnader per år är om rederier som inte betalar löpande för service behöver tillkalla service tekniker. Enligt resultatet är den kostnaden 300 000 SEK per fartyg. Den potentiella kostnaden berör enbart ett rederi som inte betalt löpande för tjänsten.

6.2 Installationer ombord

När vi undersökte vilka system för IT-säkerhet som har installerats på fartygen fick vi många olika svar, men det alla rederier hade gemensamt var att utbilda personal och förändra deras egna policy. Fem av Sex tillfrågade hade installerat fler brandväggar och gjort procedur förändringar, andra populära åtgärder var att förbjuda flyttbar teknologi, segregera nätverk, servrar från olika tillverkare och begränsa rättigheter. Den främsta strategin på både land och sjösidan är att minska chansen att personal ska göra fel. Se Tabell 5. Åtgärder kring IT-säkerhet, kap 4.4 s22.

6.3 Kostnader

IT-säkerhet per fartyg omfattar den största engångskostnaden. Kostnaden omfattar hårdvara mjukvara. IT-säkerhet i land omfattar den näst största kostnaden och omfattar även den hårdvara och mjukvara. Följande är engångskostnader för installation av hårdvaran och mjukvaran ombord på fartyg och iland. Där installationskostnaden är något högre på fartyg.

Licens, service och underhåll utgör den största löpande kostnaden per år. I kostnaden ingår service av både mjukvara samt hårdvara och underhåll av dessa system. Utbildning är den näst största löpande kostnader. Dom tillfrågade rederierna ansåg att utbildning var den största. Resultatet visar att den inte är den största kostnaden.

Det går inte att dra slutsatsen att kostnaderna representerar vad utgifterna är för fartygen. Av dom sex deltagande rederierna har svaren på frågorna varierat. Det har förekommit olika tolkningar av frågorna och därmed olika svar. Dom presenterade engångskostnader och

.

löpande kostnader bygger på svar från intervjuobjekten där svaren emellanåt har behövts att tolkas av oss som intervjuare. En viss fel representation kan därmed förekomma.

Land kostnader representeras av fyra av sex deltagare. Utbildningskostnader representeras av fyra av sex deltagare. Den genomsnittliga kostnaden per år för licenser, service och underhåll bygger på svar från fem av sex deltagare. IT-säkerhetskostnader per fartyg bygger på svar från en av sex deltagare.

Undersökningen ger stöd för att rederier hellre väljer en specifik IT-säkerhets försäkring än att låta P&I täcka fartygen vilket var i linje med vad BIMCOs undersökning fann. Fyra av sex rederier angav att dom omfattades specifik försäkring som täcker IT-säkerhet.

6.4 Framtida satsningar

Vår sista fråga ville undersöka vilka framtida satsningar som sker inom IT-säkerhet och vad dessa kostar, denna fråga sökte främst svar genom intervjudelen Tema två, framtidssatsningar. Dock blev svaren på dessa frågor korta och intetsägande och det blev därför svårt att få fram ett svar på denna frågan. Detta hade till stor del att göra med de frågor vi valde att ställa under intervjun, något vi i efterhand förstod. Det enda vi fick fram genom våra frågar var att det fanns utbildningar för personal och att det är billigare att utbilda landpersonal än fartygspersonal.

6.5 Rekommendationer till fortsatt arbete

Vår undersökning pekade mot att det verkar finnas ett glapp mellan vad försäkringsbolag anser att man ska uppnå i IT-säkerhetsnivå och vad rederierna faktiskt håller för nivå. BIMCOs undersökning pekade på att det är en klar majoritet av rederier som inte får utbetalning av försäkringsbolagen vid IT-incidenter. Det hade varit intressant att brygga det gapet med en undersökning som redogör mer exakt för vad försäkringsbolagen anser är en tillräcklig nivå av IT-säkerhet. Även ta reda på vart det är som försäkringsbolagen anser att rederierna brister i sin IT-säkerhet. Är det exempelvis brister som har beskrivits i denna undersökning, ex AIS, satellit och GNSS eller är det andra brister som ligger till grund.

.

KÄLLFÖRTECKNING

Ayala, L. (2016). *Cybersecurity Lexikon*. Apress, Berkeley, CA

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF,
WORLD SHIPPING COUNCIL (2020) *The Guidelines on Cyber Security onboard Ships*.
Hämtad:https://www.bimco.org/about-us-and-our-members/publications/the-gudelines-o-cyber-security-onboard-ships

Bateman. Tom. (2013, 16/10). *Police warning after drug traffickers' cyber-attack.* Hämtad: https://www.bbc.com/news/world-europe-24539417

BIMCO & Safety at sea. (2020). *Cyber security whitepaper.*
Hämtad:https://ihsmarkit.com/Info/0819/cyber-security-survey.html

Paris. Costas. (2018, 25/6). *China's cosco shipping hit by cyberattack in U.S.*
Hämtad:https://www.wsj.com/articles/chinas-cosco-shipping-hit-by-cyberattack-in-u-s-1532548557

CyRim. (2019). *Shen attack. Cyber risk in Asia pacific ports.* Loyd's, London

Credder. (2019). Hämtad:http://www.credder.com

Hellenic shipping news. (2020, 21/7) *Maritime Cyber Attacks Increase By 900% In Three Years.* Hämtad: https://www.hellenicshippingnews.com/maritime-cyber-attacks-increase-by-900-in-three-years/

IMO. (2017, a) *Maritime cyber risk management in safety management systems.* IMO. Hämtad:
https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

IMO. (2017, b). *Guidelines on maritime cyber risk management.* Hämtad:
https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

IOActive. (2014). *A Wake-up Call for SATCOM Security.* Hämtad:
https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

.

Joanna Briggs Institute. (2017). *Critical Appraisal tools for use in JBI Systematic Reviews Checklist for Qualitative Research.* Hämtad:https://jbi.global/sites/default/files/2019-05/JBI_Critical_Appraisal-Checklist_for_Qualitative_Research2017_0.pdf

Maurantonio Caprolu, Roberto Di Pietro, Simone Raponi, Savio Sciancalepore, Pietro Tedeschi. (2020). *Vessels Cybersecurity: Issues, Challenges, and the Road Ahead.* IEEE Communications Magazine.

Martyn Denscombe. (2010). *The Good Research Guide: for small-scale social research projects. Fourth Edition.* Open University Press.

Mission secure. (2020). *A Comprehensive Guide to Maritime Cybersecurity*. Hämtad från:https://www.missionsecure.com/resources/comprehensive-guide-to-maritime-security-ebook

Reuters staff. (2019, 5/11). *Marine firm James Fisher reports cyber breach.* Hämtad:https://www.reuters.com/article/idUSKBN1XF1SQ

Transportstyrelsen. (2020, 6/10). *Aktuell information.* Hämtad:https://www.transportstyrelsen.se/sv/sjofart/Fartyg/sjosakerhetsarbete/aktuell-information/

Trafikanalys. (2012). *Svensk sjöfarts konkurenssituation.* Hämtad:https://www.trafa.se/globalassets/rapporter/underlagsrapporter/2011-2015/2012/svensk-sjofarts-konkurrenssituation.pdf

.

BILAGOR

Bilaga 1

Intervjumall

TEMA 1 Budget

Hur har kostnaderna ändrats efter 2017, då IMO:s Resolution MSC.428(98) adopterade?

Vilka kostnader har ni nu?

Vilken del inom IT-säkerheten är “dyrast”?

Vilken del inom IT-säkerheten är “billigast”?

Hur tror de att kostnaderna kommer att ändras efter 2021?

TEMA 2 Framtidssatsningar

Finns det några utbildningar för personal ombord/iland angående IT-säkerheten?

Tror ni att priset på utbildningar kommer att öka?

Är det skillnad i pris på utbildningar riktade mot landsidan/fartyget?

Kommer man behöva utöka resurserna ombord/iland?

TEMA 3 Finansiering

Vad kostar det att installera nya system för IT-säkerheten på fartygen?

Vad har det kostat att utbilda personal ombord i IT-säkerhet?

Vad kostar det på landsidan att installera nya system angående IT-säkerheten?

Vad har det kostat att utbilda personal iland?

Kommer ni att ha ekonomiska resurser till att hålla jämn takt med vad lagar kan kräva i framtiden?

TEMA 4 Strategi och säkerhetshot

Vad har man installerat/gjort på fartygen för att öka säkerhetsnivån?

Vilken skillnad i strategi finns det på landsidan gentemot fartygssidan?

Vilket av hoten anses allvarligast? (Phising, Spear-phising, Malware etc)

Vilket av hoten är störst mot fartygen?

Vilket av hoten är störst mot organisationen?

.

Bilaga 2

BILAGA 2. Sid 16

Databas/ Bibliotek	Sökord	Träffar	Lästa	Full text	Granskad	Använda
Chalmers Lib	Vessel Cyber Security	3569	3	2	2	1
Chalmers Lib	Data security, Security issues	1420	2	1	1	1
Chalmers Lib	Data protection; Computer Security; Cybersecurity	139421	5	3	2	1

Bilaga 3

BILAGA 3. Sid 18

Media	Kredibilitet Kritiker/Allmänhet	Antal bedömningar
Reuters	100% / 78%	10 – 49
Wall Street Journal	87% / N/A	15 – 4
BBC	75% / 74%	8 - 133

.

Bilaga 4

Andreas Meyer
Landalabergen 11
41129 Göteborg
Sverige
Telefon:0768406016

Tobias Öjbro
Lindholmsalen 25
41753 Göteborg
Sverige
Telefon:0768445515

Mail: Andreasmeyer.261@gmail.com
Mail: Tobias.ojbro@outlook.com

Postnummer och ort:

Land:

Organisationsnummer:

Rederi:

Telefon:

Säte:

Mot bakgrund att ovanstående Andreas Meyer & Tobias Öjbro studie deltagare, avser ingå i en studie tecknas nedan avtal om sekretess då uppgifter av konfidentiellt slag kan komma att lämnas.

1. Konfidentiell information

Konfidentiell information är information om företagen, oavsett slag, som kan komma att lämnas under parternas samarbete som berör kunskap, affärshemligheter eller annan information oavsett typ om vardera avtalsparten vars yppande kan komma att skada något av företagen.

2. Icke-konfidentiell information

Information som är allmänt veterlig, eller som avtalsparterna redan vet om varandra sedan innan samarbetets början, anses inte vara konfidentiell information.

3. Sekretessen gäller

Detta avtal om sekretess innebär att ingen utav avtalsparterna får lämna ut sådan konfidentiell information om varandra till någon utomstående, såsom personer, företag, myndigheter och organisationer.

4. Undantag från sekretess

Konfidentiell information kan dock ges ut om den ena avtalsparten tillåter den andra avtalsparten att göra detta, eller om myndighet beslutat att sådan information skall lämnas ut.

5. Återlämnande av konfidentiell information

Vid upphörandet av parternas samarbete skall konfidentiell information återlämnas. Återlämnande skall också ske om någon utav av avtalsparterna kräver detta.

6.Anonymitet

Deltagarna kommer vara anonyma, deltagande är frivilligt. Ingen information som kan identifiera företaget som deltar i studien kommer publiceras.

7. Övrigt

Om något bör tilläggas till avtalet kan detta skrivas här.

.

Andreas Meyer & Tobias Öjbro

Datum och ort
20/11 2020 Göteborg

Underskrift

Andreas Meyer & Tobias Öjbro

Namnförtydligande

Datum och ort

Underskrift

Namnförtydligande

INSTITUTIONEN FÖR MEKANIK OCH MARITIMA VETENSKAPER
CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige 2021
www.chalmers.se

CHALMERS