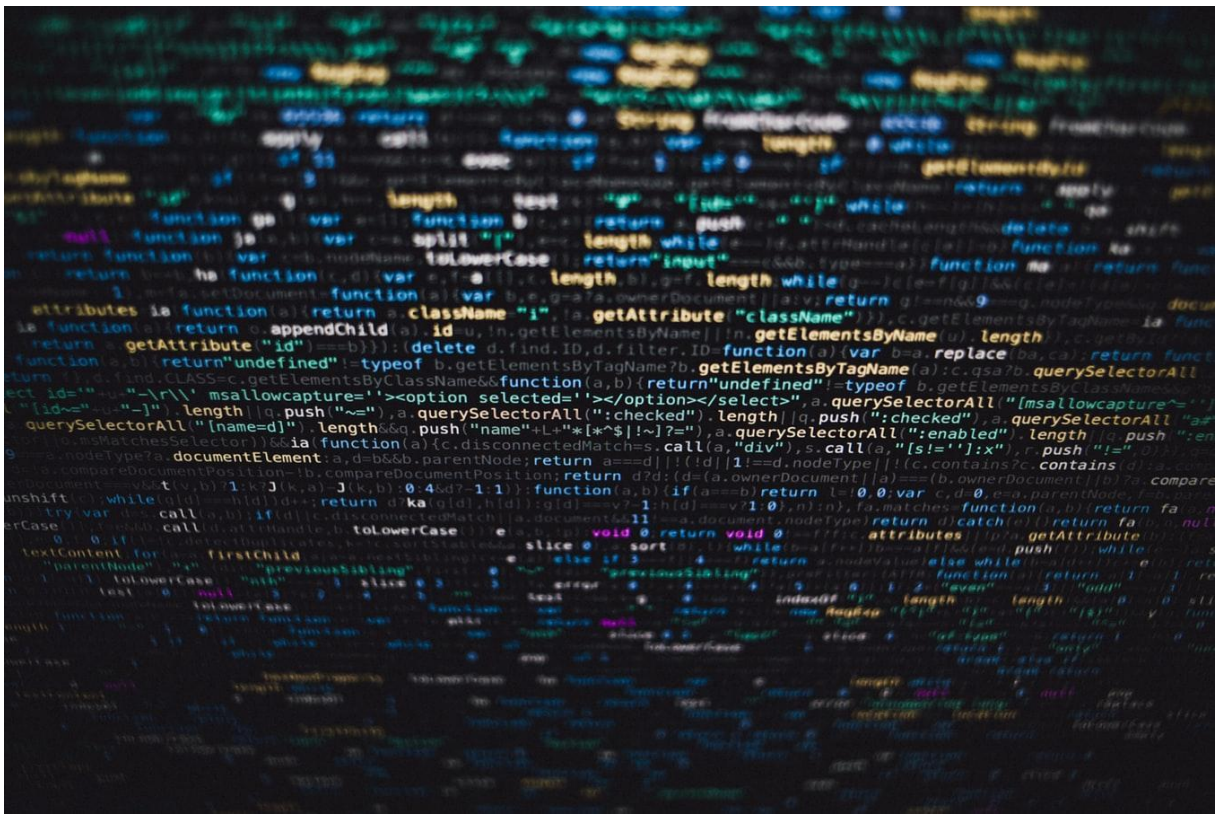
CHALMERS



Cyberhot 2000-talets största risk

Hur förberedda är svenska tankrederier inför IMO 2021?

Examensarbete för Sjöfart & Logistik programmet

NICLAS SVANSTRÖM
WILLIAM MEYER

Mekanik och maritima vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige 2020

Cyberhot 2000-talets största risk

Hur förberedda är svenska tankrederier inför IMO 2021?

NICLAS SVANSTRÖM
WILLIAM MEYER

Mekanik och maritima vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige, 2020

Cyberhot 2000-talets största risk
Hur förberedda är svenska tankrederier inför IMO 2021?
Cyberthreat the 20th centuries highest risk
How prepared are Swedish tanker owners for IMO 2021?

NICLAS SVANSTRÖM
WILLIAM MEYER

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

Omslag:
[Omslagsbilden visar en datorskärm innehållande kod.]

Tryckt av Chalmers
Göteborg, Sverige, 2020

Cyberhot 2000-talets största risk
Hur förberedda är svenska tankrederier inför IMO 2021?

NICLAS SVANSTRÖM
WILLIAM MEYER
Mekanik och maritima vetenskaper
Chalmers tekniska högskola

Sammanfattning

Det ökade antalet cyberattacker och incidenter på företag med anknytning till sjöfarten fick det globala organet för lagstiftning inom sjöfarten, IMO, att ta ställning till problemet. På sitt 98:e sammanträde godkändes kravet, MSC.428 (98), som kräver att rederier implementerar *Cyber Risk Management* i sina säkerhetsledningssystem. Målet med kravet är att öka medvetenhet och kunskap om cybersäkerhet inom sjöfartsindustrin. IMO har därefter utvecklat en resolution, MSC-FAL.1/Circ.3, innehållande rekommendationer för hur rederier bör implementera cybersäkerhet i deras verksamhet. Studiens syfte är att undersöka i vilken utsträckning svenska tankrederier är förberedda inför IMO:s kommande lagkrav som ska verifieras 1 januari 2021. Då lagkravet inte trätt i kraft än besvaras studiens huvudfråga med hjälp av tre delfrågor som undersöker nuläget, utmaningar med implementering samt vilken nivå på arbetet rederier tillämpat. Det är i denna studie viktigt att granska rederiernas nuvarande kunskap och erfarenhet, för att reflektera hur väl förberedda de är för framtidens krav. För att finna svar på detta genomfördes semi-strukturerade intervjuer med tre ledande rederier inom flytande bulktransport samt en IT-leverantör specialiserad inom cybersäkerhet. Studiens resultat indikerar att svenska tankrederier är förberedda inför det kommande lagkravet där arbetet ses som en viktig del i att bedriva säker sjöfart. Vidare tyder resultatet på att tankrederier arbetat med liknande lagkrav från inflytelserika organisationer redan 2018. Vidare upplever rederierna främst utmaningar i att leva upp till de tekniska kraven, där samtliga ser ett behov av stöttning från en extern IT-leverantör. Studien indikerar att nivån på arbetet för cybersäkerhet är högre än lagkravet. Sammanfattningsvis verkar rederier vara medvetna om cyberhoten och kommer sannolikt uppnå de nya lagkraven.

Nyckelord: IMO, ISM, SMS, Cyber Risk Management, Cyber Security, Cyber Attack

Abstract

The increased number of cyberattacks and incidents on shipping companies have caused the global organization of maritime legislation, IMO, to address the problem. At its 98th meeting a requirement was approved, MCS.428 (98), which require shipping companies to implement Cyber Risk Management in their Security Management Systems. The goal with the requirement is to increase awareness and knowledge of cyber security in the maritime industry. IMO has thereafter developed a resolution, MSC-FAL.1/Circ.3, containing recommendations on how shipping companies should implement cyber security in their operations. The purpose of the study is to investigate how well Swedish tanker companies are prepared for the upcoming legal requirement which should be verified 1 January 2021. Since the legal requirement has not yet come into force, the main question of the study is answered with the help of three sub-questions which examines the current situation, challenges with implementation and what level of work the shipping companies have applied. In this study, it is important to review the shipping companies´ current knowledge and experience, to reflect how well prepared they are for future requirement. To find answers, semi-structured interviews were conducted with three leading shipping companies in liquid bulk transport and an IT supplier specializing in cyber security. The study indicate that Swedish tankers are prepared for the upcoming legal requirement where the work with cyber security is viewed as an important part of conducting safe shipping. Furthermore, the results indicate that tanker companies worked with similar legal requirements from influential organizations as early as 2018. Furthermore, the shipping companies primarily face challenges in living up to the technical requirements where they experience a need for support from an IT supplier. The study indicates that the level of cybersecurity work is higher than the legal requirement. Overall, the shipping companies are well aware of the cyber threat and will likely be prepared to meet the legal requirements.

Keywords: IMO, ISM, SMS, Cyber Risk Management, Cyber Security, Cyber Attack

Förord

Författare till examensarbetet är Niclas Svanström och William Meyer, som under den sista terminen på programmet Sjöfart och Logistik vid Chalmers Tekniska Högskola besvarade studiens forskningsfrågor. Författarna vill rikta ett stort tack till alla respondenter som tagit sig tid och bidragit med erfarenhet, såväl som kunskap, till studiens resultat. Med given information förmedlar studien en aktuell uppfattning om hur väl svenska tankrederier är förberedda inför det kommande lagkravet. Tillika vill författarna tillägna ett stort tack till vår handledare, Johan Magnusson, som bidragit med nödvändig information och vägledning för att klara av att slutföra en kvalitativ uppsats av god kvalitet.

Innehållsförteckning

Figurförteckning

Tabellförteckning

Ordlista

COO - *Chief Operating Officer* är en anställd inom ett företag som erhåller en hög position. Bennett och Miles (2006) beskriver att det inte existerar en tydlig definition på vilka arbetsuppgifter som förknippas med COO, utan att det särskiljer sig mellan företag där storlek kan vara en avgörande. Vanligtvis överlåter företag allt ansvar för områden med operationellt fokus till COO, vilket inte allt för sällan inkluderar produktion, marknadsföring, försäljning och utveckling (Bennett & Miles, 2006).

CSO - *Company Security Officer* beskriver IMO (u.d.e) som en anställd som har ytterst ansvar för att utvärdera, förbereda och implementera säkerhetsplaner i rederiets verksamhet. IMO ställer krav på att alla medlemsstaters rederier måste tillhandahålla en CSO för att uppfylla de krav och kriterier som ställs från SOLAS-konventionen. Med en CSO har rederiet en ansvarig för att eliminera eventuella säkerhetshot (IMO, u.d.e).

Cyberattack - Ett försök utförs av en hackare med syfte att förstöra, alternativt skada, ett datorsystem eller nätverk (Lexico, u.d.a).

Cyber incident - Synonym till cyberattack.

Cyber Risk Management – Ett strukturerat arbete för cyber riskhantering.

Cyber Security - Cybersäkerhet.

Digitalisering - Enligt Gartner (u.d.) är digitalisering likställt med tillämpning av digital teknik med syfte att öka värdeskapande möjligheter samt intäkter. Med andra ord är det en process för att gå över till en mer digital verksamhet (Gartner, u.d.).

DoC - *Document of Compliance* är ett certifikat som bevisar att rederiets säkerhetsledningssystem (SMS) är godkänt i enlighet till de kriterier som ställs.

DPA - *Designated Person Ahsore* är en anställd inom en rederiverksamhet vars syfte är att vara länken mellan fartyget och landsorganisation. Ihre (2016) menar att DPA förknippas med rederiets säkerhetsorganisation och är länken mellan fartyg och land vid händelse av olycka. Arbetsuppgifter inkluderar också arbete med förberedelser av varierande risker i enlighet med SMS och ISM. (Ihre, 2016, s. 63).

DPO – *Data Protection Officer* är ytterst ansvarig för arbetet i uppfyllandet av de krav som ställs på en organisation för att skydda personal, kunder och leverantörers personuppgifter (European Data Protection Supervisor, u.d.).

Hackare - En person som hjälp med av en dator utför ett otillåtet intrång i syfte att erhålla obehörig data (Lexico, u.d.b).

IMO - *International Maritime Organisation* är ett underorgan till Förenta Nationerna med syfte att agera mellanstatlig samarbetsorganisation till flaggstaten. Organisationen ansvarar för sjösäkerhet och miljöskydd.

ISM - *International Safety Management code* är en kod som via referering är nära sammanlänkad till SOLAS. I koden beskrivs specifika krav för hur rederier bör arbetet med säkerhetsledning.

ISO 27 001 - Svenska institutet för standarder (u.d.) beskriver att verksamheter idag består av allt mer information. Information existerar inte bara hos IT-relaterade företag utan också inom andra industrier, exempelvis produktionsföretag. Värdet i informationen anknyts inte till tillgången utan värdet av informationen existerar i historia som ligger till grund för hur produkten tillverkas, vilka komponenter företaget använder och hur komponenterna monteras. Av den anledning är det viktigt för företag att skydda sin information men emellertid besitta okomplicerad tillgång till den vid behov. Svenska institutet för standarder (u.d.) menar att ISO 27001 hjälper företag att på ett strukturerat arbetssätt erhålla en bättre kontroll över säkerheten av dess information (Svenska institutet för standarder, u.d.). Calder och Watkins (2015) menar att det effektivaste arbetssättet för ett företag att arbeta med ISO 27001 är att implementera *Information Security Policy* (ISMS). Med hjälp av en ISMS policy visar företaget dess kunder och leverantörer att man identifierat risker inom verksamheten och implementerat effektiva processer för att skydda sig mot dessa (Calder & Watkins, 2015).

Managementbolag - Det var inte längesedan som fartyg drevs av en enskild aktör, så kallad redare, med eget ansvar för att driva fartygen operationellt, kommersiellt och tekniskt inom kapaciteten av företaget. Ihre (2016) menar att så är det inte längre, det finns flertal fartyg som trafikerar internationell trafik som drivs med hjälp av managementavtal. Avtalen inkluderar ett ansvarsområde, alternativt flera, där crew-, technical- och commercial management är några av de vanligt förekommande alternativen. Med hjälp av outsourcing av ett ansvarsområde överlåter redaren ansvaret till ett företag med specialiserad kunskap inom funktionen (Ihre, 2016).

MSC.428 (98) - Lagkrav från IMO som kräver att företag ska implementera *Cyber Risk Management* i sitt sjösäkerhetsarbete.

MSC-FAL.1/Circ.3 - Rekommendationer för hur rederier bör arbeta med cybersäkerhet.

OCIMF - *Oil Companies International Maritime Forum*.

SMS - *Safety Management System* är ett krav från ISM-koden som kräver att rederier och dess fartyg besitter ett bra säkerhetsledningssystem.

TMSA - *Tanker Management Self-Assessement*.

1 Inledning

Idag transporterar sjöfartsnäringen tillsammans upp till 90 % av volymen allt gods. Jones och Kimberly (2019) menar att sjöfarten anses vara en kritisk komponent för global tillväxt och ökad världsekonomi (Jones & Kimberly, 2019). Enligt Förenta Nationerna (UN, 2016) är sjöfartsindustrin ett av de viktigaste transportalternativen i och med dess omfattande nätverk av infrastruktur som anses vara en grundläggande faktor för ökad import- och exporthandel. Till följd av ökat antal handelsrutter uppdagas kontinuerligt ett infrastrukturnätverk som förser världens befolkning med essentiella varor (UN, 2016).

Transport av gods sker idag med varierande fartygstyper med hänsyn till konstruktion, utrustning och ålder. I avseende till vilken handelsvara som fraktas ombord fartyget har digitaliseringen utvecklats i olika takt, där artificiell intelligens och automation är två faktorer som drivit utvecklingen framåt. I sin tur har digitaliseringen lett till att fartyg idag är konstruerade med allt mer omfattande utrustning i form av operationella- och informationssystem. Men med digitaliseringens möjligheter finns även en baksida i form av nya hot och risker. Nya angreppssätt har etablerats till följd av fartygens ökade digitalisering vilket också innebär att industrin exponeras mot nya faror i syfte att inaktivera, skada eller förstöra. Cyberhot rankades 2013 på plats 15 av de största riskerna inom affärsverksamhet. Det har skett en exponentiell utveckling sedan dess och numera är cyberhot rankad som den största risken (Allianz, 2020). Munich RE (u.d) menar rentav att cyberhot är 2000-talets största risk. Orosmoment så som dataintrång förknippas alltmer med cyberattacker där företag som Maersk och COSCO blivit exempel på hur illa drabbad sjöfartsindustrin kan bli (Tam & Jones, 2019).

Till följd av den stigande hotbilden och utförda attacker har det globala organet för säkerhet inom sjöfart, IMO - International Maritime Organisation, tagit ställning till problemet. Sedan 2017 arbetar IMO med cybersäkerhet genom resolutionen, MSC-FAL.1/Circ.3. Resolutionen innehåller riktlinjer och rekommendationer som organisationen råder rederier att förhålla sig till (IMO, 2017a). Enligt Allianz (2020) finns det indikationer som tyder på att utvecklingen av hotet kommer att fortsätta framöver. Därmed har IMO beslutat att införa lagkrav på att rederier ska implementera *Cyber Risk Management* i sitt sjösäkerhetsarbete. Genom att implementera resolutionen, MSC.428(98), förväntas rederier öka aktsamhet och skydd (IMO, 2017a). Lagkravet är något som kommer få en stor inverkan på sjöfarten vilket bidrar till ett intresse hos oss som författare att undersöka hur redo svenska tankrederier faktiskt är för detta.

1.1 Syfte

Syftet med denna studie är att undersöka och skapa en djupare förståelse för IMO:s nya lagkrav om *Cyber Risk Management* som träder i kraft 1 januari 2021 samt hur redo tankrederier är för detta. Genom en kvalitativ datainsamling i form av semistrukturerade intervjuer utvärderas hur tankrederier arbetar med cybersäkerhet och om detta arbete är proaktivt eller reaktivt. Tillika belyser studien de risker ett rederi löper till följd av att agera passivt till den mer digitaliserade verkligheten. Vidare syftar studien till att undersöka vilka utmaningar rederier finner med resolutionerna samt om deras cybersäkerhet överträffar lagkraven genom att rederier tagit egna initiativ.

1.2 Frågeställning

I detta examensarbete behandlas följande huvudfrågeställning som besvaras med hjälp av tre underfrågor:

- Hur redo är svenska tankrederier inför de nya riktlinjer och krav som ställs från IMO 2021?
  - En nulägesbeskrivning av existerande kunskap och erfarenhet
  - Vilka utmaningar finns med implementeringen av resolutionerna MSC.428(98) och MCS-FAL.1/Circ.3 i rederiets säkerhetsledningssystem?
  - En analys av arbetsnivå som beskriver om tankrederier endast uppfyller kraven eller tas egna initiativ utöver dessa?

1.3 Avgränsningar

Sjöfartsnäringen är en globalt verksam industri där rederier kommer i kontakt med flera olika företag i varierande länder. Lagar och krav sätts på internationell basis, av den anledningen avgränsas rapporten till regelverk och lagar som stadgats internationellt. Studien avgränsas även geografiskt till företag med sjöfartsnäring inom Västra Götalands län. Vidare avgränsas undersökningen till gods i flytande form där företag med anknytning till flytande bulk kommer att intervjuas. Tillika baseras rapporten på konventioner av det globala organet IMO. Konventioner som avgränsar ämnet är ISM - International Safety Management Code och SMS - Safety Management System. Avsnitt om konventionerna avgränsas till ämnet cybersäkerhet, vilket resulterat i att flera avsnitt från konventionerna lämnas obesvarade i rapporten.

Eftersom studien utförs innan lagkravet har trätt i kraft bör hänsyn tas till att perspektiv från rederier och IT-leverantör kan komma att ändras efter verifikation av rederiernas DoC den 1 januari 2021. Det är först efter verifikation som rederierna besitter rätt auktoritet till att besvara om de lever upp till lagkravet eller inte.

2 Bakgrund

I detta kapitel redovisas en bakgrund bestående av information insamlat från tidigare utförda arbeten tillika vetenskapligt arbete. Med hjälp av detta kapitel förser författarna den bakomliggande information nödvändig till läsaren för att förstå varför ämnet är teoretisk och praktiskt relevant.

2.1 Bakgrund

Sjöfartsnäringen kan idag genom sitt globala infrastrukturnätverk och karaktär frakta stora volymer till ett förmånligt pris och är därmed ett ledande transportalternativ. Med hjälp av befintlig infrastruktur trafikerar rederiernas specialiserade fartyg handelsrutter världen över. Tam och Jones (2019) menar att fartygen tillsammans med dess ägare är verksamma på en marknad som förknippas med hård konkurrens och många krav. Till följd av dessa faktorer, tillsammans med önskan om kostnadseffektivitet, söker industrin nya system som kan underlätta arbetsbelastning och säkerhet. Resultatet leder till en snabbt växande utveckling av komplexa IT-system som möjliggör ökad effektivitet och säkerhet. IT-systemen definieras som IT - informationsteknologi och OT - operationsteknogolier. Tam och Jones (2019) menar att IT förknippas med navigation, kommunikation, sensorer och övervakning, medan OT utgör grunden för fartygets framdrivning, lasthantering och utrustning som används vid förtöjning och ankring. Tidigare nämnda system samarbetar tillsammans med den mänskliga faktorn för att tillsammans optimera utnyttjandet av fartyget. Men det är också dessa tre roller som konstaterats vara de största riskfaktorerna för den marina miljön. De moderna systemen ombord fartyg, tillsammans med den digitaliserade resa som utförs inom den landbaserade operationella sidan, ökar risken för cyberrelaterade attacker (Tam & Jones, 2019).

DiRenzo, Goward, & Roberts (2015) menar att industrins resa inom digitalisering introducerades av system såsom GPS - Global Positioning System, ECDIS - Electronic Chart Display Information System, AIS - Automatic Identification System och VDR - Voyage Data Recorder. Dessa är några av de system som bidragit till ökad säkerhet inom industrin. ECDIS är ett elektroniskt sjökort som förser besättningen ombord med ett sjökort innehållande realtidsinformation såsom fartygets position i förhållande till land och kartlagda föremål (DiRenzo, Goward, & Roberts, 2015). Systemet är anpassat för att integreras tillsammans med GPS, AIS och radar. DiRenzo, et al. (2015) beskriver att med utvecklingen av ECDIS tillåts fartyget att manövreras med en mindre besättning och i vissa fall med ensam vakthållning på grund av de navigationsrelaterade fördelarna som systemet förser. DiRenzo, et al. (2015) menar att ECDIS fördelar illustreras av containerrederiet Maersk fartygsklass Tripple-E, ett fartyg med en längd av 400 meter och en lastkapacitet av 18,000 containrar, som med hjälp av systemet kan drivas med en besättning av endast tretton personer. Systemen bidrar inte bara med fördelar utan innebär även viss risk. Det är dessa system som drastiskt exponerat industrin mot nya risker och sårbarheter i form av dataintrång (DiRenzo, Goward, & Roberts, 2015).

Sårbarheterna i systemen är tydliga när University of Texas-Austin tillsammans med forskarna Psiaki, O´Hanlon, Powell, Bhatti, Wesson, Humphreys och Schofield (2013) utför ett fjärrstyrnings

experiment på en 213-fot lång yacht. Psiaki, et al. (2013) beskriver att syftet med experimentet var att undersöka utmaningarna med att utföra en attack på fartygets GPS-mottagare och ta över kontrollen av fartygets styrning. Med hjälp av metoden *spoofing* skapade forskarna falska GPS signaler som var starkare än de två satellitsignalerna ombord, vilket resulterade i att fartyget fick en felaktig position. Psiaki, et al. (2013) menar att genom attacken med spoofing utlöstes inga navigationslarm och varken systemen eller besättning hade kännedom om att fartyget ett flertal gånger ändrat kurs. Forskare som befann sig ombord fartyget kunde tillsammans med besättningen känna fartygets girar, men då besättningen förlitade sig på de elektroniska sjökorten, ansågs fartyget var på rätt kurs. Psiaki, et al. (2013) menar att undersökningen visar ett stort gap mellan spoofings kapacitet och vad industrins system är kapabla till att upptäcka (The University of Texas at Austin, 2013).

Emellertid beskriver Chernov och Sornette (2019) att det är inte bara experiment som utförs av forskare. Under 2011 till 2013 utfördes flera upprepade attacker mot Port of Antwerps datorsystem. Chernov och Sornette (2019) beskriver att syftet med attackerna var att gömma utvalda containrar för hamnmyndigheterna. Utvalda containrar etiketterades innehålla bananer, men i verkliga fallet bestod innehållet i containrarna av narkotika skickat från Sydamerika med hjälp av fartyg (Chernov & Sornette, 2019).

Med tanke på ökade attacker valde IMO på sitt 98:e sammanträde av MSC- Maritime Safety Committee att implementera *Cyber Risk Management* i fartygets SMS. Med hjälp av MSC.428(98) menar IMO (2017b) att resolutionen ställer krav på att risken uppmärksammas i samtliga säkerhetsförordningar med hänsyn till ISM. IMO (2017a) beskriver att implementering av reglerna utförs med hjälp av rekommendationerna i MSC-FAL.1/Circ.3 som syftar till att ligga till grund för rederierna och dess fartyg att uppmärksamma sårbarheter och IT-säkerhetsrisker inom verksamheten. IMO önskar att riktlinjerna ska hjälpa rederier i arbetet att öka skydd mot cyberattacker och intrång (IMO, 2017a).

Maersk (2017b) beskriver bland annat att de blev angripna av en global cyberattack, vid namn NotPetya. Maersk (2017a) menar att de var en av flera organisationer som föll offer för attacken, som tror sig vara utförd av en liten grupp hackare som använde sig av metoden *Malware*. Attacken resulterade i att Maersk affärssystem, tillika operationella system för terminaler och fartyg, slutade att fungera som i sin tur gjorde att fartygen och alla landterminaler runt om i världen stod stilla. Konsekvenserna av attacken resulterade i stora ekonomiska förluster, uppskattningsvis 250–300 miljoner dollar. Till följd av attacken förlorade Maersk all sin existerande data vilket medförde att verksamheten fick återställa alla IT-system. Förutom att Maersk drabbades hårt som företag, berördes även kunder och invånare runt om i världen som inte fick sitt gods i tid (Maersk, 2017a).

Attacken på Maersk indikerar vikten av implementering av *Cyber Risk Managemen*t i verksamheters säkerhetsarbete. Gard (2019) menar att den amerikanska kustbevakningen anser att det är ett ofrånkomligt krav att adressera säkerhetsrisken i form av cybersäkerhet inom verksamheter. Tillika menar Gard (2019) att kustbevakningen beskriver vikten av att arbeta proaktivt med cybersäkerhet för att inte falla offer för det växande hotet. De menar att

cybersäkerhet inte bara en IT-fråga utan det är en grundläggande faktor för en väl fungerande marin operationell verksamhet i 2000-talet (Gard, 2019).

2013 ansågs cybersäkerhet vara den 15:e största risken mot handeln, sju år senare anser försäkringsbolaget Allianz (2020) för första gången att cybersäkerhet med dess attacker och incidenter är den största risken mot global handel. Dessutom menar Allianz (2020) att risken drastiskt stigit på grund av att antal attacker ökat till följd av verksamheters tillförlitlighet till datasystem (Allianz, 2020). Med hänsyn till ovan ser författarna betydelse i att undersöka svenska rederiers existerande kunskap inom ämnet. Rapporten undersöker rederiernas förberedelser och attityd inför kommande regelverket.

3 Teoretisk referensram

Kapitlet inleds med en beskrivning av grundläggande fakta om IMO, som är organisationen bakom det nya kravet. Tillika beskrivs krav från andra inflytelserika organisationer inom industrin. Efter genomgång av denna teoretiska bakgrund avlutas kapitlet med ett faktabaserat avsnitt om de hot som IMO 2021 - Cyber Risk Management syftar till att eliminera. Syftet med teorin är att presentera en systematisk överblick om varför svenska tankrederier bör agera i frågan.

3.1 IMO - International Maritime Organisation

IMO är en underorganisation inom Förenta Nationerna som har till syfte att förbättra det maritima tonnaget (IMO, u.d.f). Organisationen syftar vidare till att förebygga utsläpp och föroreningar samt höja den maritima säkerheten inom sjöfartsindustrin. Arbetet utförs med hjälp av ett antal regelverk vars syfte är att säkerställa samtliga aspekter inom sjöfart. IMO (u.d.f) menar att åtgärderna täcker konstruktion och fartygsdesign, utrustning, bemanning och avfallshantering. Samtliga eftersträvar att säkerställa att den maritima transporten utförs säkert, miljövänligt och energieffektivt. IMO utför sitt arbete primärt genom organisationens konventioner, koder, protokoll och rekommendationer. Med hjälp av ett samarbete med länder sprids budskapet världen över (IMO, u.d.f).

IMO:s arbete med cybersäkerhet tog fart 2017 då organisation såg en ökad efterfrågan i arbetet med IT-säkerhet. Med hjälp av kommittén för sjösäkerhet, MSC, formulerade IMO på sitt 98:e sammanträde ett lagkrav med hjälp av MSC.428(98). Med hjälp av resolutionen kräver IMO att rederier tar ställning i det akuta behovet för ökad medvetenhet och höjd beredskap för cybersäkerhet innan 1 januari 2021 (International Maritime Organisation, [IMO], u.d).

3.1.1 SOLAS - Safety of life at sea

IMO (u.d.a) beskriver att SOLAS är en internationell konvention utvecklat av IMO som reglerar många aspekter inom sjöfarten. Huvudsakligen syftar SOLAS till att kräva minimistandarder för hur fartyg ska vara konstruerade och utrustade. Kravet grundar sig i att fartyg ska vara byggda för säker framdrift, framförallt vad gäller livräddning, eldsläckning och radioutrustning ombord. SOLAS tillämpas på alla internationellt gående lastfartyg med 500 bruttoton eller mer (IMO, u.d.a).

Tiberg, Schelin, och Widlund (2015, s. 63) förklarar att samtliga framstående sjöfartsnationer har ratificerat SOLAS-konventionen. Sverige har med hjälp av riksdagen infört de krav som anges i SOLAS genom Fartygssäkerhetslagen (Tiberg et al., 2015).

3.1.1.1 ISM Code - International Safety Management Code

ISM-koden definieras som Internationella säkerhetsorganisationskoden för säker drift av fartyg och förhindrande av förorening. Transportstyrelsen (2020) beskriver att från 1980 fram till 90-talet var olycksdrabbade årtal för sjöfarten världen över. Under denna tid inträffade ett flertal sjörelaterade olyckor. Utredningar visade bristande säkerhetsarbetet ombord på fartygen. Tillika ansåg man

relationen mellan fartyg och verksamheten som bristfällig. Transportstyrelsen (2020) förklarar att IMO identifierade ett stort behov av att utveckla ett säkerhetsorganisationssystem, SMS. Systemet riktar sig till det företag som ansvarar för fartygets drift. Det var också under denna tidsperiod som ISM- koden konstruerades (Transportstyrelsen, 2020). Tiberg, Schelin, och Widlund (2015, s. 81) förklarar att huvudsakliga syftet med ISM-koden är att genom vägledning uppnå en internationell standard av säkerhet ombord på fartygen och att skapa en säkrare arbetsmiljö ombord. Lika viktigt är koden för att förhindra föroreningar från fartyg. Att arbetet med kraven från koden innefattar att identifiera riskfyllda situationer för att undvika dem samt utveckla säkerhetskompetensen hos samtliga anställda (Tiberg et al., 2015).

3.1.1.2 SMS - Safety Management System

IMO (u.d.c) beskriver att säkerhetsledningssystem, SMS, är ett organiserat system för att säkerställa fartygets säkerhet samt bevara den marina miljön. Säkerhetsledningssystemet utformas och implementeras av rederiet själva. Ett säkerhetssystem säkerställer att de obligatoriska säkerhetsreglerna, riktlinjer och standarder som rekommenderas av IMO efterföljs av rederiets samtliga fartyg (IMO, u.d.c).

3.1.1.3 DOC - Document of compliance

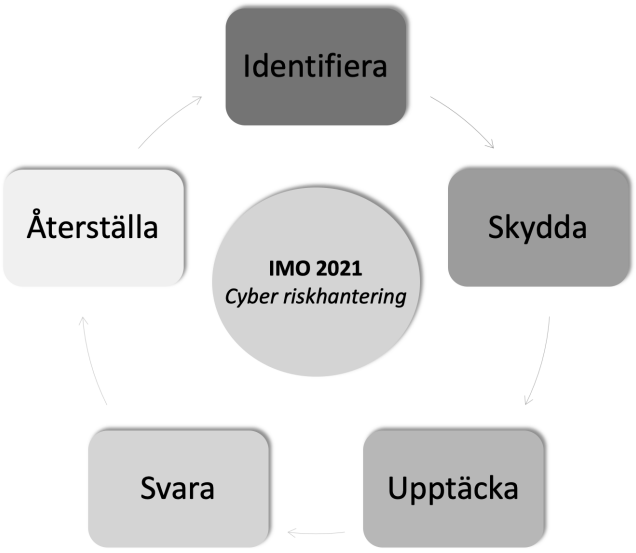
Dokumentet om godkänd säkerhetsorganisation, DoC - Document of Compliance, är ett certifikat som utfärdas till de rederier som uppfyller de överensstämmelser och krav från ISM-koden. Certifikatet utfärdas av flaggstatens myndigheter genom att granska rederiets SMS och hur genomförandet av säkerhetssystemet är utfört (Deutsche Flagge, u.d.). IMO (u.d.d) förklarar att det är just i DoC som rederiet uppvisar att de på ett lämpligt sätt hanterar kraven från IMO angående *Cyber Risk Management* enligt ISM-koden (IMO, u.d.d). Tiberg, Schelin, och Widlund (2015, s. 82) beskriver att om det saknas certifikat för godkänt säkerhetsledningssystem, får fartyget inte brukas för sjöfartsdrift. Efterlevnadskontroller undersöker så att rederier och dess fartyg har en godkänd säkerhetsorganisation. Vad gäller Sverige är det Transportstyrelsen som utför dessa inspektioner samt utfärdar certifikaten (Tiberg et al., 2015).

3.1.2 IMO 2021 - Cyber risk management

Sjöfartsindustrin integrerade och digitaliserade system för att underlätta och effektivisera arbetet ombord fartygen, har resulterat i en ny sårbarhet. Det är tydligt att rederierna tillsammans med fartygen blir exponerade mot otillåtet dataintrång mot nätverk, operativsystem och affärssystem. Arbetet för att eliminera risken bör omhändertas genom riskhantering av begreppet cybersäkerhet. Begreppet har blivit ett mer omtalat fenomen under 2000-talet. Försäkringsbolaget Allianz (2020) menar att man ser en drastisk ökning av organisationer och verksamheter som fallit offer för skadliga attacker.

Med hänsyn till den drastiska utveckling av attacker de senaste åren har begreppet diskuterats internationellt. Då sjöfartsindustrin sträcker sig världen över antog IMO som övergripande organ för sjöfartssäkerhet och regelverk begreppet i diskussion. En attack kan vara förödande och därmed bör riskhantering och hinder mot en otillåten access implementeras av ledningen för rederiorganisationen. IMO antog MSC.428(98) på sitt 98:e sammanträde och ställer därmed krav på att begreppet och *Cyber Risk Management* inkluderas i rederiernas existerande SMS-kod (IMO, 2017b).

För att hjälpa rederiorganisationer i sitt arbete med cybersäkerhet har IMO konstruerat riktlinjer i form av resolutionen MCS-FAL.1/Circ.3. Transportstyrelsen (2020) beskriver att med hjälp av resolutionen tillhandahåller rederier rekommendationer för hur implementeringen av *Cyber Risk Managemen*t ska gå till. För att enklare illustrera de viktiga moment som en rederiorganisation bör belysa i sitt arbete med cybersäkerhet används nedan modell.



Figur 1. Förslag på hur rederier kan arbeta med Cyber riskhantering. Författarnas egenutvecklade figur.

Modellen bygger på de fem fundamentala element som IMO rekommenderar att ett rederi ska belysa i sitt arbete med *Cyber Risk Management*. IMO (u.d.d) föreslår att de fundamentala elementen implementeras i rederiernas kontinuerliga arbete med cyberriskhantering. IMO (u.d.d) menar för att ett rederi ska besitta ett effektivt arbeta med *Cyber Risk Management* är det viktigt att direktiv och beslut börjar på en ledningsnivå. Med hjälp av att uppmärksamma cyberrisker på denna nivå är det lättare att sprida medvetenhet och kunskap vidare till samtliga nivåer inom företaget. IMO (u.d.d) beskriver att det är agerandet från rederiets ledningsnivå, tillika kultur, som avgör hur omfattande arbetet med cybersäkerhet är inom organisationen (IMO, u.d.d). IMO (2017a) rekommenderar att ett rederis arbete innefattar följande:

Punkt 1, identifiera *(Identify)*, syftar till att rederierna bör definiera vem eller vilka individer inom organisationen som har ansvar för *Cyber Risk Management*. Individen eller individerna med ansvarsroller ska identifiera sårbarheter och risker med att bedriva rederiets system, tillgångar och data (IMO, 2017a).

Punkt 2, skydda *(Protect)*, syftar till att rederier bör implementera rutiner för riskkontroll- och åtgärdsprocessen i händelse av en cyberincident. Tillika rekommenderas rederierna att implementera en beredskapsplan som fungerar som ytterligare skydd vid cyberincident (IMO, 2017a).

Punkt 3, upptäcka *(Detect)*, syftar till att uppmärksamma rederierna att utveckla och implementera nödvändiga aktiviteter (handlingar) som ska ligga till grund för att verksamheten i god tid upptäcker cyber incidenter (IMO, 2017a).

Punkt 4, svara *(Respond)*, syftar till att rederierna med hjälp av utvecklade och implementerade aktiviteter har en responsplan och etablerat motstånd mot en cyberincident. Som en följd av tidigare nämnda aktiviteter och återställande system, besitter rederiet kontroll av de system som blivit påverkade av en cyberincident (IMO, 2017a).

Punkt 5, återvinna *(Recover)*, syftar till att rederierna kontinuerligt utför säkerhetskopiering av nödvändiga system. Vid en cyberincident kan dessa kopior återställa verksamheten och dess operationer till omständigheterna innan händelsen (IMO, 2017a).

3.2 Industrins krav för transport av flytande bulk

Oruc (2019) menar att IMO:s resolution MSC.428 (98) ställer obligatoriska krav på rederier att adressera cybersäkerhet. Som tillägg till resolutionen såg varierande inflytelserika organisationer anledning till att implementera krav på att rederier ska arbeta med cybersäkerhet. Oruc (2019) beskriver att OCIMF är en av de inflytelserika organisationer som i ett tidigt stadie valt att belysa den stigande risken. Organisationen kräver genom TMSA och SIRE att tankrederier tar hänsyn till cybersäkerhet från 1 januari 2018 (Oruc, 2019).

3.2.1 OCIMF

Oruc (2019) menar att sjöfartsindustrin med fokus på transport av flytande bulk är en industri som präglas av många olyckor med förödande konsekvenser. Med hänsyn till konsekvenserna av olyckorna fanns incitament till att starta en icke-vinstdrivande organisation med syfte att minska olyckor och därav de förödande utsläppen. Oruc (2019) menar att en av dessa organisationer är OCIMF - Oil Companies International Marine Forum, som år 1971 blev delegerade rådgivande status av IMO. Oruc (2019) beskriver att OCIMF är en organisation som arbetar med att höja kvaliteten av de fartygtonnage som trafikerar världshaven. Arbetet utförs i synnerhet genom SIRE - Ship Inspection Report Program, med fokus på fartyget och TMSA - Tanker Management and Self Assessment program, med fokus på rederiet. Informationen från inspektioner sammanställs i OCIMF:s databas som sedan medlemmar tar del av (Oruc, 2019).

3.2.1.1 SIRE

SIRE är ett självbedömningsprogram konstruerat av OCIMF med syfte att implementera en kvalitetsstandard på marknaden. Oruc (2019) beskriver att genom rederiernas egenbedömning erhålls en hög kvalitet, som i sin tur ökar säkerheten för fartyget och dess besättning. För att utvärdera fartygens kvalitet utförs granskning av en auktoriserad inspektör som med hjälp av ett väl formulerat formulär utvärderar fartyg, såväl som besättning. Oruc (2019) beskriver att från och med september 2018 är cybersäkerhet en del som inspektören utvärderar. Under kapitel 7, *Maritime Security*, ställer inspektören ett antal frågor med fokus på rederiets och fartygets arbete med cybersäkerhet. Under inspektion undersöks bland annat hur väl nedan frågor uppfylls (Oruc, 2019):

Fråga 7.14 - “Finns policy och procedurer för cyber security inkluderat i fartygets Safety Management System samt om det finns en respons plan ombord?”

Fråga 7.15 - “Är besättningen ombord medvetna om rederiets policy för kontroll av fysisk tillgång till fartygets IT och OT system?”

Fråga 7.16 - “Har rederiet en policy eller vägledning för hur personliga enheter kan användas ombord?”

Fråga 7.17 - “Främjar rederiet aktivt om medvetenhet för cyber security och speglas detta arbete ombord fartygen?” (Oil Companies International Marine Forum, [OCIMF], 2019)

Med hjälp av mottagen information fyller inspektören i uppgifterna i SIRE. Oruc (2019) menar att från programmet tillhandahåller alla medlemmar, som består av oljeterminaler, hamnmyndigheten och handelshus med mera, vital information om fartygets kvalitet och om alla de krav som parten önskar uppfylls (Oruc, 2019).

3.2.1.2 TMSA

Oruc (2019) menar att TMSA är ett program utvecklat av OCIMF som syftar till att ligga som fundamental grund för tankrederiers utvärdering, mätning och förbättring av sin egen SMS. Rederiet utvärderar och bedömer sin SMS jämfört med viktiga nyckeltal uppsatta av OCIMF. Oruc (2019) menar att resultatet av företagets egen utvärdering publiceras i programmets system som granskas av TMSA-experter via kontorsrevisioner. Kontrollerna utförs inte utefter ett förutbestämt schema utan de stora oljebolagen, så som Shell och BP, besöker rederierna för att utvärdera och granska hur väl rederiets lämnade uppgifter stämmer överens med aktuell information. Under en granskning utvärderas företagets arbete med SMS utifrån ett antal viktiga nyckeltal som visar prestation. Oruc (2019 beskriver att prestationsmålen är uppdelade i fyra nivåer, där den fjärde nivån är den svåraste och den första representerar minimumförväntningarna. Oruc (2019) menar att vid den senaste revisionen av TMSA valde OCIMF att implementera element 13 som belyser marin säkerhet. Här utvärderas rederiernas samarbete med cybersäkerhet genom två nyckeltal. De två prestationsmåtten är implementerade med syfte att sätta press på rederier att beakta hotet och den växande risken. De två nyckeltalen mäter huruvida rederiet belyser cybersäkerhet i sin SMS (Oruc, 2019),

KPI 13.2.3 - “Rederiets policy och procedurer innehåller cyber security där det finns nödvändiga riktlinjer och begränsningsåtgärder.”

KPI 13.2.4 - “Rederiet arbetar aktivt med att främja medvetenhet för cyber security” (Oruc, 2019).

3.3 Cyberattack

Sjöfartsindustrins vardag präglas av en allt mer ökad oro för cyberattacker. För att en handling ska definieras som cyberattack krävs det att bedragaren utför en attack med syfte att begå en cyberbrottslighet. En sådan attack beskrivs som när en bedragare riktar en direkt handling mot offret som inte allt för sällan är ett företag. Ayala (2016) menar att handlingen utförs i syfte att förstöra, inaktivera, störa eller skada ett företags cyberspace. Med hjälp av att ett intrång i datorsystemets kan den obehöriga aktören stjäla viktig information. Ayala (2016) beskriver att möjligheten för dataintrång drastiskt ökat i takt med företags ökade tillförlitlighet till datorer.

Ayala (2016) beskriver vidare att en cyberattack kan både vara riktad och oriktad. Vid en oriktad attack är det inte offret eller företaget som är i centrum utan snarare antalet enheter eller användare som attacken når. En riktad attack syftar istället till att angripa ett specifikt offer. Ayala (2016) beskriver att en riktad attack är inte allt för sällan mer skadlig i jämförelse till en oriktad då den ofta kräver månader av förberedelser av hackaren. Ayala (2016) menar att genom planering konstrueras attacken specifikt till verksamheten, personalen eller kontoret som attacken utförs på. En förklaring till detta är att riktade attacker kan vara utförda av individer som blivit betalda (Ayala, 2016, s. 43).

3.3.1 Phishing

Phishing är en angreppsmetod som utförs på en digital plattform. Ayala (2016) menar att metoden använder sig av falska e-postmeddelande och webbplatser för att erhålla viktig information. Från utseende av meddelandet eller internetsidan anses offret inte se någon skillnad mellan äkta och förfalskade. Ayala (2016) beskriver att med hjälp av denna metod lurar bedragaren individer att avslöja viktig information på begäran. Offret tror att det är en pålitlig källa som förfrågan begärs från, trots att så inte är fallet. Ayala (2016) menar att syftet är att leda offret till en falsk webbplats alternativt begära offret att avslöja känslig personlig- eller företagsmässig information via e-postmeddelande. Den tilldelade informationen används i sin tur för att kräva offret på ett agerande som är fördelaktigt för bedragare, till exempel en lösensumma (Ayala, 2016, s. 119).

3.3.2 Malware

Ayala (2016) menar att malware är en skadlig programvara konstruerad i syfte att skada ett system. Det finns ett antal olika malware-typer där virus, trojanska hästar och spionprogram är några av de mest förekommande. Vad som kännetecknar malware är dess metod som utgår från att med hjälp av obehörig access påverka ett system. De negativa effekterna av metoden speglar åtkomsten av systemets integritet och tillgänglighet för systemets ägare (Ayala, 2016, s.104).

3.3.3 Ransomware

Ransomware beskrivs av Ayala (2016) som ett alternativ till malware där offrets datorsystem infekteras av en skadlig kod. För offret anses filen, innehållande ransomware, vara en legitim fil baserat på utseende. Emellertid menar Ayala (2016) att systemet infekteras med en skadlig kod som tar över kontrollen över systemet och kan endast mot betalning få bort begränsningen. Bland annat används ransomware genom att använda skadlig kod och genom detta systematiskt låsa viktiga filer (Ayala, 2016, s.129).

3.3.4 Spoofing

Ayala (2016) definierar spoofing som när ett system får olaglig överföring till sig från obehöriga aktörer. Ayala (2016) menar att aktörerna sänder förfalskade överföringar i form av till exempel e-postadresser, GPS-signaler eller IP-nummer för att på ett obehörigt sätt försöka få tillträde i ett annat säkerhetssystem. På samma sätt kan en obehörig aktör agera som korrekt upphovsrättshavare och kan därmed placera en förvrängd eller felaktig version av det ordinarie verket. Ayala (2016) beskriver att i verkliga fallet besitter bedragaren trafik från en annan plats och använder metoden för att avslå en tjänst eller service (Ayala, 2016, s.150).

4 Metod

Nedan presenteras studiens metodologi och tillvägagångssätt för att nå resultatet och svar på forskningsfrågor. Inledningsvis presenteras studiens fallstudie och därefter redogörs metod för datainsamling. Kapitlet redogör vidare för urvalet och genomförande av intervjuer samt hur analys av insamlad data därefter gått till. Avslutningsvis presenteras en reflektion över forskningsetiken.

4.1 Fallstudie

Studiens fundamentala angreppssätt är baserat på en kvalitativ fallstudie, som bland annat Bell (2015) menar är en studie som rymmer möjligheten att på djupet studera en begränsad del av ett problem. Under denna studie fokuserar den kvalitativa metoden på att djupare förstå och förklara de bakomliggande motiv för att införa en ny lagstiftning för cybersäkerhet (Bell, 2015). Denscombe (2014) anser att det är viktigt för uppsatsförfattare att noggrant överväga om ämnet i fallstudien är relevant, där utgångspunkten baseras på om ämnet i fråga har några tydliga gränser eller ett distinkt slut som utesluter ämnet från att falla in i andra sociala fenomen. Uppfyller ämnet beskrivna kriterier tillåts författarna i djupet undersöka specifika delmål i relevant fakta. En fallstudie är en relevant angreppsmetod till att undersöka uppsatsens ämne och besvara frågor, då metoden inte bara är intresserad av *vad* som inträffar utan också en förklaring till *varför* dessa faktorer inträffar (Denscombe, 2014). Därmed är inte bara regelverket för *Cyber Risk Management* intressant, utan också i vilken utsträckning företag är förberedda och dess attityd inför det kommande regelverket. Med hjälp av en fallstudie beskriver Denscombe (2014) beskriver vidare att en fallstudie är en lämplig metod för att belysa ett specifikt ämne där uppsatsen syftar till att besvara en snäv frågeställning i hänsyn till ett annars omfattande segmentet, så som sjöfartsindustrin- Uppsatsförfattare utför fallstudien med hjälp av en undersökning av fyra verksamma företag inom transport av flytande bulk, där fokus läggs på skyldigheten att förhålla sig till regelverken uppsatta av IMO.

4.2 Datainsamling

I studier är insamling och analys av redan existerande arbeten och information av stor vikt (Denscombe, 2014). Bryman och Bell (2012) beskriver att det finns två alternativ till hur uppsattsförfattare bör hantera data och information till att besvara uppsatsens forskningsfrågor. Bryman och Bell (2012) menar att det finns primär- och sekundärdata, vilket hanterar olika typer av data beroende på var informationen härstammar ifrån. Primärdata beskrivs som insamling av information där författarna finner information till uppsatsens ämne och frågeställning. Av den anledning ses primärdata som information som är speciellt framtagen till att besvara uppsatsens syfte. I studien består primärdatan av data från intervjuer som utförts med relevanta respondenter. Respondenterna är noggrant utvalda individer som besitter rätt kunskap och erfarenhet för att besvara intervjufrågorna, för att primärdatan ska vara användbar för studien. Sekundärdata är data som redan existerar inom ämnet, så som tidigare forskning eller specifik litteratur relevant till ämnet (Bryman & Bell, 2012). Under denna uppsats beskrivs studiens bakgrund och teoretisk referensram med hjälp av insamlad sekundärdata. Med hjälp av redan existerande forskning och

litteratur byggs den fundamentala grunden av relevant information för att hjälpa läsaren att förstå bakgrunden till lagkravet. Lika viktigt är uppsatsens forskningsfrågor som besvaras med hjälp av primärdata. Med hänsyn till vald metodologi kompletterar primär- och sekundärdata varandra med nyfunnen och redan existerande fakta, för att på bästa sätt besvara uppsatsens forskningsfrågor. Det specifika datainsamlingsmetoderna förklaras mer ingående i kommande delavsnitt.

4.2.1 Semistrukturerade intervjuer

Bell (2015) föreslår att vi som forskare inledningsvis bör överväga vilken information vi behöver, och varför vi behöver den, innan tillvägagångssättet bestäms. Då företags arbete inom cybersäkerhet är omfattande och är i olika stadier beroende på företagets digitala mognad, menar vi att en kvalitativ datainsamling är att föredra. För att samla in data tillämpas semi-strukturerade intervjuer med fyra intervjuobjekt som härstammar från deltagande företag i fallstudien. Bell (2015) menar att denna typ av metod för datainsamling gör det möjligt för forskarna att ställa följdfrågor vilket bidrar till en mer rik datakvalitet än övriga metoder. Syftet med intervjuer är att få en uppfattning av svenska rederiers dagliga arbete inom ämnet, tillika dess attityd och syn på den ökade risken för dataintrång. Med hjälp av intervjuer erhåller författarna en djupare förståelse för bakgrunden till den nya lagstiftningen IMO 2021-Cyber Risk Management. Tillika bidrar respondenter med kunskap och erfarenhet vilket resulterar i att uppsatsen visar uppdaterad och aktuell information inom ämnet. Vidare beskrivs genomförande av intervjuer i avsnitt 4.2.3.

4.2.2 Urval

Utvald målgrupp för intervjuer är svenska tankrederier, där urvalet baseras på rederier med kontor i Västra Götalands Län. Via branschorganisationen Svensk Sjöfarts (u.d.) hemsida, innehållandes en medlemslista, valdes ett antal potentiella intervjudeltagare. Kommunikation med rederier inleddes via mejl med en kort introduktion till vi som författare samt beskrivning av studiens syfte. Genom att i ett tidigt stadie förklara syftet med studien kunde rederierna utföra en egenkontroll och se över om de hade anställda med rätt kunskap, erfarenhet och auktoritet för att svara på intervjufrågorna. Av de åtta företag som fick frågan om att delta i studien, svarade endast tre och godkände en intervju. Den fjärde respondenten, IT-leverantör, möjliggjorde för studien att erhålla ett leverantörsperspektiv på cybersäkerhet. Denscombe (2014) rekommenderar att urval av deltagare avgränsas till närhetsprincip och tidsmässiga faktorer, vilket vi även tillämpat i denna studie. Nedan sammanställs urvalet i en tabell.

Tabell 1. Sammanställning av intervjurespondenter

Respondenter	Befattning	Företag
1	QA Coordinator	Rederi A
2	HSE Manager *(DPA & CSO)*	Rederi B
3	Crew & Quality Controller	Rederi C
4	COO	IT-Leverantör

4.2.3 Deltagare

Denscombe (2014) beskriver att desto fler respondenter desto bättre, då det styrker generaliserbarheten av rapporten. Sammanlagt utfördes fyra intervjuer med respondenter med varierande befattning. Befattning kom att spela en stor roll i respondentens möjlighet att besvara intervjufrågorna, där en respondent ansvarig för Quality Control inte hade samma inblick i säkerhetsfrågor som en respondent ansvarig för HSE-Health Safety och Environment. Men de olika befattningarna på deltagarna möjliggjorde unika perspektiv på situationen.

4.2.3 Genomförande

I en intervju samlas data in med hjälp av utvalda frågor som ställs i en förutbestämd sekvens mellan intervjuare och respondent. Denscombe (2014) beskriver att beroende på vilken frihet intervjuaren önskar i intervjun, med hänsyn till följdfrågor, bör struktur övervägas. Av den anledning anser författarna att semi-strukturerade intervjuer är att föredra, då det finns nyckelfrågor alltid besvaras men att det utöver detta är möjligt att ställa följdfrågor beroende på de svar som erhålls från respondenten.

Denscombe (2014) rekommenderar att intervjuguiden utvecklas med hänsyn till uppsatsens frågeställning. Vid framställning av intervjufrågor har vi dessutom valt att koppla till den teoretiska referensramen i form av IMO:s rekommendationer. Intervjuguiden delades in i tre tydliga kategorier med hänsyn till uppsatsens frågeställningar och teori. Kategorierna är nulägesbeskrivning, utmaningar med implementering och nivåanalys. Intervjuguiden för studien finns bifogad i bilaga 3. Denscombe (2014) föreslår att intervjuerna spelas in för att sedan transkriberas, vilket är ett tillvägagångssätt vi tillämpat i studien. Detta har i sin tur underlättat för att analysera insamlad data att utföra ett mer detaljrikt efterarbete (Denscombe, 2014). Denscombe (2014) menar att transkribering av intervjumaterial från intervjuer är ett omfattande arbete eftersom det är tidskrävande. Därmed ställdes endast frågor med hög relevans till ämnet.

Samtliga intervjuer genomfördes på distans via digitala kanaler så som Skype eller FaceTime. Vid intervju närvarade båda uppsattsförfattare där frågor ställdes i turordning i enlighet med konstruerad intervjuguide. Båda författarna agerade intervjuare där frågor och följdfrågor ställdes till respondent. Denscombe (2014) beskriver att intervjuer med en part är enklare att utföra i motsats till gruppintervjuer. En förklaring till detta är omfattningen av individer inblandade. Denscombe (2014) menar att vid ett lägre antal är det lättare och mer flexibelt att arrangera och utföra en intervju (Denscombe, 2014). Vid varje intervjutillfälle inleddes samtalet med en kortare beskrivning av uppsatsen och dess syfte. Därmed fick respondenten får en grundläggande förståelse för vilken typ av information som eftersöktes.

4.2.4 Litteraturstudie

Litteratur som bidrar till att besvara rapportens frågeställning inhämtas från diverse databaser i form av Google Scholar, Scopus och Chalmers bibliotek. Sökord så som “Digitalisation”, “Cyber-Security”, “Cyber-Attacks”, “IMO”, “ISM”, “SMS”, “Risk assessment” och “Risk Management” används för att erhålla vetenskapliga artiklar, konferensartikel och böcker som är relevant till forskningsfrågan. Smith (2017) beskriver att informationssökning till en uppsats är en omfattande del innehållande en hel del falsk information (Smith, 2017). För att erhålla en god kvalitet och

förståelse av den information man läser är det viktigt att författarna skiljer på vad som är sant och falskt. Av den anledningen har vi använt oss av metoden CRAAP. Fielding (2019) beskriver att med hjälp av metoden tas ett antal viktiga frågor i beaktning som hjälper författarna att vara källkritiska till det som tolkas från litteratur, men i synnerhet internet. Fielding (2019) menar att metoden rekommenderar författarna att noggrant granskar den valda webbsidan, där fokus bör vara på dess trovärdighet. Grunden i utvärderingen av trovärdighet inleddes med att vi undersökte om det fanns utskrivna författare, referenser samt vilket syfte som låg till grund till att materialet publicerats på internet. Mot den bakgrund har vi använt oss av en ett systematiskt angreppssätt som sorterar och utvärderar endast aktuell och relevant forskning till IMO 2021-Cyber Risk Management (Fielding, 2019).

4.3 Analys av data

Till att börja med analyserades ett flertal arbeten och dokument i syfte att erhålla viktig information om varför *Cyber Risk Management* är i behov av att lagstiftas. Då lagkravet är ställt från IMO granskades tillika organisationen och dess syfte. Detta för att skapa en förståelse för läsaren. Nästa steg var att granska resolutioner innehållande ämnet *Cyber Risk Management*. Valet av att granska dessa dokument i ett tidigt stadie grundade sig i dess betydelse för rederiverksamheten. Analysen av dessa dokument var möjlig då alla dokument och krav fanns tillgängliga på IMO:s webbportal för granskning. Vi kunde enkelt kartlägga vilka krav som svenska rederier behöver förhålla sig till eftersom dokumenten var tydligt strukturerade och formulerade.

Nästa steg i analys av data bestod i att transkribera utförda intervjuer. Som tidigare nämnt är uppsatsen baserad på semistrukturerade intervjuer där insamling av data är fokuserat på en kvalitativ datainsamling. För att reducera risken att detaljer från intervjun gick förlorade och för att säkerställa en god kvalitet beslutade vi oss för att transkribera materialet tätt efter intervjutillfällena. I arbetet med transkribering beskriver Denscombe (2014) att fokus inte bör läggas på det enskilda orden utan istället dess betydelse. Fördelarna med att transkribera materialet direkt efter intervjutillfället grundar sig i att författarna fortfarande erhåller möjlighet att minnas detaljer som är relevanta till innehållsanalysen (Denscombe, 2014). För att strukturera analysen av insamlad data från intervjuerna valde vi att använda oss av Graneheim och Lundman (2004) 5-stegsmodell där fokus på informationssökning utgår från koncepten manifest och latent. Genom koncepten kunde vi analysera synliga och uppenbara komponenter i form av manifesta innehåll, men således också det latenta innehåll som återspeglar en djupare förståelse och de bakomliggande betydelserna av texten (Granheim & Lundman, 2004).

Under det första steget rekommenderar Granheim och Lundman (2004) att ett flertal gånger läsa igenom det transkriberade materialet för att erhålla en känsla av helhetsförståelse till informationen (Granheim & Lundman, 2004).

Därefter beskriver Granheim och Lundman (2004) är att analysera texten där fokus bör ligga på att kondensera informationen för att identifiera det som är av intresse till att besvara uppsatsens forskningsfrågor. För att urskilja relevant information mot icke-relevant, ska information som är meningsfullt i förhållande till ämnet eftersökas. För att på bästa sätt erhålla högsta kvalitet av

information som besvarar syftet föreslår Granheim och Lundman (2004) att plocka ut meningar, stycken eller ord som är av betydelse och relevans till ämnet och benämner dessa som meningsbärande enheter. De meningsbärande enheterna ska urskilja sig från övriga texten, däremot kvarstår omgivande text i sin helhet för att inte tappa sammanhanget kring det viktiga delarna. För att eliminera risken för att väsentlig text går förlorad är det av stor vikt att flertal gånger noggrant bearbeta texten (Granheim & Lundman, 2004). Med hjälp av meningsbärande enheter och kondensering menar Granheim och Lundman (2004) att texten blir mer lätthanterlig och tydlig. Därefter kodas de kondenseringar och meningsbärande enheter som tydliggjorts i det transkriberade materialet. Koderna benämns med hjälp av etiketter som syftar till att återspegla det centrala budskap som de kondenserade meningsbärande enheterna utgör. Kod kan av den anledning anses vara en samlingsterm av ett fåtal ord som beskriver meningsenheternas innebörd (Granheim & Lundman, 2004). I det fjärde steget menar Granheim och Lundman (2004) att koder som liknar varandra eller innehåller likartad uppfattning bildar en subkategori. Granheim och Lundman (2004) menar att i takt med bearbetning av texten enligt analysprocessen steg skapas ett mönster av koder som alla delar likartat innehåll. Dessa koder som delar mening kategoriseras till en subkategori och bildar därav en grupp innehållande delad uppfattning om ämnet i fråga (Granheim & Lundman, 2004). Avslutningsvis organiseras subkategorier som delar uppfattning eller liknar varandra till kategorier. Granheim och Lundman (2004) beskriver att det dock är viktigt att kategorier inte är likartade, utan att varje kategori bör vara unik (Granheim & Lundman, 2004).

Vi har i analys av insamlad data följt Granheim och Lundmans (2004) rekommendationer för att ingen text, som besvarar studiens syfte, lämnas utan meningsbärande enheter, kondensering, kod, subkategori eller kategori. Nedan sammanfattas analysens tillvägagångssätt i enlighet till Granheim och Lundmans (2004) i en tabell.

Tabell 2. Studiens dataanalys enligt Granheim och Lundman (2004)

Granheim och Lundman (2004) *Rekommendationer*	**Uppsatsens tillvägagångssätt -** *i förhållande till rekommenderar analysmetod*
Steg 1 - Förståelse för text	Vi läste ett flertal gånger igenom det transkriberade materialet. Syftet var att erhålla en känsla av helhetsförståelse för respondenten och dess svar.
Steg 2 - Finna meningsbärande enheter och kondensering	I nästa steg fokuserade vi på att kondensera informationen, för att sedan plocka ut meningar, stycken eller ord som är av betydelse och relevans till ämnet och studiens syfte. Dessa utplock benämndes som meningsbärande enheter.
Steg 3 - Kodning i form av etiketter	Därefter kodade vi kondenseringar och meningsbärande enheter som tydliggjorts i det transkriberade materialet. Koderna benämndes med hjälp av etiketter, i form av ett eller flertal ord, som

	syftar till att återspegla det centrala budskap som de kondenserade meningsbärande enheterna utgjorde.
Steg 4 - Organisera i subkategorier	Därefter organiserades koder som liknade varandra och/eller innehöll likartad uppfattning. Dessa blev i sin tur subkategorier.
Steg 5 - Organisera i kategorier	Subkategorier delades in genom att undersöka eventuell delad uppfattning, eller i annat fall liknar varandra till en kategori.

4.4 Etik

Denscombe (2014) menar att när författare överväger att använda intervjuer som datainsamlingsmetod är det av stor betydelse att tillämpa en god forskningsetik på förhand. Syftet med god forskningsetik är att skydda och garantera intervjurespondent säkerhet där författarna innan intervju bör överväga om det innebär en risk att utföra intervjun. Vi som uppsatsförfattar har uppfyllt god forskningsetik genom att uppfylla de fyra huvudprinciper konstruerade av *The Nuremberg Code* och *Declaration of Helsinki* (Denscombe, 2014*)*. Första principen syftar till att skydda deltagaren, där fokus bör ligga på att respondenten inte ska lida skada som konsekvens av medverkan i intervju. Den andra principen syftar till att respondent inte ska med hjälp av tvång medverka i intervju, där vikt bör ligga på att medverkan är frivillig och information om intervjuns syfte förmedlas i samband med förfrågan om deltagare vilja. För att styrka andra principen anser Denscombe (2014) att respondent i skriftlig form godkänner deltagande, för att på så sätt skydda författarna från felaktiga anklagelser i efterhand. Den tredje principen handlar om att forskning bör utföras öppet och ärligt med hänsyn till utredning av information. Uppsatsförfattarna förverkligade den tredje principen genom att innan påbörjad intervju tydligt fråga respondent om godkännande till intervjun spelades in för att sedan efter transkribering i sådana fall radera inspelning. Tillika har vi varit tydliga med att beskriva syftet och upplägget av intervjun, för att på så sätt inte undanhålla information som kan uppfattas påtryckande alternativt anklagande. Den fjärde, och sista, principen handlar om att intervjuer och uppsats bör följa nationell lagstiftning. Utöver tidigare nämnd forskningsetik har vi även valt att anonymisera respondenter. Det enda som publicerats är befattning eller position inom företaget, då det är viktigt att bevisa att respondenter besitter rätt kunskap och auktoritet till att besvara intervjufrågorna (Denscombe, 2014).

5 Resultat

I följande kapitel presenteras det resultat som tagits fram baserat på utförda intervjuer. Resultatet är fördelat i enskilda avsnitt för varje respondent, detta för att presentera resultat på ett systematiskt och tydligt sätt för läsaren. Till att börja med beskrivs respondentens befattning för att visa att hen har kunskap och auktoritet till att svara på intervjufrågorna samt hur de i sitt arbete möter cybersäkerhet. Till att börja med beskrivs nuvarande arbete med cybersäkerhet där en nulägesbeskrivning syftar till att identifiera rederiernas existerande kunskap och erfarenhet inom området. Därefter presenteras de utmaningar som rederierna upplevt med att implementera resolutioner i syfte att uppfylla kraven från IMO. Slutligen presenteras den information som berör vilken nivå rederiet har valt att arbeta med *Cyber Risk Management*.

5.1 Rederi A

Första respondenten arbetar som QA Coordinator på ett större tankrederi. Rederiet har en egen avdelning som är ytters ansvarig för implementeringen av lagkraven samtidigt som rederiet också har ett nära samarbete med ett IT-företag. Avdelningen och IT-företaget har tillsammans arbetat fram dokumentationen. IT-företaget ansvarar vidare för driften av alla system, både på kontor och fartyg.

5.1.1 Nulägesbeskrivning

Respondenten påträffade begreppet cybersäkerhet första gången privat och upplever att de flesta som tillhör den yngre generationen är ganska medvetna kring ämnet. Respondenten säger att när kraven från oljebolagen, och senare IMO, angående cybersäkerhet kom till sjöfarten var första tanken att ha en god lösenordshantering, det vill säga att inte ha för lätta eller samma lösenord på olika system. Enkla saker så som att inte sätta upp en lapp med lösenordet på datorskärmen. Respondenten fortsätter och förklarar att när de väl skulle implementera detta på rederiet förstod de ganska snabbt att det omfattade mer än lösenordshantering.

"...man fick en känsla av att de är mycket bredare än bara ett litet lösenordsproblem liksom"
(Respondent 1)

Respondenten förklarar att rederiet har sedan lång tid tillbaka haft en IT-policy som innefattar riktlinjer och regler för generellt internetnyttjande samt lösenordshantering för de anställda, men att rederiet nu fått göra en ny utökad policy efter kraven. Respondenten beskriver att den nya policyn innefattar en inventering av vilka hot och risker rederiet tillsammans med IT-företaget har identifierat inom området samt en handlingsplan för hur de ska hantera en eventuell situation. Vidare förklarar respondenten att en riskutvärdering tillsammans med IT-företaget för rederiets fartyg också är genomfört, där de kom fram till att det inte finns speciellt mycket hot. Detta förklarar respondenten att det inte existerar så mycket system som går att koppla upp sig mot externt utan att man måste vara fysiskt ombord för att koppla upp sig med dator. Fördelen är att man får en fysisk säkerhet för systemen när de inte går att komma åt externt, nackdelen är

kostnaden och planeringen för en inspektör att komma ombord och utföra service vilket man hade kunnat genomföra online på distans annars säger respondenten.

Respondenten anser att man skulle vara naiv om man inte reflekterade över cyberhotet och att man då har missat en poäng i det senaste utvecklingssteget inom industrin, men i dagsläget anser respondenten att det finns många andra större risker och hot som känns mer relevanta än cyberhotet. Samtidigt upplever respondenten att hotet också kommer att öka i takt med att mer avancerade system tillkommer till industrin och att allting blir mer integrerat.

"...men just idag skulle jag sagt att det finns många andra hot som känns mer relevanta eller liksom större risker." (Respondent 1)

Risken för att just rederiet skulle bli utsatt för ett riktat dataintrång bedömer respondenten som låg. Detta grundas i att rederiet är relativt anonymt och att det inte finns något specifikt hot mot deras verksamhet förklarar respondenten. Den största risken respondenten beskriver är de slumpmässiga massutskick av phishing-mejl i kombination med mänskliga faktorn. Vidare beskriver respondenten hur ett av rederiets fartyg nyligen blev utsatt av just ett phishing-mejl. Respondenten förklarar att det hela resulterade i en mindre driftstörning ombord och att personalen hade problem att komma åt servern och mejlen som var utslaget under en mindre period.

"... ja vi hade en kollega som öppnade det av misstag… så där hade vi en liten driftstörning kan man säga, vi låg nere ett litet tag men det är faktiskt förvånansvärt smidigt, IT-företaget återskapar det som försvann så att det löste sig väldigt bra" (Respondent 1)

5.1.2 Utmaningar med implementering av resolution

Arbetet med *Cyber Risk Management* förklarar respondenten att det är hens avdelning, som benämns QA Department, på rederiet som har drivit arbetet men att det är rederiets Company Security Officer som har yttersta ansvaret för implementeringen. Fortsatt förklarar respondenten att hens avdelnings tillsammans med IT-företaget samt input från andra avdelningar på rederiet tagit fram riktlinjer och procedurer angående IT-säkerheten. Ombord på rederiets fartyg är det kapten som är ytters ansvarig för implementeringen summerar respondenten.

De sårbarheter som rederiet har identifierat i samband med cybersäkerhet så nämner respondenten servermiljön, mejl och telefoni vilket benämns som IT-system samt de OT-system ombord där respondenten syftar på driftsystem och lastsystem. Vidare förklarar respondenten att detta också är kopplat till fartygets ålder, äldre fartyg är inte lika stort bekymmer medans de nyare har mer automationssystem och driftsystem som har mer informationsteknik och är mer integrerade med fartygets server. Återigen tar respondenten upp exemplet att kunna utföra support eller service på distans och lägger vikten på att man måste säkerställa att det finns bra procedurer och rutiner för hur detta genomförs, eftersom man öppnar en digital dörr till någon så vill man inte att någon ska kunna få tillgång utan att få en form av godkännande. Mer beskriver respondenten att rederiets Safety Management System ligger på deras servrar som ett datorsystem men att det inte skulle vara särskilt allvarligt om något skulle hända där men att det fortfarande är identifierat som en sårbarhet.

Respondenten förklarar att man måste ha rutiner som innefattar cybersäkerhet och att detta kontrolleras specifikt under SIRE inspektioner. Respondenten säger att rutinerna ser olika ut beroende på fall till fall, men oftast innebär det att man ska kontakta IT-företaget eller rederiets Company Safety Officer så får dem göra en utvärdering om situationen och vilka åtgärder som ska vidtas. Ett exempel på en åtgärd är att isolera de system som har blivit utsatt för virus förklarar respondenten. Det som mer kontrolleras under en SIRE inspektion är de USB låsen som av rekommendationer från OCIMF ska finnas ombord bland annat till ECDIS säger respondenten. Respondenten är skeptisk till USB låsen och förklarar att det är enkelt för inspektören att fysiskt verifiera att det faktiskt sitter ett USB lås i ECDIS och respondenten upplever att det mest är för syns skull. Ytterligare beskriver respondenten att det finns olika nivåer av rutiner inom verksamheten för cybersäkerhet. Det är krav på lösenordshantering, periodvis byte av lösenord samt hur säkra lösenorden är med antal och typer av tecken dels det praktiska i vardagen att anställda inte lämnar något system inloggat när man lämnar datorn eller terminalen. Fortsättningsvis beskriver respondenten en högre nivå där man tar hänsyn till cybersäkerhet med underleverantörer i upphandlingar av olika system till befintliga fartyg men också under nybyggnation av fartyg.

För att i god tid upptäcka ett cyberhot beskriver respondenten två nivåer av aktiviteter inom rederiet, den mänskliga medvetenheten samt IT-program och brandväggar. För att öka medvetenheten och kunskapen hos verksamhetens anställda har både kontor- och ombord personal genomfört en utbildning gällande cybersäkerhet. En väsentlig del i rederiets arbete är att alla anställda har fått skriva under rederiets omfattande IT policy där det är beskrivet hur man ska förhålla sig till IT och OT. Signaturen ses som en fundamental grund för att veta att personal förstått riskerna. Policyn tecknas av alla nyanställda men också om någon anställd skulle växla fartyg inom rederiet. När rederiet anställer nya befäl till fartygen får de genomgå en introduktionskurs på kontoret som omfattar två dagar där de får ta del av verksamhetens policys, utbildningar, arbetssätt och rutiner förklarar respondenten. Vidare förklarar respondenten att de använder sig av vanliga antivirusprogram och tillägger att alla program och system har automatiska uppdateringar som användare inte kan neka så alla program och system alltid har den senaste uppdateringen för att minska säkerhetsrisken. Ytterligare beskriver respondenten ett program som filtrerar mejl från udda avsändare och reagerar på massutskick, programmet larmar om ett sådant mejl kommer och då får användaren göra ett aktivt val utan att behöva öppna de om mejlet är ok eller skräp. Ibland kan det hända att viktig information blir stoppad av programmet därför är det bra att man själv får välja säger respondenten.

"...de funkar ganska bra, och det är faktiskt väldigt ofta jag tror jag kanske har fyra, fem, sex såna mejl per dag som jag liksom aktivt verifiera om dom är ok eller om det bara är skräp."
(Respondent 1)

Om ett cyberhot skulle inträffa hos rederiet så tror respondenten att det skulle innebära en mindre driftstörning och att det inte skulle ta speciellt lång tid innan verksamheten är igång igen. Det är heller inget arbete som går förlorat fortsätter respondenten, det utförs säkerhetskopiering av

rederiets verksamhet flera gånger per dygn. Respons planen för ett cyberhot är som en checklista där det står vem som ska göra vad och vad som ska göras avslutar respondenten.

5.1.3 Analys av nivå

Respondenten säger att eftersom rederiet är inom tank segmentet och menar på att det har blivit en vardag med alla olika krav från organisationer och oljebolag samt att implementeringen av kraven från IMO inte var någon större utmaning för verksamheten. Det enda som respondent beskrev som lite utmanande var att förklara för hens äldre kollegor varför de måste ha lite mer avancerade lösenord samt varför de behöver byta lösenord oftare.

"...sen tror jag också detta är en generationsgrej, jag tror det är lättare att utan behöva förklara så mycket för någon lite yngre vad det här är, som ändå kanske förstår att man inte ska ha sin frus namn som lösenord…" (Respondent 1)

Respondenten anser att man bäst skyddar sig mot ett dataintrång är medvetenhet och beskriver med ett exempel att man kan ha ett jättebra och säkert system men att systemet aldrig blir bättre än personen som brukar systemet. Mer tillägger respondenten att man måste ha en diskussion med underleverantörerna när man köper system, hur uppdateringar ska ske och vad det finns för möjligheter till distanssupport och hur säkerheten kring det ser ut.

Respondenten upplever att sjöfartens cyberhot är mer specifikt om man jämför med andra industrier. Då syftar respondenten på fartygen och beskriver att om ett fartyg skulle bli utsatt för en omfattande cyberattack som i sin tur slår ut hela fartyget och är därför behov av fysisk hjälp kan det bli svårt, ett fartyg har inte direkt en adress likt ett kontor. Vidare upplever respondenten att liknande lagkrav borde implementeras i andra industrier och nämner att det redan finns lite för alla industrier att förhålla sig till och syftar på GDPR-lagstiftningen men tillägger att den inte alls är så utförlig och specificerad som sjöfartens.

Respondenten säger att rederiets arbete med cybersäkerhet omfattar mer än vad de kommande lagkraven kräver. Med tanke på att rederiet är verksamma inom tanksjöfart menar respondenten att på grund av SIRE inspektionerna och tidigare krav från oljebolagen att de redan lever upp till kraven från IMO. Avslutningsvis tror respondenten att alla tankrederier är oftast väl förbereda oavsett lagstiftning jämfört med andra segment inom industrin.

"...jag tror alla tankrederier hade nog svarat samma men de är typ vårt standardsvar oavsett vad du frågar om för någon lagstiftning" (Respondent 1)

5.2 Rederi B

Andra respondenten arbetar på ett medelstort tankrederi och arbetar som HSE Manager. Befattning hos rederiet innebär att respondenten är ytterst ansvarig för säkerhetsfrågor, främst relaterat till DPA och CSO. Rederiet i fråga arbetar med dokumentation och utbildning relaterat till cybersäkerhet inom organisationen. Men respondenten beskriver emellertid att rederiet valt att outsourca de tekniska bitarna till en IT-leverantör med specialiserad kunskap om cybersäkerhet.

5.2.1 Nulägesbeskrivning

Respondenten beskriver att rederiet i fråga inte opererar några avancerade system på kontoret och menar därför att dessa inte heller är integrerad med övrig verksamhet. Respondenten menar att begreppet cybersäkerhet förknippas med det klassiska syntänket. Det vill säga att rederiet besitter rätt procedurer för att skydda lösenord till verksamhetens program och mejl. Tillika förknippar respondenten begreppet, cybersäkerhet, med det tillvägagångssätt som rederiet implementerat för att säkerställa att rederiets system oavbrutet fungerar. Första gången begreppet cybersäkerhet påträffade för respondenten var jobbrelaterade.

"Utifrån min synvinkel så är de ju mestadels bara de enkla grejerna, bland annat lösenordsskyddade. Vi håller inte på med så avancerade saker… man kan ju inte ta över en båt till exempel, en hacker kan ju inte köra båten via mejlen om man säger så. Samtidigt innebär det att allt ska fungerar och att ingen ska förstöra dem, varken medvetet eller omedvetet." (Respondent 2)

Respondenten förklarar att det är väldigt mycket av de arbete som rederiet gör sker online och att det skickas väldigt mycket information över internet. Fortsatt beskriver respondenten att ett av de stora hoten mot verksamheten skulle vara en attack som slog ut internet och mejlen och skulle det ligga nere så skulle verksamheten bli lidande för att fungerar inte de systemen så kan de inte utföra sitt jobb.

"Jag skulle säga att hoten det är att våran verksamhet… blir lidande, att vi inte kan göra vårat jobb om grejerna inte fungerar. Väldigt mycket bygger på att man ska göra saker online på olika ställen och skicka väldigt mycket information. Funkar inte systemen så är ju vi helt utslagna. Om mejlen eller internet ligger nere så kan vi gå och hämta kaffe, de är inte mycket mer vi kan göra." (Respondent 2)

Respondenten menar att verksamheten betraktar cyberattacker som ett allvarligt och verkligt hot. Respondenten beskriver att rederiet så gott som dagligen blir testade av försök till dataintrång. Rederiet har outsourcat IT-säkerheten och respondenten förklarar att det företaget är duktiga på att hålla borta mycket av de hoten som kommer på mejl, även om respondenten är transparant och erkänner att olyckor har förekommit.

"Om man inte ser upp, de kommer ju nästan dagligen olika skojiga mejl, nån som vill att man ska klicka på nått och såna här grejer… nu är ju IT-leverantörens spamfilter och grejer väldigt bra, dom är duktiga på att hålla undan sånt. Men de har väl ändå hänt någon har gjort något misstag." (Respondent 2)

Respondenter vittnar om att rederiet flertal gånger fallit offer för de konsekvenser som förknippas med cyberattack. Rederiet har vid flertal tillfällen blivit utsatta där anställda av misstag öppnat ett infekterat mejl. Attackerna har resulterat i att rederiets system slagit ut helt vilket i sin tur påverkar kontor såväl som fartyg.

"Jag vet inte om man kan kalla det för dataintrång, men vi har ju haft några gånger till exempel, någon som öppnat nått mejl som dom inte borde gjort som slagit ut hela systemet… det har ju hänt, de har väl inte legat nere någon längre stund men de är klart de har blivit problem de har de ju" (Respondent 2)

5.2.2 Utmaningar med implementering av resolution

Respondenten beskriver att rederiet implementerat ett antal procedurer i samband med *Cyber Risk Management*. Procedurerna har implementerats på kontor såväl som fartyg, där alla grundar sig i att öka medvetenhet och skydd för cybersäkerhet. Respondenten beskriver att säkerheten ombord fartygen är ett komplicerat ämne där rederiet saknar kompetens. Av den anledning anser rederiet att det är ett bra komplement att outsourca detta område till en professionell IT-leverantör som besitter specialiserade lösningar för att skydda fartygets omfattande system. Arbetet består bland annat av att flytta serverar till IT-leverantörens lokaler, med hjälp av detta elimineras risken för nedstängning. Respondenten beskriver att servrarna står bakom låsta dörrar, kyld miljö och förses med egen eltillförsel för att garantera drift.

Respondenten säger att det som rederiet skickar mellan kontoret och fartygen inte är av något större värde eller intresse för en genomsnittlig hacker att stjäla. Emellertid menar respondenten att det största hotet rederiet identifierat med att bedriva rederiverksamhet med fokus på data och tillgång skulle vara att någon konkurrent skulle följa deras dagliga verksamhet. Med hjälp av att en konkurrent får insikt i verksamheten kan hen agera affärsmässigt fördelaktigt. Men det är inte bara konkurrenter som rederiet uppfattar som hot utan respondenten menar att man identifierat cyberattacken ransomware som ett påtagligt hot.

"Ja det är nog det stora hotet i så fall. För att hackare vet att det blir så jäkla jobbigt om vi blir av med våra system…" (Respondent 2)

För att upptäcka ett potentiellt cyberhot i god tid och ta eventuella säkerhetsåtgärder har rederiet använt sig utav utbildningar. Utbildningarna fokuserar på att höja kunskap och medvetenhet om *Cyber Risk Management* hos rederiets anställda på kontor och fartyg. Utöver detta har rederiet implementerat ett antal procedurer för ökad cybersäkerhet. Bland annat godkänns leverantörer som utför arbeten hos rederiet på förhand, detta grundar sig i att man inte tillåter en obehörig aktör att få tillträde till nödvändiga system. Tillika menar respondenten att IT-leverantören har spärrat ett antal webbsidor och program som förknippas med ökad risk. Respondenten förklarar att rederiet tillsammans med IT-leverantör låst alla webbsidor till en början, där anställda efterhand får uttrycka vad dom tycker att rederiet bör låsa upp. Detta arbetssätt möjliggör att rederiet tillsammans med sina anställda utför egenkontroll där man noggrant väljer det webbsidor som tillåts. Respondenten beskriver att proceduren kan uppmärksammas lite hämmande men samtidigt är det ju för att inga olyckor eller misstag ska äga rum. Tillika är alla skrivare ombord fartyget utrustad med ett eget USB uttag som kan användas av inblandade aktörer vid begäran av utskrift av dokument, där önskad part kan ansluta USB stickan direkt i skrivaren. Skrivaren är inte ansluten till fartygets övriga nätverk och kan då inte gå bakvägen in på servern den vägen. Arbetet med att helt eliminera hanteringen av USB stickor ombord är svårt, lösningen med sjökortuppdateringarna till ECDIS är

något som ännu inte är löst och uppdateringarna flyttas fortfarande med USB sticka säger respondenten.

Respondenten uttrycker att hen känner sig bekväm med de tillvägagångssätt och procedurer rederiet tagit för att skydda sig för cyberattacker. Om en attack förekommer menar respondenten att de åtgärder man tagit förverkligar rederiets syn på att verksamheten ska fortsätta bedrivas oavsett om en cyberattack förekommer eller inte. Respondenten beskriver också att om ett system ligger nere så finns ett antal telefonsystem vilket fungera som kommunikationsmedel då mejl eller andra program ligger nere. Tillika menar respondenten vidare att om det skulle bli en störning i verksamheten är frågan bara om hur stor omfattningen är. Respondenten beskriver att skull exempelvis hela ekonomiprogrammet försvinna skulle detta i sin tur resultera i att fakturor och löner släpar efter, men inte allvarligare än det. Den centrala beredskapsplanen vid ett dataintrång mot verksamheten är att anställda kontaktar deras IT-leverantör för att erhålla hjälp.

5.2.3 Analys av nivå

Arbetet med att implementera cyber risk hantering och uppfylla de kriterierna som har ställts från IMO har inte uppfattas som några svårigheter inom verksamheten. Respondenten säger att de flesta inom verksamheten har förståelse för arbetet med cybersäkerhet och är införstådda att det är så de nya rutinerna ser ut nu.

"Nä de har varit, ganska okej jag tror dom flesta har förståelse för enkla grejerna att inte installera några program eller stoppa in USB stickor hej vilt och olika grejer och så, de har inte vart nån… inga svårigheter med de nä." (Respondent 2)

Baserat på respondentens erfarenhet så beskriver hen att man bäst skyddar sig mot ett dataintrång är en blandning av medvetenhet, kunskap och tekniken från deras IT-leverantör. Respondenten fortsätter att förklara betydelsen om att vara medveten om riskerna och ger exemplet att någon anställd av misstag kan lämna ut ett lösenord till fel person och då är det lätt komma runt tekniken.

Respondenten upplever att alla verksamheter som använder datorer och kommunikation ställs inför samma cyberhot som sjöfarten och att reglerna och procedurerna skulle kunna appliceras på vilken verksamhet som helst. Vidare ger respondenten exemplet att många företag har flera lokaler, kontor och dotterbolag runt om i världen som kan jämföras med rederiernas fartyg.

Respondenten förklarar att arbetet de gör i nuläget för att uppfylla lagkravet har sin grund från oljebolagen och att det är de som har drivit deras arbete hittills. Respondenten uttrycker en oro över att allt mer system och program förlitar sig på uppkoppling till internet. Avslutningsvis anser respondenten att det är en styrka att rederiet själva har hand om dokumentationen gällande cybersäkerhet och menar att detta arbetssätt ger dom full egenkontroll. Respondenten menar att ur ett cybersäkerhets perspektiv är det bra om rederierna inte förlitar sig för mycket på att driva systemen med hjälp av en dator utan istället mänsklig kraft.

"...en styrka som vi har är att vi gör allting själva… detta gör att vi klarar oss och har koll på det som bör göras… och de kanske är bra ur cyber security att vi kanske inte lagt ut allting på

dataprogram, vi har ju fortfarande lite pärmar och papper kvar som vi kan slå i om de behövs." (Respondent 2)

5.3 Rederi C

Respondenten arbetar på ett mindre tankrederi med befattning som Crew och Quality Controller. I arbetet med *Cyber Risk Management* har rederiet valt att dela upp ansvaret till två utomstående företag. Vad gäller dokumentation med anknytning till det nya lagkravet använder sig rederiet av ett utomstående managementbolag som har fokus på att hjälpa rederier med varierande uppgifter. Ansvaret för att uppfylla lagkravet utifrån ett tekniskt perspektiv har valts att delegeras till ett teknikföretag med IT-lösningar för den maritima industrin.

5.3.1 Nulägesbeskrivning

Respondenten påträffade för första gången studiens forskningsämne, cybersäkerhet, i ett företagsrelaterat sammanhang. Respondenten beskriver att cybersäkerhet främst handlar om att säkerställa att ingen obehörig aktör får tillgång till rederiets system.

"För mig rent personligt så är det ju att vi ska säkerställa så att vi inte blir hijacked... att inte kommer någon in i våra system och förstör våran verksamhet…" (Respondent 3)

Vidare beskriver respondenten att mycket av arbetet med *Cyber Risk Management* handlar om att eliminera risken för otillåtet intrång i rederiets nödvändiga system. Syftet med att säkerställa så att inte otillåtet intrång kan förekomma grundar sig i att man inte vill att system förstörs som i sin tur resulterar i att rederiet förlorar inkomst eller människoliv.

Respondenten ser att risker och hot mot verksamheten existerar främst i förhållande till att bli hackade. Hen anser att hackningen i sin tur resulterar i ett krav på lösensumma alternativt sabotage vilket i sin tur genererar ökade kostnader för rederiers IT-avdelning. Respondenten beskriver också att den inte bara är IT-avdelningen som påverkas av ett intrång utan också övriga anställda på grund av att affärssystem inte allt för sällan är ur funktion under en attack vilket förhindrar det dagliga arbetet. Respondenten beskriver att en tidigare chef definierade personer med syfte att otillåtet ta sig in i något utav företagssystem som de nya piraterna på havet.

"... tidigare chef kallade hackare de nya piraterna." (Respondent 3).

Respondenten anser att hotet är verkligt men att risken för att bli utsatta för en attack som mindre rederi är liten. Svaret har sin grund i att respondenten anser att risken minineras i ett mindre rederi i förhållande till ett större på grund utav dess anonymitet. Dock härstammar svaret också ifrån att rederiet i fråga aldrig blivit utsatta för ett dataintrång.

"I relation till större rederier så tror jag risken är betydligt mindre för att vi är ett litet och ganska anonymt företag … Men visst det kan hända, man vet aldrig." (Respondent 3)

5.3.2 Utmaningar med implementering av resolution

Respondenten beskriver att rederiet valt att outsourca allt arbete förknippat med DoC till dess managementbolag. Av den anledning är det managementbolaget som ansvarar för rederiets dokumentation rörande *Cyber Risk Management* och ser till att uppfylla de kriterier som ställs från IMO. Tillika har rederiet ingen egen besättning utan valt att delegera denna funktion till samma managementbolag. Respondenten menar att samarbetet fungerar bra och att managementbolaget erbjuder utbildningar till besättningen i syfte att öka kunskap och erfarenhet i ämnet. Dessutom bidrar managementbolaget med riktlinjer till rederiet på hur man ska uppnå kriterierna som ställs från IMO. På samma sätt har rederiet valt att outsourca den tekniska biten till en utomstående IT-leverantör med specialiserad kunskap för IT-lösningar inom den maritima industrin. Med andra ord har rederiet delat upp arbetet med *Cyber Risk Management* till två utomstående bolag där de tekniska kriterierna uppfylls av en utomstående IT-leverantör och utbildningar samt dokument uppfylls i samarbete med managementbolaget.

Rederiet arbetar kontinuerligt för att identifiera vilka sårbarheter det finns med att bedriva rederiverksamhet. Tillsammans med dess managementbolag har de identifierat sårbarheter som formulerats till en prioriteringslista. Respondenter menar att listan syftar till att hjälpa landpersonal såväl som besättning ombord fartygen med att vara vaksamma och försiktiga med det punktade riskerna. Respondenten menar att listan underlättar för anställda i arbetet med att identifiera påtagliga risker förknippade med driften av fartyg. Tillika har alla rederiets fartyg utvärderas där en riskanalys har legat till grund för att identifiera risker bland de system som är installerade ombord det specifika fartyget.

"... varje fartyg har gjort sin egen riskanalys, där de identifierat exakt vad dom ser som risk på sina fartyg..." (Respondent 3)

Ett av systemen som identifierats som risk är det elektroniska sjökortet ECDIS, vilket är ett potentiellt system som kan användas för otillåtet intrång. Tillika anser rederiet att system som är förknippade med fartygets framdrift eller förflyttning av last är förknippade med ökad risk och det är därmed av stor vikt att skydda. Respondenten menar att det fundamentala arbetet för att skydda sig för cybersäkerhet grundar sig i att bibehålla egenkontroll över fartyget.

Respondenten beskriver att med hänsyn till att rederiets fartyg transporterar olja och kategoriseras som oljetanker så blir dom vid flertal tillfällen inspekterade genom så kallade vetitingar. Vid inspektionstillfället utvärderas fartyget och dess besättning för att kontrollera om de uppfyller kraven som är nedskrivna av OCIMF i formuläret, SIRE version 7 (VIQ7). Respondenten uttrycker att rederiets fartyg aldrig fått en anmärkning vid dessa inspektioner, vilket respondenten tror beror på att rederiets arbete kan ses som en kopia på kriterierna i VIQ7.

"Vi har inte fått en enda anmärkning på detta sen de kom in 2018..." (Respondent 3)

Rederiet arbetar tillsammans med deras samarbetspartner för IT-frågor med att installera säkerhetskontroller såsom brandväggar. Dessutom har rederiet en strukturerad säkerhetskontroll över de underhållsarbeten som utförs ombord fartygen. Tillsammans med IT-leverantören

utvärderas och godkänns alla underhållsarbeten på förhand. Med hjälp av detta strukturerade arbetssätt bibehåller företaget kontrollen över vilka som får tillgång till systemen vilket resulterar i att risken för otillåtet intrång elimineras. Vidare har man identifierat att USB stickor är en potentiell risk. Respondenten beskriver att portabla USB stickor är vanligt förekommande ombord fartyget, där inblandade parter i driften av fartyget önskar att skriva ut dokument frekvent. Rederiets lösning till problemet är att installera en speciell skrivare ombord som inte är kopplad till fartygets övriga nätverk och kan av den anledningen inte heller påverka negativt om ett virus är ett faktum.

Respondenten uttrycker att i händelse av att ett system ligger nere så har rederiet dokument vilket beskriver hur anställda ska agera för att återställa systemen. Dock anser respondenten att den största risken är besättningen ombord, därmed arbetar rederiet med att utbilda anställda för att öka kunskap och erfarenhet.

"... den största risken är människan just nu, de ombord..." (Respondent 3)

Utöver utbildningar har IT-leverantör i syfte att säkerställa säker drift hjälpt rederiet med att separera besättningens nätverk från de nätverk som används i affärsändamål. Tillika beskriver respondenten att IT-leverantören övervakar rederiets system varje dag i syfte att identifiera hot eller fel.

Respondenten beskriver att trots att rederiet har varierande ålder på sina fartyg är systemen för cybersäkerhet likvärdiga. Det är ingen större skillnad mellan systemen för säkerhet dock finns det en viss skillnad på hur man övervakar system tillika vilka spärrar och brandväggar som existerar.

Med tanke på de sårbarheter och risker som förknippas med att bedriva rederiverksamhet så beskriver respondenten att tillsammans med IT-leverantören har man utformat en beredskapsplanering. Bland annat innehåller beredskapsplaneringen en backup-plan som vid händelse av ett dataintrång kan återställa alla berörda system till sitt ursprungliga tillstånd.

"Absolut ... vi har en backup-plan emergency plan hur de ska återställa allting..." (Respondent 3)

Respondenten beskriver att mycket av arbetet för att eliminera risken och i god tid upptäcka ett otillåtet intrång grundar sig i personligt ansvar. Det är viktigt att anställda individuellt utvärderar om det är en verklig avsändare till mejlet samt att ständigt vara skeptisk till allt som inte är av vanlig praxis. Rederiet utför kontinuerligt utbildningar i säkerhetsfrågor där *Table Topdrills* fungerar som ett möte där anställda diskuterar ämnet samtidigt som kunskap och erfarenhet förmedlas och utbytes mellan anställda. Om en anställd på rederiet är i behov av att öppna ett mejl som utmärker sig för att vara av riskkaraktär menar respondenten att IT-leverantören hjälper rederiet med att undersöka om det är okej eller inte att öppna. Om olyckan är framme och en händelse i form av en attack utförs beskriver respondenten att rederiet kontaktar dess IT-leverantör som med hjälp av säkerhetskopior återställer nödvändiga system till ursprungligt tillstånd.

"… ja man ska ju titta att det är en riktig avsändare… sen titta ständigt på allt konstigt och inte klicka på sånt man inte känner igen… om man nu måste klicka då ska vi kontakta IT-leverantör och fråga, vad är detta, kan vi öppna den och så där...." (Respondent 3)

Med hänsyn till allt arbete som rederiet utför i relation till *Cyber Risk Management* beskriver respondenten att de är övertygade om att rederiet lever upp till det kriterier som ställs från kommande lagkrav. Respondenten beskriver att antagandet har sin grund i de avklarade SIRE inspektioner och det underliggande arbetet tillsammans med IT-leverantören. Mot denna bakgrund har rederiet en kunskap och erfarenhet för att bemöta de kriterier som förknippade med resolutioner från IMO.

"Vi uppfyller den! Det vet jag för det har jag intyg på av IT-leverantören som vi använder till vetting-bolagen. Inspektörerna tycker att det ser jättebra ut, jättenöjda och jätteglada… så jag tror vi uppfyller alla, eller ja, jag vet att vi gör det" (Respondent 3)

5.3.3 Analys av nivå

Respondenten beskriver att arbetet med att leva upp till de kriterier som ställs från IMO har inte inom rederiet upplevts som utmanande. Med tanke på att rederiet i fråga är av mindre typ så har det själva inte kapacitet att arbeta med IT-säkerhetsfrågor på egen hand utan har valt att outsourca till företag med specialiserad kunskap inom ämnet. Respondenten beskriver att utifrån hens erfarenhet så är det viktigt att besitta expertkompetens inom IT-området för att rederiet själv ska besitta kunskap för att leva upp till de krav som ställs från IMO 2021. Respondenten anser att delegering till ett professionellt företag är ett väl fungerande alternativ.

"....hade vi inte haft våran IT-leverantör så hade vi inte klarat av det, det kan jag säga… vi är alldeles för få... du måste verkligen vara expert och vanliga rederiarbetare klarar inte det, du måste vara en high tech, nästan IT-nörd för att klara det… det tror jag." (Respondent 3)

Respondenten upplever vidare att dataintrång inte är unikt för sjöfarten, utan att risken är aktuell inom andra industrier. Respondenten besitter själv erfarenhet av flertal attacker som utförts inom rederier och underleverantörer, båda förknippade till sjöfartsindustrin. Vad som kännetecknar dessa attacker är den gemensamma faktorn om att otillåten access till företagens system resulterar i att det läggs ner. För att låsa upp systemen och återställa dem till ursprungligt tillstånd krävs företagen på en lösensumma.

Respondenten anser att utifrån hens erfarenhet är stora företag väl insatta i ämnet medan det finns det mindre kunskap och förberedelser inom små organisationer. Avslutningsvis anser respondenten att rederiet i fråga är väl förberedda på det kommande lagkravet. Det finns en stark känsla av att rederiet inte bara uppfyller kraven utan även att rederiet arbetar utöver vad lagstiftningen kräver.

"Nej jag tror vi är över ... men det är min känsla ..." (Respondent 3)

5.4 IT-leverantör

Den fjärde respondenten arbetar som COO - Chief Operating Officer hos en välkänt IT-leverantör med specialiserad kunskap inom cybersäkerhet. Företaget besitter lång erfarenhet inom området och arbetar inte allt för sällan tillsammans med tankrederier för att skräddarsy system som förhindrar och skyddar så att obehöriga aktörer inte har möjlighet att utföra otillåtna intrång i rederiets system. Med hjälp av detta delkapitel förmedlas ett utomstående perspektiv till studiens forskningsfrågor vilket ökar studiens pålitlighet.

5.4.1 Nulägesbeskrivning

Med tanke på respondentens långa erfarenhet inom IT-säkerhetsfrågor minns inte hen om begreppet påträffades i ett privat eller företagsrelaterat sammanhang för första gången. Respondenten menar att vad som är viktigt att belysa är begreppets utveckling inom sjöfarten det senaste 10 åren. Respondenten menar att cybersäkerhet är ett begrepp som har funnits under en längre tid, men dess innebörd har kommit att ändras över tid. Eftersom respondenten har arbetat inom IT-säkerhetsindustrin under en längre tid menar hen att ordet cybersäkerhet är ett populistiskt ord för det annars vanligt förekommande säkerhet.

"Cyber Security är ett populistiskt ord för säkerhet" (Respondent 4)

Respondenten beskriver att intresset för cybersäkerhet expanderade i takt med att användandet av internet blev en självklarhet. Rederier ansåg att internet var ett system som underlättade för besättning såväl som landpersonal. Av den anledning menar respondenten vad industrin idag förknippar med begreppet, cybersäkerhet, var inte densamma under internets blomstrande tid. Grunden i vad vi idag förknippar med cybersäkerhet fick sin start i samband med Maersk incidenten, NotPetya. Vi denna attack tog en utomstående aktör kontroll över verksamhetens datasystem som i sin tur genererade förödande operationella och ekonomiska konsekvenser. Attacken var ett allmänt uppvaknande inom sjöfartsindustrin där flertal företag inte besatt förmåga att skydda sig för det stigande hotet. Det var under denna tid som företag såväl som lagstiftande organisationer uppmärksammade att problemet är verkligt.

"Maersk-incidenten kan ses som starten av det vi förknippar Cyber Security med idag"
(Respondent 4)

Respondenten menar att intresset från sjöfarten att skydda sig började redan 2004 då de första fartygen installerades med internet. Intresset med att skydda sig vid den tidpunkt förknippades då inte med begreppet cybersäkerhet utan ansågs mer vara en säkerhetsrutin, eftersom man installerade ett nytt system ombord. I takt med att flertal företag såg syfte i att använda internet uppmärksammade samtidigt IT-leverantörer ett accelererande antalet data intrångsförsök hos rederiers kontor och fartyg. Respondenten beskriver att redan 2006 hjälpte hen som IT-leverantör rederier med att installera spamfilter och uppdelade nätverk mellan nöjes- och affärsrelaterat i syfte att skydda mot intrång. Besättningen ombord var vid den tidpunkt kritisk till de krav som IT-leverantören ställde på säkerhet eftersom åtgärderna innebar en viss reglering i användandet av internet, där flertal webbsidor inte var aktuella.

"Vid den tid ansåg besättningen att man var en jobbig jävel som bara förstörde, den attityden ser vi inte ombord idag" (Respondent 4)

Respondenten menar att det största hotet inom cybersäkerhet mot sjöfartsindustrin är internt. Respondenten beskriver att det flesta fall av dataintrång hos rederier beror på att en anställd av misstag tryckt på en länk eller godkänt nedladdning av en fil. Dessutom är det vanligt att anställda använder sig av USB stickor som är infekterade med virus vilket i sin tur påverkar rederiets system. Dessa typer av intrångsförsök hos rederier förknippas som ransomware och phishing. Tillika anser respondenten att aktörer från främmande land eller konkurrent som agerar med en uppsåtlig handling att skada ett rederi inte existerar. Svaret grundar sig i att rederier besitter väldigt lite information som anses vara av värde för en hackare.

"Det finns ingen utomstående aktör eller hackare som är intresserad av färgbeställningar, flygbiljetter eller grossistbeställningar" (Respondent 4)

Emellertid menar respondenten att hotet dagligen existerar i rederiers system och program. Respondenten beskriver att idag är det svårare att urskilja om exempelvis ett mejl är infekterat med virus eller inte med tanke på att det ser normalt ut i förhållande till övriga mejl. Av den anledning anser respondenten att rederier som inte besitter kontroll över tillbörliga system för att sortera otillåten access, såsom spamfilter och brandväggar, agerar felaktigt.

Respondenten upplever att cyberattacker är ett riktigt hot, men att det nödvändigtvis inte är riktat mot verksamheter som förknippas med sjöfart. Respondenten menar att syftet med attacken inte är att specifikt rikta sig mot en sjöfarts verksamhet utan snarare till vilken verksamhet som helst. Respondenten menar att hotet mot en verksamhet existerar så länge verksamheten använder sig av internet eller annan uppkoppling. Vad som kännetecknar det större hotet inom sjöfartsindustrin är om en främmande aktör får kontroll över OT-system, där framdrivning och navigation är några av systemen. Besitter en aktör kontroll med syfte att utföra en skadlig handling kan ECDIS eller maskin användas för att orsaka förödande konsekvenser. Respondenten beskriver att teoretiskt sätt existerar hotet så länge ett system är uppkopplat mot internet eller med sladd till annan uppkoppling.

"Besitter fel aktör kontroll av ett LNG-fartyg kan en skadlig handling få förödande konsekvenser" (Respondent 4)

5.4.2 Utmaningar med implementering av resolution

Hos IT-leverantören arbetar en ytterst ansvarig Security Officer med efterlevnaden av de krav som ställs från IMO såväl som oljebolag. Respondenten beskriver att företaget samarbetar kontinuerligt tillsammans med en DPO för att konstruerat ett strukturerat tillvägagångssätt för att möta de krav som ställs från OCIMF och IMO. Respondenten beskriver att arbetet bland annat består av att vara certifierade i enlighet med ISO 27 001 vilket innehåller vägledning för implementering av informations säkerhetskontroll som ligger till grund för ett pålitligt säkerhetsarbete. Respondenten beskriver att arbetet med att uppfylla kraven inte alltid är upp till IT-leverantören utan beslut tas tillsammans med rederi om hur ansvarsområden ska delegeras. I respondentens kundportfölj finns

mindre och större rederier som alla delar uppfattningen om att den tekniska biten för IT-säkerhet är svårt.

"ISO 27001 är ett utav de tillvägagångssätt som finns i arbetet med Cyber Security"
(Respondent 4)

Respondenten beskriver att arbetet med IT kan variera mellan företag. Men vad som kännetecknar stora rederier är att de inte allt för sällan besitter en egen IT-avdelning där Security Officer eller IT-Manager har ytterst ansvar för cybersäkerhet. Inom de mindre rederierna existerar inte samma omfång av IT-avdelningar utan ansvariga personer består av DP och tekniska chefer. Respondenten menar att oberoende av storlek så är hotet ett faktum och av den anledning samarbetar man tillsammans med kund för att eliminera risken av ett intrång. Om ett dataintrång har påträffats ombord ett fartyg eller kontor existerar en strukturerad beredskapsplan med ett stegvis förarbetat tillvägagångssätt. Om en attack har skett innebär det första steget att identifiera vad som har hänt. Utifrån händelse utvärderas skador där en analys utformas som förmedlas till kontaktperson hos rederiet. Om olyckan påträffats ombord ett fartyg kontaktas kapten som i sin tur tillhandahåller analysen innehållande information om när, var och hur händelsen inträffade. Baserat på informationen är kaptenen kapabel att i sin tur undersöker skadan och identifierar hur omfattande skadan är. I det flesta fall menar respondenten att ett infekterat USB resulterat i att system lagts ner och satt igång nödvändiga responsåtgärder. I de fall där det existerar ett infekterat USB klipps denna på mitten för att inte användas igen, IT-leverantören reparerar skadorna på distans, där kapten sedan får en ny USB sticka att använda.

Om en olycka är framme och fartyget är infekterat menar respondenten att det är viktigt att man tillhandahåller en säkerhetskopia av nödvändiga system. Respondenten beskriver att med hjälp av en säkerhetskopia kan berörda system återställas till sitt ursprungliga tillstånd innan attacken. Hur ofta man säkerhetskopierar varierar mellan rederier, men respondenten beskriver att inom deras företag har man valt att utföra säkerhetskopieringar hela tiden mot bakomliggande servrar. Men alternativen existerar också från dagligen, veckovis, månadsvis, halvårs och årsvis. Respondenten beskriver att omfång av hur många system som ska säkerhetskopieras baseras på vilka system som anses vara nödvändiga för att bedriva verksamheten. Den viktigaste faktorn är att inte rederi ska förlora för mycket nödvändig information vilket i sin tur påverkas tidsmässigt och ekonomiskt.

"Ibland använder vi 3 månader gamla säkerhetskopior åt kunder. Bakomliggande faktorer kan vara att kapten av misstag raderat nödvändig fil, programvara eller genväg på skrivbord"
(Respondent 4)

5.4.3 Analys av nivå

Att hjälpa rederier leva upp till de kriterier som ställs från IMO och TMSA anses inte från respondenten som krävande. Respondenten menar att som anställd hos en IT-leverantör har man arbetat med liknande krav sedan 2006. Med fokus på sjöfart upplever inte respondenten att deras kunder ser det kommande lagkravet som krävande med tanke på att arbetet med cybersäkerhet har existerat länge. Liknande kriterier och krav på cybersäkerhet krävdes från de stora oljebolagen redan 2018, men även då låg de skandinaviska rederierna i framkant och befann sig på en nivå

ovanför kraven. Vad som särskiljer arbetet i enlighet med IMO från de tidigare kriterierna är kraven på dokument. Respondenten beskriver att det inom företaget ser ett skifte i arbetsuppgifter. Tidigare arbetade man mer med tekniska uppgifter till skillnad från idag där det är ett skifte till att mer tid läggs på att skriva tydliga dokument innehållande tillvägagångssätt och procedurer. Respondenten beskriver att rederier förr i tiden inte var intresserade hur IT-leverantören arbetar för att skydda dom mot cyberattacker utan mer att dom gjorde det. Idag är rederierna intresserade av hur arbetet med cybersäkerhet pågår och att detta arbetet tecknas skriftligt i dokument. Respondenten menar att detta grundar sig i kraven från IMO där procedurer och tillvägagångssätt är viktigt att formulera tydligt på dokument för att man ska klara inspektioner på efterlevnad.

"Vi går från de vanliga IT-sysslorna till att arbeta mer med dokument uppfyllande" (Respondent 4)

Att effektivt arbeta med att skydda sig inom ämnet cybersäkerhet består av att förstå helhetsperspektivet. Respondenten beskriver att förstå helhetsperspektivet är essentiellt, rederierna bör identifiera vilka risker som förknippas med att bedriva verksamheten. Men respondenten uttrycker också att rederier bör identifierar svaga länkar mellan fartyg och kontor. När rederier identifierade sårbarheter och risker är det viktigt att inte 100% fokusera på att eliminera en risk utan det är viktigare att vara förberedd på det mesta. Respondenten beskriver att det är bättre för rederier att arbeta på en rimlig nivå där man har möjlighet att lyckas. Lyckas man implementera en rimlig nivå menar respondenten att rederiet står på en bra grund för att skydda sig. Respondenten beskriver att rederiet bör kontinuerligt utföra riskanalyser, baserat på dessa implementeras uppföljande aktiviteter efterhand när rederiet identifierar vad som kräver mer arbete än vad grundnivå stipulerar. Att enbart arbeta med att utforma dokument, köpa en låda eller ett virusprogram är inte lösningen till att skydda sig mot cyberattacker. Att kontinuerligt utföra riskanalyser, lägga arbetet på en rimlig nivå bidrar tillsammans till ett sunt helhetsperspektiv anser respondenten. Respondenten uttrycker att det är den rätta vägen att gå i frågan om att skydda sig mot cybersäkerhet.

"Att köpa en röd låda, virusprogram eller ett dokument löser inte problemet" (Respondent 4)

Respondenten beskriver att samtliga rederier med anknytning till tanktransport inom Skandinavien befinner sig på en nivå i sitt arbete som är över vad kriterierna från IMO kräver. Respondenten menar att flertal rederier ser arbetet som en konkurrensfördel då det besitter trovärdiga system som fungerar trots att en tredje part försöker göra intrång i fartyget eller kontorets system. Med hjälp av att rederiet kan bedriva sin verksamhet dygnet runt året runt förlorar det ingen inkomst till följd av att ett system är nedlagt. Emellertid menar respondenten att lagkravet är öppet för egen tolkning där utländska rederier inte arbetar i frågan på samma sätt som skandinaviska. Respondenten menar att detta kommer att ändras i takt med att kunder och leverantörer blir med digitaliserade. Respondenten menar att det redan idag sker en förändring där fartyg, hamn och oljeföretag samarbetar för att lastning och lossning processer sker snabbare. En utav de centrala utvecklingarna under senaste åren är Bill of Lading som skickas elektroniskt mellan sändare och mottagare. Att utföra detta ställer krav på alla parter besitter ett trovärdigt datorsystem som inte havererar.

"IMO kräver att man identifierar hot, men kräver ingen nivå av hur mycket rederierna ska arbeta med hotet. Av den anledningen kan man enbart identifiera hotet utan fortsatt arbete"
(Respondent 4)

Respondenten anser att framtiden inom cybersäkerhet inte förknippas med striktare ansvar. Dock anser respondenten att tydligare definition av vilken nivå arbetet bör ligga på kommer att formuleras i framtiden. Direktiven kan förknippas striktare för det rederi som inte tillhandahåller en hög grad av arbete i dagsläget.

5.5 Resultattabell

I detta avsnitt presenteras de resultattabeller som används i syfte att besvara studiens forskningsfrågor. Vidare redogör bilaga 1 för analysen av det transkriberade materialet där Granheim och Lundmans (2004) analysprocess tillämpats. I tabellen ställs information från rederier i jämförelse till IMO:s rekommendationer i form av resolution MCS-FAL.1/Circ.3. Med hjälp av tabellen utvärderas hur rederier valt att implementera och arbeta med *Cyber Risk Management* i deras SMS. Med hänsyn till att MCS-FAL.1/Circ.3 innehåller rekommendationer för hur rederier bör arbeta med *Cyber Risk Management* anses tabellerna vara en bra bedömningsgrund på hur väl förberedda svenska tankrederier är inför det kommande lagkravet.

För att ta del av en mer ingående redogörelse av resultatet presenteras analyserat material i förhållande till studiens forskningsfrågor samt intervjufrågor i bilaga 2.

6 Diskussion

I följande kapitel diskuteras uppsatsens huvudsakliga komponenter med utgångspunkt i studiens forskningsfråga "Hur redo är svenska tankrederier inför de nya riktlinjer och krav som ställs från IMO 2021?" och tillhörande underfrågor gällande nulägesbeskrivning, utmaningar med implementering samt analys av nivå. Diskussionen baseras på de resultat som erhållits genom intervjuer och vad tidigare forskning inom ämnet samt den teoretisk referensramen. Kapitlet avslutas med en metoddiskussion där en beskrivning om vilka implikationer vald metodologi inneburit under studiens arbetsgång. Tillika diskuteras studiens reliabilitet och validitet. Avslutningsvis presenteras förslag till vidare forskning inom området.

6.1 Resultatdiskussion

Detta avsnitt delas upp i enlighet med studiens forskningsfrågor. Med hjälp av att jämföra rederiernas arbete med tidigare forskning skapas en förståelse för i vilken utsträckning svenska tankrederier är redo för det nya regelverket IMO 2021 - Cyber Risk Management. För att inte endast analysera rederiernas perspektiv i frågan har vi inkluderat en IT-leverantörsperspektiv på cybersäkerhet. Genom att kombinera perspektiven skapas en trovärdig diskussion där inte bara ett perspektiv tas i åtanke.

6.1.1 Nulägesbeskrivning

Studiens resultat visar att svenska tankrederier är väl medvetna om begreppet, cybersäkerhet, där majoriteten respondenter påträffade begreppet för första gången i ett företagsrelaterat sammanhang. Samtidigt tyder resultat i studien på att cybersäkerhet är ett begrepp som existerat under en längre period men ändrat mening över tid. Begreppet härstammar från internets uppkomst, då begreppet främst förknippades med onödiga säkerhetsåtgärder utan syfte. Respondenter menar att vid den tidpunkt existerade inte hotet i samma omfattning. Industrins synpunkt har kommit att ändras över tid där man sett en utveckling av attacker i relation till expansionen av internet. Idag anser försäkringsbolaget Allianz (2020) att cybersäkerhet är det främsta hotet mot global handel, vilket bland annat styrks av studiens resultat som visar att hotet existerar dagligen hos rederier. Respondent med specialiserad kunskap inom området beskriver att hotet existerar så länge ett rederi är uppkopplat mot internet eller en server. Sedermera visar studiens resultat också att hotet mot ett dataintrång expanderar i takt med rederiers val av att automatisera och digitalisera sin verksamhet. Denna problematik delar också Allianz (2020). Försäkringsbolaget menar att hotet är nära förknippat med verksamheters ökad tillförlitlighet till dess datasystem. Det är tydligt att det effektivitets fördelar ett företag söker med att digitalisera sin verksamhet samtidigt resulterar i en exponering av nya hot.

Resultat indikerar att vad sjöfartsindustrin idag förknippar med cybersäkerhet grundar sig i Maersk incidenten 2017, NotPetya. Vid denna attack föll flertal företag offer för attacken, varav Maersk var ett av dem. Tidigare forskning tyder på att konsekvenserna av attacken uppmärksammades av

flertal industrier där man delade uppfattning om att man inte är förberedd på ett liknande hot. Industrin delade uppfattning om att man inte besitter rätt procedurer eller system för att skydda sig. Studiens resultat stärker resonemanget och menar att Maersk (2017b) incidenten är den bakomliggande faktorn till en drastisk utveckling av åtgärder från lagstiftande- och inflytelserika organisationer (IMO/OCIMF). Studien tyder på att rädslan än idag förknippas med Maersk-incidenten. Respondenterna förknippar cybersäkerhet med att säkerställa så att en utomstående aktör inte har möjlighet att penetrera nödvändiga system. Rädsla existerar hos rederierna där oro uttrycks för att ett intrång ska resultera i utomstående kontroll eller sabotage av verksamheten. Dock indikerar studien på att graden av oro varierar mellan respondenterna, där åsikter tyder på att det finns värre hot inom industrin i nuläget att oroa sig över.

Emellertid visar historiska fakta att attacken inte var riktat mot Maersks organisation specifikt. En oriktad attack syftar inte till att attackera det enskilda företaget utan snarare antalet enheter och användare som attacken når, menar Ayala (2016). Studien delar uppfattningen och menar att sjöfartsindustrin inte främst förknippas som en industri som förmedlar värdefull information på samma sätt som andra industrier. Färgbeställningar, flygbiljetter, grossistbeställningar är inget av värde hos en hackare utan det är snarare sabotage eller kontroll över system i utbyte av en lösensumma som är intressant. Ayala (2016) beskriver att denna form av attack mot företag förknippas med begreppen malware, ransomware och phishing. I studiens resultat är det också dessa attackmetoder som är aktuella. Flertal respondenter vittnar om händelser där rederierna fallit offer för attackmetoderna. Vad som kännetecknar orsaken till att attackerna lyckas är organisationernas misstag. Resultatet visar att rederier förknippar anställda som den största risken mot deras verksamhet där oaktsamhet och misstag kan orsaka förödande konsekvenser. Studien beskriver att det inte är handlingar av uppsåt som ofta förekommer utan att det är anställdas misstag som resulterar i ett lyckat intrång. Flertal rederier vittnar om att anställda av misstag öppnat ett infekterat mejl eller besökt en virusbenägen hemsida som i sin tur resulterat i en nedstängning av berörda system.

Studien indikerar att hotet existerar dagligen inom rederiernas organisationer. DiRenzo, Goward och Roberts (2015) menar att en orsak till att hotet existerar är rederiernas system vilket drastiskt exponera industrin mot nya risker. Respondenterna delar DiRenzos, et al. (2015) uppfattning och beskriver att hotet grundar sig i rederiernas tillförlitlighet till deras omfattande system som finns på kontor, såväl som fartyg. Detta till följd av att systemen i någon form är uppkopplat till internet eller annan server vilket exponerar möjligheten till intrång. Studien tyder på att rederierna förlitar sig mycket till att systemen fungerar, där en nedstängning associeras som katastrofalt mot verksamheten.

6.1.2 Utmaningar med implementering

Omfattningen av det arbete som rederier utför i syfte att skydda sig mot cybersäkerhet varierar, där rederiets organisationsstruktur spelar en central roll. Det framgår av studiens resultat att beroende på om rederiet i fråga valt att outsourca delar av de traditionella funktionerna förknippat med rederiverksamheten till ett utomstående företag, speglar också kontrollen av arbetet förknippat med *Cyber Risk Management.* Studien visar att rederier som själva besitter ansvar för alla funktioner såsom crew-, technical- och operational management, definieras ansvariga personer tydligare. I

dessa fall är ansvariga personer inom rederiet ofta en befattning med syfte att säkerställa säkerhetsfrågor såsom DPA, CSO, superintendent eller QA Coordinator. Motsatsvis visar studiens resultat att rederier som valt att outsourca delar av rederifunktionerna till ett managementbolag eller IT-leverantör besitter sämre kontroll inom rederiet. I dessa fall ansvarar managementbolaget för utbildningar och dokument, medan IT-leverantör ansvarar för den tekniska aspekten. En viktig slutsats är att kontrollen av arbetet med *Cyber Risk Management* inte är densamma när ett rederi outsourcat delar av funktionerna. Dock visar resultatet från studien att flertal rederier upplevt det svårt att leva upp till de tekniska IT-kraven. Det framkom att rederierna upplevde det svårt på grund av att man ofta saknade rätt kompetens inom rederiet. Av den anledning anses det vara ett bra komplement att outsourca IT-arbete till ett utomstående företag med specialiserad kunskap för att vara säker på att rederiet besitter rätt skydd.

Tam och Jones (2019) konstaterar att det är den mänskliga faktorn tillsammans med IT- och OT-system som sammantaget förknippas som de tre största riskfaktorerna för den maritima industrin. Resultat i studien delar samma uppfattning som Tim och Jones (2019) där man anser att det största riskerna som existerar inom industrin idag är att en utomstående aktör genom en cyberattack betvinga OT i form framdrivning, eller i IT i form av ECDIS, att agera utom besättningens kontroll. Som tidigare nämnt anses det interna hotet i form av anställda vara en avsevärd riskfaktor inom sjöfartsindustrin. Psiaki et al. (2013) tillsammans med övriga forskare bevisade att sårbarheterna är ett faktum när det med hjälp av attackmetoden spoofing sände felaktiga GPS-signaler som styrde ett fartyg på felaktig kurs. I studien beskrev en respondent att det är just den här risken man vill eliminera genom ett väl strukturerat *Cyber Risk Management* arbete. En respondent i studien med specialiserad kunskap om IT-säkerhet förtydligade att uppdateringar av elektroniska sjökort ECDIS sker dagligen med USB-stickor där ett infekterat USB kan resultera i förödande konsekvenser. Av den anledning är ett viktig resultat i studien att uppdateringen av ECDIS är en av de främsta sårbarheterna, som än idag saknar en pålitlig lösning.

Studien tyder på att svenska rederier identifierade sårbarheter och risker med att bedriva rederiverksamhet. Utöver det tidigare nämnda sårbarheterna i form av anställda, IT- och OT system visar rederiernas riskanalyser på att de största sårbarheterna också är hijacking, virusmejl, servermiljö och telefoni. Studien indikerar på att rederier dagligen utsätts för virusmejl, vilket Ayala (2016) menar är en angreppsmetod som använder falska e-postmeddelande och webbplatser för att erhålla viktig information. Informationen används i sin tur i syfte att kräva offret på en lösensumma. Studiens resultat indikerar att flertal rederier fallit offer för attackmetoden. Tillika vittnar respondenterna om händelser där rederier fallit offer för attackmetoden ransomware. Ayala (2016) definierar ransomware som en skadlig kod vilket begränsar offrets åtkomst till aktuellt system. Vad som kännetecknar händelserna hos rederierna är önskan på lösensumma för att låsa upp systemet.

IMO (2017a.) beskriver att rederiers arbete med cybersäkerhet bör inkludera aktiviteter eller åtgärder som syftar till att i god tid upptäcka cyberattacker. Studiens resultat visar att svenska tankrederier arbetar med aktiviteter och åtgärder för att uppfylla detta. En central aktivitet för alla rederier innefattar utbildningar, som avser att öka medvetenhet och kunskapen hos rederiernas personal. Med hjälp av dessa utbildningar vet anställda iland såväl som besättning ombord hur de

ska agera i angivna situationer samt bli mer uppmärksamma, kritiska och reflektera över deras beslut framför skärmen. Flera gemensamma aktiviteter som nämns är av den enklare nivån som krav på lösenordshantering samt att logga ur program och system efter användning, kan upplevas som väl simpla saker men bevisligen effektiva aktiviteter. OCIMF (2019) menar att rederier bör besitta en IT policy som i sin tur främjas och förmedlas till anställda. Resultatet indikerar på att rederier tagit detta i åtanke och mot bakgrunden av OCIMF och IMO har rederiet konstruerat en väl formulerad IT policy. IT policyn ses som en central aktivitet i rederiets arbete mot cyberattacker, där varje anställd bekräftar med en underskrift att de har tagit del och förstått informationen om hur man förhåller sig till företagets IT- och OT-system. Tillika beskriver OCIMF genom sina SIRE inspektioner att rederier bör implementera regler för hur personliga kommunikationsmedel får användas ombord. Respondenter menar att svenska tankrederier tillåter användning av personliga kommunikationsmedel, men för att dessa inte ska påverka fartygets IT system så har majoriteten av rederier delat nätverk. Detta innebär att man besitter ett nätverk för nöje och ett separat för affärs ändliga ändamål. Denna aktivitet tyder på viljan om att fartyget inte ska påverkas av anställdas misstag.

En viktig slutsats i studien är vikten av en bra beredskapsplan. Planen fungerar för rederiets anställda iland såväl som besättningen ombord fartygen. Planen innehåller tillvägagångssätt vid händelse av en attack. IMO (2017a) rekommenderar med hjälp av resolution, MCS-FAL.1/Circ.3, att rederier bör implementera en beredskapsplan men uttrycker inga tydligare rekommendationer. Enligt studien är den centrala beredskapsplanen att ringa IT-leverantören alternativ IT-företag för att erhålla hjälp. Ytterligare visar studien att rederier besitter en beredskapsplan vilket innefattar att man bör identifiera omfattning av attacken där man är intresserad av att veta när, var och hur attacken genomfördes. Nästa steg är att fastställa om något system ligger nere och i sådana fall vikten av det systemet för att fortsätta bedriva verksamheten. Den centrala uppfattningen är att med hjälp av att rederiet kontinuerligt sparar säkerhetskopior av nödvändiga system kan dessa fungera som lösning till en attack. Återställer rederiet berörda systemet till en kopia innan attacken eliminerar man risken att viruset finns. Om man identifierat andra orsaker till nedläggning av system såsom ett USB minne så klipps detta på mitten för att eliminera risken av att detta används av misstag igen. Sammantaget visar resultatet att det är viktigt att rederier säkerhetskopierar regelbundet på grund utav att vid en attack så återställer man till nyast utförda kopia, är den för gammal riskerar rederiet att gå miste om mycket arbete.

6.1.3 Analys av nivå

IMO (2017b) beskriver att *Cyber Risk Management* ska inkluderas i rederiers existerande SMS kod vid första verifieringen av DoC den 1 januari 2021. Sammantaget visar resultatet på att rederier inte upplever det svårt att leva upp till kriterierna från IMO gällande *Cyber Risk Management*. Emellertid beskriver respondenterna att kravet är vagt och tillåter mycket egen tolkning av rederierna själva. Respondenten menar att det inte finns tydliga kriterier som tydliggör hur mycket rederierna bör arbeta för att förhindra hoten. Respondenten beskriver att IMO kräver att man ska identifiera hoten men uttrycker inte i skriftlig form något krav på hur mycket rederierna bör arbete för eliminera dessa. Detta kan i sin tur innebära att rederier endast behöver skriftligt dokumentera att man identifierat hoten, men uttrycker inte vidare vilka åtgärder man tagit för att eliminera hoten. Resultatet visar också att framtiden inte innebär striktare regler från IMO sida, dock visar resultatet

på att framtiden innebär tydligare krav där IMO förtydligar existerande krav med hjälp av bättre formulering. Detta kan i sin tur upplevas som striktare ansvar för vissa rederier som inte valt att lägga ner tillräckliga resurser vid den första verifieringen av DoC.

Resultat visar att tanknäringen är förberedd på det nya lagkravet från IMO på grund utav att rederierna tidigare stött på liknande krav. Oruc (2019) beskriver att de stora oljebolagen krävde redan 2018 att tankrederier ska ta hänsyn till cybersäkerhet i rederiets säkerhetsorganisation arbete. Resultatet i studien sammankopplar till Oruc (2019) resonemang och beskriver att tankrederier länge arbetat med krav på att man bör besitta en policy för cybersäkerhet, tillika öka medvetenheten hos besättning om det risker som förknippas med att bedriva ett fartyg. Sammantaget visar studien på att det finns redan en grundläggande nivå av arbete hos svenska tankrederier.

Vad som kännetecknar resultatet är att man bäst skyddar sig för hotet genom att öka medvetenheten inom organisationen. Mot bakgrunden av att det största hotet är internt styrker resultatet att utbildningar och ökad kunskap är bra för att inte göra misstag. Resultat visar också att förstå *Cyber Risk Management* helhetsperspektivet är viktigt, där rederier inte bör fokusera 100% på ett område utan bör lägga arbetet inom organisationen på en rimlig nivå. Respondenter menar att med hänsyn till att verksamheten kontinuerligt utför riskanalyser för att identifiera nya hot uppmärksammar rederiet själva vad fortsatt arbetsbelastning bör läggas.

Studien synliggör att svenska tankrederier är väl förberedda för det kommande lagkravet. Det finns en grundläggande nivå där samtliga respondenter uttrycker sig bekväma för att den 1 januari 2021 verifiera sitt arbete med *Cyber Risk management.* Vad som kännetecknar alla respondenter är övertygelsen om att de besitter en nivå utöver vad lagstiftningen kräver, där alla delar uppfattning om att svenska tankrederier alltid ligger i framkant vad gäller efterlevnad till lagkrav.

6.2 Metoddiskussion

Vi som uppsatsförfattarna har innan, under och efter arbetsprocessen analyserat vald metodologi noggrant. Vår ambition under arbetsprocessen har varit att med hjälp av en högkvalitativ metod presentera resultat som anses innehålla hög trovärdighet och giltighet. Det huvudsakliga syftet med studien var att analysera om svenska tankrederier är förberedda inför det kommande regelverket utformat av IMO gällande *Cyber Risk management*. Utifrån det huvudsakliga syftet med studien ansåg vi att det fanns mening att välja en metod med grunden i kvalitativ datainsamling. Av den anledning användes fallstudie, eftersom metoden tillåtit oss att på djupet undersöka ett specifikt ämne mer detaljrikt, där det inte bara är intressant att analysera *vad* svenska tankrederierna gör utan också *varför* de arbetar med frågan så som de faktiskt gör (Denscombe 2014). Bell (2017) menar att tillåta respondenterna tala fritt under intervjuer kan anses vara till nackdel då svaren kan variera i både mängd och kvalitet. Dock visade sig medverkande respondenter erhålla goda kunskaper och erfarenheter inom ämnet och insamlad data ansågs därav vara tillräcklig till att besvara studiens forskningsfrågor. Vi har varit väl medvetna om den kritik som riktas mot intervjuer eftersom Bell (2015) beskriver att intervjuer innebär en stor tidsomfattning, där man under kortare projekt endast finner utrymme till att utföra ett fåtal. Tillika kan intervjuaren i vissa fall vara en svaghet, där författarnas svaghet består av dess begränsad erfarenhet utav att utföra intervjuer (Bell, 2017).

Detta var något vi hade i åtanke innan utförandet och något som vi förberedda oss noggrant för att hantera.

Vi uppmärksammade fallstudie tillåter ett brett urval av metoder för datainsamling. Bell (2015) menar att datainsamling kan ske med hjälp av observationer, enkäter, intervjuer eller med fler olika metoder. Vi som uppsattsförfattare såg anledning att använda oss av semi-strukturerade intervjuer eftersom metoden tillåter följdfrågor för att erhålla en mer rik datainsamling. Att använda intervju som forskningsverktyg har också sina stora fördelar i och med sin flexibilitet, där Bell (2015) menar att intervjuare utefter sin förmåga har möjlighet att ställa följdfrågor för att följa upp idéer, sondera svar samt fånga känslor och uttryck hos respondenten (Bell, 2015).

Urval och målgrupp till intervjuerna representerades av svenska rederier med fokus på transport av flytande bulk, med andra ord tankrederier. Inklusionskriterierna var anställda med ansvar eller specialiserad kunskap inom cybersäkerhet. Det kom att visa sig att det var svårt att rekrytera respondenter till intervjun. Vi skickade ut en förfrågan till samtliga rederier inom Västra Götalandsregionen, men svar erhölls endast från tre av dessa. Vad gäller utomstående företag valdes på förhand en IT-leverantör som arbetar med cybersäkerhet dagligen.

Vi upplevde att vissa respondenter under intervjuerna kände sig något hämmade i sina svar på grund av att de spelades in. Detta blir ibland oundvikligt menar Denscombe (2014) men vi försökte eliminera risken genom att använda god forskningsetik och belysa anonymiteten under studien, för att eventuella svar inte ska påverka respondentens efterhand.

Nu i efterhand har vi som uppsatsförfattare reflekterat kring om studien eventuellt hade kunnat förbättras genom en enkätundersökning, som då skulle kunna komplettera intervjuerna. I och med omständigheterna med COVID-19 var de relativt få rederier som tackade ja till intervju eftersom det är brist på personal på grund av permitteringar. En enkätstudie skulle vara mindre tidskrävande vilket hade kunnat bidra till att fler rederier medverkade.

Efter att information insamlats med hjälp av en kvalitativ datainsamling i form av semi-strukturerade intervjuer fanns ett antal sätt för att analysera insamlad data. Uppsatsförfattarna såg anledning till att använda Granheim och Lundmans (2004) femstegsmodell för innehållsanalys. Beroende på hur författarna uppfattar materialet tolkar de ett antal kategorier som kan bidra till resultatet och svara på forskningsfrågor. Hänsyn bör tas till att tolkningen och benämningen av kategorier kan variera mellan forskare och därav finns det möjlighet att samma data tolkas olika vilket också reflekterar slutresultatet. Vad gäller reliabilitet så nämner Bell (2017) att begreppet har att göra med om studiens tillvägagångssätt presenterar samma resultat trots att den utförs vid annan tidpunkt eller undersökare. Vi tycker att det är svårt att mäta reliabilitet vid kvalitativa intervjuer och menar därmed att resultatet kan variera med hänsyn till aktuell lagstiftning om cybersäkerhet. Av den anledning är det viktigt att fånga det som förmedlas vid det aktuella tillfället så att undersökningen speglar rådande situation. Vad gäller validitet menar Bell (2017) att begreppet handlar om hur väl resultatet besvarar önskad fråga. Av den anledning har vi som författare varit noggranna med att förklara hur resultat erhållits samt hur detta resultat analyserats under studiens gång. Detta resonemang stärks av Walsham (1995) som menar att en studie med

fokus på kvalitativ datainsamling syftar till att tolka andras förklaringar, vilket i sin tur bidrar till en mer detaljerad beskrivning av studiens arbetsprocess. Walsham (1995) menar av den anledning att det viktigt att tydligt visa tillvägagångssätt för att studien ska besitta hög validitet.

6.3 Förslag till vidare forskning

Den här studien är avgränsad till att undersöka hur förberedd svensk tanknäring är för det kommande lagkravet med kraft från 1 januari 2021. Vi upplever att cybersäkerhet är ett relativt nytt och outforskat ämne. Av den anledning ser vi mening i att applicera studiens forskningsfrågor på andra segment inom den maritima industrin, såsom kryssning, torrlast, bil och rullande lastindustrin. Med hjälp av ett bredare perspektiv skapas en uppfattning om hur hela den maritima industrin ser på det kommande lagkravet. Tillika kan en vidare forskning analysera de olika industri segmenten sinsemellan, där en analys resulterar i en utvärdering om det finns olika bakomliggande faktorer som påverkar hur väl industrin väljer att applicera ämnet i sitt dagliga arbete. Vi ser också mening för kommande forskning att utvärdera hur försäkringsbolag ser på ämnet. Eftersom studien visar på en ökning av ämnets risknivå för varje år, ger det anledning till att tro att den finns en tilltagande oro eftersom att försäkra fartyget grundar sig i tanken om att förflytta risken från fartygsägaren till försäkringsbolaget.

7 Slutsatser

Syftet med den här studien är att besvara forskningsfrågan "Hur redo är svenska tankrederier inför de nya riktlinjer och krav som ställs från IMO 2021?". Mot bakgrunden av studien resultat redogörs en genomgående positiv inställning till IMO 2021 - *Cyber Risk Management*. Detta innebär att samtliga rederier som medverkat till studien upplever att de klarar av kraven. Vidare så indikerar resultatet att rederiernas arbete är på en nivå utöver vad lagstiftning kräver. I detta sammanhang anser rederierna det vara en konkurrensfördel att besitta ett pålitligt datasystem som aldrig slutar fungera. Vad gäller attityden mot det nya lagkravet visar resultatet att lagkravet ses som ett verktyg som används för att effektivisera rederiernas arbete med datasäkerhet. Resultatet indikerar emellertid att kunskapen och erfarenheten kan variera mellan rederier. Storlek anses vara en avgörande faktor men tillika om rederiet besitter ansvar för traditionella funktioner såsom crew-, technical- och operational management spelar en central roll. Dock visar resultat att samtliga rederier upplever det svårt att leva upp till de tekniska IT-kraven, samtliga respondenter delar uppfattning om att en utomstående IT-leverantör anses vara ett bra komplement.

Vad gäller hot utmärker sig tre väsentliga begrepp: människan, IT- och OT-system. Det första begreppet, människan, avser en anställd som av misstag orsakar en cyberattack vilket resulterar i tidsmässiga och ekonomiska konsekvenser för rederiet. Det andra begreppet, IT-system, avser hot riktat mot fartygets navigation och kommunikation. Lika viktigt är det sista begreppet, OT, som avser system förknippade med fartygets framdrivning och lasthantering. En viktig slutsats är att flertal intrång hos rederier orsakas av att en anställd av misstag tryck på fel webbplats eller länk. Tillika är en viktig slutsats att det inte är informationen inom sjöfarten i sig som intresserar en utomstående aktör, utan att attackerna förknippas som oriktade.

En fundamental slutsats i studien är att ett helhetsperspektiv är den bästa lösningen till att bemöta det stigande hotet, cybersäkerhet, samt det nya lagkravet *Cyber Risk Management*. Helhetsperspektivet innebär att rederier bör öka medvetenhet och kunskap inom ämnet, där utbildningar och diskussionsmöten för anställda fungerar som ett bra supplement. Vidare indikerar resultatet att rederierna inte bör fokusera endast på dokumentation och riskera att sakna tekniskt försvar. Att besitta en grundläggande nivå inom samtliga delar anses vara fundamentalt för att bemöta hotet, såväl som kraven. Med hjälp av kontinuerliga riskanalyser uppmärksammar rederier själva vad som kännetecknar sårbarheter inom deras verksamhet. Resultatet pekar på att rederiernas fas till automatisering och digitalisering är en avgörande faktor på hur utsatta just deras verksamhet är.

Utifrån studiens resultat, baserat på medverkande företag, visas en god attityd och kompetens mot det kommande lagkravet. Medverkande företag delar uppfattning om att svenska tankrederier står på en bra grund för att möta det kommande lagkravet. Studiens resultat visar att rederierna arbetat proaktivt med IMO:s kommande lagkrav. Arbetet härstammar från de stora oljebolagen, som 2018 krävde ansvar för cybersäkerhet i form av SIRE- och TMSA inspektioner. Resultatet indikerar att framtida krav troligtvis inte kommer vara strängare, däremot tydligare. För de rederier som inte står på en bra grund inom samtliga delar kan tydligare krav upplevas striktare.

8 Referenser

A.P. Möller - Maersk A/S. (2017a). *Annual Report.* Hämtat från Maersk: https://investor.maersk.com/static-files/250c3398-7850-4c00-8afe-4dbd874e2a85

A.P. Möller - Maersk A/S. (den 28 Juni 2017b). *Cyber attack update.* Hämtat från Maersk: https://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

Allianz. (Januari 2020). *Allianz Risk Barometer.* Hämtat från Allianz: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Ayala, L. (2016). *Cybersecurity Lexikon.* New York: Apress.

Bell, J. (2015). *Introduktion till forskningsmetodik.* Lund: Studentlitteratur AB.

Bennett, N., & Miles, S. A. (Maj 2006). *Second in Command: The Misunderstood Role of the Chief Operating Offier.* Hämtat från Harvard Business Review: https://hbr.org/2006/05/second-in-command-the-misunderstood-role-of-the-chief-operating-officer

Bryman, A., & Bell, E. (2012). *Företagsekonomiska forskningsmetoder.* Stockholm: Liber.

Calder, A., & Watkins, S. (2015). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002.* London: Kogan Page.

Chernov, D., & Sornette, D. (2019). *Critical Risks of Different Economic Sectors: Based on the Analysis of More Than 500 Incidents, Accidents and Disasters.* Hämtat från https://link-springer-com.proxy.lib.chalmers.se/book/10.1007%2F978-3-030-25034-8

Denscombe, M. (2014). *The good research guide: for small scale research projects.* Hämtat från: http://eds.b.ebscohost.com/eds/detail/detail?vid=0&sid=0096390a-aee8-4166-8e45-7ac18edeef38%40pdc-v-sessmgr05&bdata=JkF1dGhUeXBlPXNzbyZzaXRlPWVkcy1saXZlJnNjb3BlPXNpdGU%3d#AN=clec.DAW29300840&db=cat07472a

Deutsche Flagge. (u.d.). *Safety management (ISM)*. Hämtat från Deutsche Flagge: https://www.deutsche-flagge.de/en/safety-and-security/ism/documents-and-certifications

DiRenzo, J., Goward, D. A., & Roberts, F. S. (2015). The Little-known Challenge of Maritime Cyber Security. *2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA),* 2015, Corfu. doi: 10.1109/IISA.2015.7388071

European Data Protection Supervisor. (u.d.). *Data Protection Officer (DPO)*. Hämtat från European Data Protection Supervisor: https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

Fielding, J. A. (2019). *Rethinking CRAAP: Getting students thinking like fact-checkers in evaluating web sources.* Hämtat från https://crln.acrl.org/index.php/crlnews/article/view/24195

Fransen, F., Kerkdijk, R., & el Quajdi, N. (Juni 2019). *Security at Machine Speed.* Hämtat från TNO: https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/trusted-ict/cybersecurity/

Gard. (den 10 July 2019). *Ship operators cannot afford to turn a blind eye to cyber security*. Hämtat från Gard: http://www.gard.no/web/updates/content/27958640/ship-operators-cannot-afford-to-turn-a-blind-eye-to-cyber-security

Gartner. (u.d.). *Gartner Glossary: Digitalization*. Hämtat från Gartner: https://www.gartner.com/en/information-technology/glossary/digitalization

Ihre, R. (2016). Managementuppdrag. i R. Ihre, *Kommersiella Sjöfartavtal* (ss. 223-224). Stockholm: Jure Förlag AB.

Ihre, R. (2016). Rederiets Landorganisation. i R. Ihre, *Kommersiella Sjöfartsavtal* (s. 63). Stockholm: Jure Förlag AB.

IMO. (den 25 Maj 2016). *Maritime Safety Committee (MSC), 96th session, 11-20 May 2016*. Hämtat från http://www.imo.org/en/MediaCentre/MeetingSummaries/MSC/Pages/MSC-96th-session.aspx

IMO. (den 5 Juli 2017a). *Guidelines on Maritime Cyber Risk Management.* Hämtat från http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

IMO. (den 16 Juni 2017b). *Maritime Safety Committee (MSC), 98th session, 7-16 June 2017*. Hämtat från http://www.imo.org/en/MediaCentre/MeetingSummaries/MSC/Pages/MSC-98th-session.aspx

IMO. (u.d.a). *International Convention for the Safety of Life at Sea (SOLAS), 1974*. Hämtat från http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

IMO. (u.d.b). *Introduction to IMO*. Hämtat från http://www.imo.org/en/About/Pages/Default.aspx

IMO. (u.d.c). *ISM Code and Guidelines on Implementation of the ISM Code*. Hämtat från http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx

IMO. (u.d.d). *Maritime cyber risk*. Hämtat från http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx

IMO. (u.d.e). *SOLAS XI-2 and the ISPS Code*. Hämtat från International Maritime Organisation: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

IMO. (u.d.f). *IMO what it is.* Hämtad från http://www.imo.org/en/About/Documents/What%20it%20is%20Oct%202013_Web.pdf

Lexico. (u.d.a). *Cyberattack*. Hämtat från Lexico: https://www.lexico.com/definition/cyberattack

Lexico. (u.d.b). *Hacker*. Hämtat från Lexico: https://www.lexico.com/definition/hacker

Munich RE. (u.d.). *Cyber Risks: Cyber threats are one of the biggest security risks of the 21st century*. Hämtat från Munich RE: https://www.munichre.com/en/risks/cyber-risks.html

OCIMF. (den 22 Febuari 2019). *Ship Inspection Report (SIRE) Programme: Vessel Inspection Questionnaires for Oil Tankers, Combination Carriers, Shuttle Tankers, Chemical Tankers and Gas Tankers, Seventh Edition (VIQ 7).* Hämtat från Oil Companies International Marine Forum: https://www.ocimf.org/media/127546/SIRE-Vessel-Inspection-Questionnaire-VIQ-Ver-7007.pdf

Oruc, A. (2019). Tanker Industry is More Ready against Cyber Threats. *International Conference on Marine Engineering and Technology.* 2019, Oman. doi: 10.24868/icmet.oman.2019.030

Psiaki, M. L., O'Hanlon, B. W., Powell, S. P., Bhatti, J. A., Wesson, K. D., Humphreys, T. E., & Schofield, A. (2014). *GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase.* Hämtat från https://repositories.lib.utexas.edu/bitstream/handle/2152/63214/Psiaki_WROD_2014.pdf?sequence=2&isAllowed=y

Smith, M. D. (November 2017). *Arming students against bad information.* Hämtat från https://journals-sagepub-com.proxy.lib.chalmers.se/doi/pdf/10.1177/0031721717739595

Svensk Sjöfart. (u.d.). *Våra medlemmar*. Hämtat från Svensk Sjöfart: http://www.sweship.se/medlemskap/vara-medlemmar/

Svenska Institutet för Standarder. (u.d.). *Detta är ISO 27000*. Hämtat från Svenska Institutet flr Standarder: https://www.sis.se/iso27000/dettariso27000/

Tam, K., & Jones, K. (2019). Factors Affecting Cyber Risk in Maritime. *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 2019, Oxford, ss. 1-8. doi: 10.1109/CyberSA.2019.8899382

The University of Texas at Austin. (den 29 Juli 2013). *UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea*. Hämtat från The University of Texas at Austin: https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

Tiberg, H., Schelin, J., & Widlund, M. (2015). Säkerhetsorganisation. i H. Tiberg, J. Schelin, & M. Widlund, *Praktisk sjörätt* (ss. 81-82). Stockholm: Jure Förlag AB.

Tiberg, H., Schelin, J., & Widlund, M. (2015). SOLAS-konventionen. i H. Tiberg, J. Schelin, & M. Widlund, *Praktisk sjörätt* (ss. 63-64). Stockholm: Jure Förlag AB.

Transportstyrelsen. (2020). *Aktuell information*. Hämtat från Transportstyrelsen: https://transportstyrelsen.se/sv/sjofart/Fartyg/sjosakerhetsarbete/aktuell-information/

Transportstyrelsen. (2020). *Sjösäkerhetsarbete*. Hämtat från Transportstyrelsen: https://transportstyrelsen.se/sv/sjofart/Fartyg/sjosakerhetsarbete/

United Nations. (den 22 September 2016). *Maritime Transport Is 'Backbone of Global Trade and the Global Economy', Says Secretary-General in Message for International Day*. Hämtat från United Nations: https://www.un.org/press/en/2016/sgsm18129.doc.htm

Walshamn, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, *4*(2), ss. 74-81. doi: 10.1057/ejis.1995

9 Bilagor

9.1 Bilaga 1 – Resultattabell mot resolution *MSC-FAL.1/Circ.3*

Riktlinjer - *MCS-FAL.1/Circ.3.*		**Kategori** *(Steg 5)*	**Subkategori** *(Steg 4)*
Identify	*Definiera ansvariga personer*	- Outsourcat ansvar - Inhouse ansvar	Outsourcat ansvar: - Managementbolag - IT-Leverantör - IT-företag Inhouse ansvar: - Technical Manager - HSE Manager - DPA - CSO - Superintendent - QA Department
	Identifiera sårbarheter	- Hijacking - Beroende av datasystem - Virusmejl *(Phishing)* - Konkurrenter - Ransomware - IT- och OT-system	- Hijacking, där utövarna benämns de nya piraterna - Mycket arbete bygger på olika datasystem - Virusmejl skickas till anställda *(Phishing)* - Konkurrenter som kan följa verksamheten - Ransomware som fryser system - Server, mejl och telefoni samt automations-, drift-, lastsystem
Protect	*Implementera rutiner för riskkontroll- och åtgärdsprocessen*	- Brandväggar - Förbjud av USB - Kontroll av servicepartners - Speciella skrivare - USB lås	Riskkontrollsrutiner: - Brandväggar - Förhindrande av USB användande - Underhållsarbete kontrolleras på förhand - Speciella skrivare - USB lås
	Implementera beredskapsplan	- Backup emergency plan	- Backup emergency plan återställer nödvändiga system
Detect	*Aktiviteter med syfte att i god tid upptäcka en cyberincident*	- Egenkontroll och ansvar - Table top drills - Utbildningar	- Individuell egenkontroll och ansvar - Table top drills ökar kunskap och medvetenhet

		- Antivirusprogram och filterprogram	- Utbildningar för land- och ombordpersonal - Antivirusprogram och filterprogram för mejl
Respond	*En responsplan för motståndskraft samt aktiviteter för att kunna återställa system*	- Ringa IT-leverantör - Checklist	- Responsplan är att ringa IT-leverantör - Checklista på vem som ska göra vad och vad som ska göras
Recover	*Utföra säkerhetskopiering av nödvändiga system*	- Utförs av IT-leverantör - Utförs av IT-företag	- IT- leverantören utför säkerhetskopiering - IT-företag utför säkerhetskopiering flera gånger per dygn

9.2 Bilaga 2 – Resultattabell mot frågeställning

Studiens frågeställningar	**Intervjufrågor**	**Kategori** *(Steg 5)*	**Subkategori** *(Steg 4)*
Nulägesbeskrivning av existerande kunskap och erfarenhet inom ämnet	*Vad är cyber security?*	- Säkerställa olaga intrång - Skydda lösenord - Lösenordshantering - Säkerhet	- Ingen får ta sig in i rederiets system och förstöra - Mestadels de enklare tankesättet såsom skydda lösenord - Mer avancerade lösenord - Populistiskt ord för säkerhet
	När påträffade du begreppet "Cyber Security" för första gången, var det privat eller företagsrelaterat sammanhang?	- Företagsrelaterat - Privat relaterat	- Företagsrelaterat kontor - Företagsrelaterat som ombordanställd - Privat relaterat, upplever att den yngre generationen är medvetna
	Vilka risker eller hot ser du inom området?	- Verksamheten kan inte bedrivas - Missar last - Ökad oro för människoliv - Ekonomiska konsekvenser - Ser inte så mycket hot	- Verksamheten bygger på program och system som är är verksamma online - Missar last på grund utav att fartyg inte får nödvändig information - Ekonomiska konsekvenser - Osäkerhet för människoliv - Efter riskutvärdering tillsammans med IT-företag, finns egentligen inte så mycket hot
	I vilken utsträckning tror du att ni som företag kan bli utsatta?	- Utsatta dagligen - Kan bli utsatta - Låg risk - Inga direkt riktade attacker	- Så länge man använder internet eller uppkoppling existerar hotet - Kan bli utsatta, där lösningar finns men tar tid - Låg risk, baserat på anonymitet i jämförelse till större rederier

			- Inga riktade attacker mot rederier
	Har ni som företag någon gång blivit utsatta för dataintrång eller liknande attack?	- Utsatt för Phishing	- Anställda har öppnat mejl som slår ut hela IT-systemet - Anställda ombord har öppnat mejl som slog ut fartygets IT-system
	Upplever ni på ... att cyber attacks är ett verkligt hot mot er verksamhet?	- Dagligt hot - Finns andra hot	- Dagliga phishing försök - Blir dagligen utsatta av intrång - Finns andra hot som känns mer relevanta idag
Utmaningar med implementering av resolutioner och riktlinjer	*Vem eller vilka inom er organisation har ansvar för arbetet med Cyber Risk Management?*	- Outsourcat ansvar - Inhouse ansvar	Outsourcat ansvar: - Managementbolag - IT-Leverantör - IT-företag Inhouse ansvar: - Technical Manager - HSE Manager - DPA - CSO - Superintendent - QA Department - Quality Controller
	Vilka sårbarheter har ni identifierat med att bedriva rederiverksamhet? (Fokus på tillgång och data)	- Utpressning av lösensumma - Nedstängning av system - Konkurrent får inblick i rederiet - IT- och OT-system	- Utpressning av lösensumma för nedstängda system - Vi har inget värde i det som förmedlas mellan kontor och fartyg. Däremot om en konkurrent får insikt i rederiets dagliga arbete - Server, mejl och telefoni samt automations-, drift-, lastsystem
	Har ni några rutiner för riskkontroll- och åtgärdsprocessen vid en händelse av till exempel cyber incident?	- Det måste man ha - Isolera utsatt system - Lösenordshantering	- Det finns ett antal nivåer av rutiner - Isolera utsatt system för att minimera spridning - Periodvis byte av lösenord samt hur säkra lösenorden är med antal

			och typer av tecken
	Har ni en beredskapsplanering, så att ni kan fortsätta bedriva er verksamheten trots IT-intrång? (fartygen och rederi)	- Kontakta IT-företag eller CSO - Kontakta IT-leverantör	- Kontakta IT-företag eller CSO, dem utvärdera situationen - IT-leverantör tillhandahåller en back up plan som återställer berörda system
	Vilka aktiviteter eller åtgärder har ni för att i god tid upptäcka en cyber incident?	- Spamfilter - Brandväggar - Utbildningar - Ökad - Medvetenhet, IT-program och brandväggar - Table top drills	- Spamfilter som sorterar eventuella riskfyllda mejl - Brandväggar - Förbjud av USB stickor samt USB lås - Utbildningar som fokuserar på att höja personalens kunskap och medvetenhet inom Cyber Risk Management - Utbildningar för att öka medvetenheten, antivirusprogram och spamfilter - Table top drills möten mellan anställda för att öka kunskap och erfarenhet
	Har ni en responsplan som kan försvara vid en cyber incident?	- Checklista - Kontakta IT-leverantör	- Checklista på vem som ska göra vad och vad som ska göras - Responsplan är att kontakta IT-leverantör
	Utför ni någon form av säkerhetskopiering av verksamhetens data och nödvändiga system för att kunna återställa dom vid ett intrång?	- IT-företaget utför säkerhetskopiering - IT-leverantör	- IT-företaget utför säkerhetskopiering flera gånger per dygn - IT-leverantör utför säkerhetskopiering
	Har ni upplevt det svårt att implementera cyber riskhantering?	- Ingen större utmaning	- Det har blivit en vardag med alla olika krav från organisationer och oljebolag - De flesta inom verksamheten har

			förståelse för arbete med cybersäkerhet - Outsourcat till IT-leverantör
Analys av nivå	*Baserat på den erfarenhet du har, hur tror du att man bäst skyddar sig för ett dataintrång?*	- Medvetenhet - Medvetenhet, kunskap och teknik - Utbildningar - Expertkompetens inom IT - Helhetsperspektiv	- Det finns bra och säkra system men att systemet aldrig blir bättre än personen som brukar systemen - En blandning av medvetenhet, kunskap och teknik från IT-leverantör - Ökad kunskap genom utbildningar - Expertkompetens inom IT genom outsourcing till IT-leverantör - Helhetsperspektiv, lagom nivå på samtliga delar
	Upplever du cyberhotet unikt för sjöfarten? Om inte, tycker du att liknande lagkrav om cyber riskhantering borde implementeras inom andra industrier?	- Mer specifikt för sjöfarten - Inte unikt för sjöfarten	- Mer specifikt jämfört med andra industrier - Alla verksamheter som använder datorer och kommunikation ställs inför samma cyberhot - Risken aktuell inom andra industrier
	Utifrån dina svar, upplever du att ... arbete med cybersäkerhet omfattar mer än vad lagstiftningen kräver eller skulle du säga att företaget enbart uppfyller kriterierna.	- Omfattar mer än lagkraven	- Omfattar mer än kommande lagkraven kräver, på grund av tidigare krav - En stark känsla att rederiet arbetar utöver vad lagstiftningen kräver

9.3 Bilaga 3 - Intervjuguide till respondenter

Intervjufrågor - Cyber Risk Management

Företagsnamn:
Respondent:
Befattning:
(Företagsnamn och respondent hålls anonyma i rapporten)

Introduktion (Inspelning påbörjas)
Vi vill börja med att fråga om det är okej att vi spelar in ljudet på intervjun? Direkt när materialet är transkriberat raderas ljudfilen. Vi kommer exkludera respondentnamn (alltså ditt namn) men inkludera rollbeskrivning i uppsatsen - godkänner du det här?

Vi tänkte kort berätta om upplägget. Inledningsvis kommer vi ställa mer allmänna frågor för att senare fokusera på IMO:s riktlinjer. Vi avslutar med lite sammanfattande frågor av det vi diskuterat. Om det är något du inte förstår så är det bara att säga till. Då tänkte jag lämna över till William som har några inledande frågor.

Nulägesbeskrivning

1. Vad innebär begreppet *Cyber Security* för dig?
2. När påträffade du begreppet *Cyber Security* för första gången, var det privat eller företagsrelaterat sammanhang?
3. Vilka risker eller hot ser du inom området?
4. I vilken utsträckning tror du att ni som företag kan bli utsatta?
5. Har ni som rederi någon gång blivit utsatta för dataintrång eller liknande attack?
6. Upplever ni som rederi att cyberattacks är ett verkligt hot mot er verksamhet?

Utmaningar med implementering av resolutioner såsom MSC. 428 (98) och MSC-FAL.1/Circ.3.

1. Vem eller vilka inom er organisation har ansvar för arbetet med *Cyber Risk Management*?
2. Vilka sårbarheter har ni identifierat med att bedriva rederiverksamhet? (Fokus på tillgång och data)
3. Har ni några rutiner för riskkontroll- och åtgärdsprocessen vid en händelse av till exempel cyberincident?
   Följdfråga, kan ni ge exempel på rutin som är på plats?
4. Har ni en beredskapsplanering, så att ni kan fortsätta bedriva er verksamheten trots IT-intrång? (fartygen och rederi)
5. Vilka aktiviteter eller åtgärder har ni för att i god tid upptäcka en cyberincident?
6. Har ni en responsplan som kan försvara vid en cyberincident?
   (Denna skiljer sig från beredskapsplanering eftersom det är en plan för när ett intrång faktiskt har skett och inte bara förberedelser).

7. Utför ni någon form av säkerhetskopiering av verksamhetens data och nödvändiga system för att kunna återställa dom vid ett intrång?
   Följdfråga, vilka system säkerhetskopierar ni och hur ofta?

Analys av vilken nivå företaget arbetar utefter

1. Har ni upplevt det svårt att implementera cyber riskhantering?
2. Baserat på den erfarenhet du har, hur tror du att man bäst skyddar sig för ett dataintrång?
3. Upplever du cyberhotet unikt för sjöfarten? Om inte, tycker du att liknande lagkrav om cyber riskhantering borde implementeras inom andra industrier?
4. Utifrån dina svar, upplever du att erat arbete med cybersäkerhet omfattar mer än vad lagstiftningen kräver eller skulle du säga att företaget enbart uppfyller kriterierna.