Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk

Arnt Holm Rennan

MARITIM CYBER RISIKOSTYRING I SIKKERHETSSTYRINGSSYSTEMER

Masteroppgave i maritim operativ ledelse
Veileder: Marie Hauglie-Sandvik
Mai 2023

NTNU
Kunnskap for en bedre verden

Arnt Holm Rennan

MARITIM CYBER RISIKOSTYRING I SIKKERHETSSTYRINGSSYSTEMER

Masteroppgave i maritim operativ ledelse
Veileder: Marie Hauglie-Sandvik
Mai 2023

Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk

NTNU
Kunnskap for en bedre verden

FORORD

Denne masteroppgaven er avslutningen på mastergraden ledelse av maritime operasjoner ved NTNU i Ålesund. Gjennomføringen av oppgaven har satt studiets ulike emner i en kontekst og denne blir trolig ikke mindre aktuell i årene som kommer. Jeg vil takke de rederiansatte som har stilt sin tid til min disposisjon og delt erfaringer og opplevelser. Uten dem hadde det ikke blitt noen oppgave. Samtidig må jeg få rette en stor takk til min veileder Marie Haugli-Sandvik for gode råd og konstruktive tilbakemeldinger.

En stor takk til Gry og resten av familien for støtte og for at dere har latt meg bruke av vår felles tid. Til slutt vil jeg takke Espen Erstad og Bjørn Inge Furuli for innspill og delte betraktninger i oppstartsfasen av dette studiet.

Arnt Holm Rennan

SAMMENDRAG

Bakgrunn: Rederiene er pålagt av IMO å gjennomføre cyber risikovurderinger og inkludere disse i sine sikkerhetsstyringssystemer fra første revisjon etter 1.januar 2021.

Formål: Formålet med dette studiet er å komme til kunnskap om hvordan rederiene håndterer IMO`s krav til gjennomføring av cyber risikovurderinger, hvem som er involvert og hvordan dette risikoområdet oppleves av de som er satt til å styre det. Hensikten er å belyse noen av de utfordringer rederiene står oppe i som følge av digitaliseringene vi allerede har gjennomgått og kommer til å gjennomføre.

Problemstilling: Hvordan utfører rederiene cyber risikovurderingene, hvilke roller er involvert og hvordan oppleves prosessen av de HSEQ-ansatte?

Teori: Det er benyttet teori fra IMO, veileder i cybersikkerhet om bord på skip utgitt av BIMCO, teori om verdivurderinger og risikovurderinger av tilsiktede uønskede hendelser samt noe teori om sikkerhetskultur.

Metoder: Kvalitativ metode ved bruk av semistrukturerte intervjuer, systematisk tekstkondensering som analysemetode av 5 transkriberte intervjuer.

Resultater: Funn i studiet kan tyde på at rederiene i stor grad involverer eksterne parter i gjennomføringen av cyber risikovurderinger, utvelgelse, implementering og oppfølging av risikoreduserende tiltak. Videre kan funn tyde på at risikovurderingsmetodikken som benyttes i stor grad er den samme som for utilsiktede uønskede hendelser.

Konklusjon: Rederiene gjennomfører pålagte cyber risikovurderinger, gjennom bruk av eksterne leverandører av sikkerhetstjenester. Det foreligger imidlertid en mulighet for en informasjonsasymmetri mellom leverandørene og rederiene som kan føre til at rederiene ikke mottar en tilpasset tjeneste. Gjennomføring og dokumentering av en verdikartlegging kan øke sannsynligheten for at sikkerhetsleveransene bedre tilpasses det enkelte rederi.

Nøkkelord: Cyber risikovurdering, sårbarhetsvurderinger, trusseletterretning, verdikartlegging, rederi, fartøy, BIMCO, IMO, informasjonsasymmetri.

SUMMARY

Background: The shipping companies are required by the International Maritime Organization (IMO) to conduct cyber risk assessments and incorporate them into their safety management systems from the first audit after January 1, 2021.

Purpose: The purpose of this study is to gain knowledge about how shipping companies manage the IMO's requirements for conducting cyber risk assessments, who is involved, and how this area of risk is perceived by those responsible for overseeing it. The intention is to shed light on some of the challenges faced by shipping companies as a result of the digitization processes we have already undergone and will continue to implement.

Research question: How do the shipping companies perform the cyber risk assessments, which roles are involved, and how is the process experienced by the HSEQ personnel?

Theory: The theory used includes IMO guidelines, the BIMCO guidance on cybersecurity onboard ships, theories on value assessments and risk assessments of intentional undesired events, as well as some theories on safety culture.

Method: Qualitative method using semi-structured interviews, systematic text condensation as the analysis method of 5 transcribed interviews.

Findings: Findings in the study may indicate that the shipping companies largely involve external parties in conducting cyber risk assessments, selection, implementation, and follow-up of risk-reducing measures. Furthermore, findings may suggest that the risk assessment methodology used is largely the same as that for unintended adverse events.

Conclusion: The shipping companies carry out mandated cyber risk assessments by utilizing external security service providers. However, there is a potential for an information asymmetry between the providers and the shipping companies, which may result in the companies not receiving a tailored service. Conducting and documenting a value mapping can increase the likelihood of security deliveries being better aligned with each individual shipping company.

Keywords: Cyber risk assessment, vulnerability assessments, threat intelligence, value mapping, shipping company, vessel, BIMCO, IMO, information asymmetry.

BEGREPSAVKLARING OG DEFINISJONER

BIMCO	Baltic and International Maritime Council (Kessler & Shepard, 2022).
Cyber	Benyttes om alt som er på internett og digitalt. Cyberspace refererer til en verden av sammenkoblede datasystemer og informasjonsressurser. Betegnelsen blir ikke benyttet i rammeverk for digital hendelseshåndtering, men sidestilles i denne sammenheng med betegnelsen «IKT», (Nasjonal Sikkerhetsmyndighet, 2022).
Digitalisering	Digitalisering er det å legge til rette for generering av digital informasjon samt håndtering og utnyttelse av informasjonen ved hjelp av informasjonsteknologi (Dvergsdal, 2023).
DSC	Digital Selective Call.
ECDIS	Electronic Chart Display and Information Systems.
Ekstern part	Leverandør av sikkerhetstjenester.
GPS	Global Position System.
Guideline	Veileder.
Hacking	Et teknisk angrep mot en maskin eller tjeneste som truer sikkerhetstjenestens konfidensialitet, integritet og/eller tilgjengelighet. Begrepet benyttes ofte synonymt med datakriminalitet (Nätt T. H., 2023)
IMO	International Maritime Organization.
Informasjonsasymmetri	En situasjon som er kjennetegnet av at forskjellige aktører har kjennskap til forskjellig informasjon når de skal fatte beslutninger (Andresen, 2023).
Innsider	En innsider kan være en ansatt eller en tredjepart, en forretningspartner, klient, konsulent eller samarbeidende

	kontraktør, et individ du stoler nok på til å gi vedkommende tilgang til systemene dine (NSM, 2016).
Intensjon	At noen har et ønske om å utgjøre en trussel mot deg eller dine verdier (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).
Integritet	At informasjonen eller data ikke blir endret utilsiktet eller av uvedkommende (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).
ISM koden	International Safety Management Code.
IT	Informasjonsteknologi systemer. Bruker data som informasjon (IMO, 2017).
Jamming	En bevisst utsending av radiostøysignaler, for å forstyrre, stenge eller hindre mottak av signaler fra annen stasjon, og for å påvirke posisjonstjenester, f.eks. GPS (Engerengen, 2023).
Kapabilitet	Evne, kunnskaper, ferdigheter som skal til for å utføre en handling (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).
Keylogger	Tastaturlogger, eller keylogger, er en mekanisme som fanger opp og lagrer eller sender videre alle tastetrykk en bruker utfører på tastaturet (Nätt T. H., 2022).
Konfidensialitet	At informasjonen eller data ikke blir kjent for uvedkommende (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).
Malware	Ondsinnet programkode.
OT	Operasjonell teknologi systemer. Bruker data for å kontrollere eller monitorere fysiske prosesser (IMO, 2017).
Ransomware	Løsepengevirus.
Risikovurdering	Med risikovurdering menes i dette studiet sammenheng risikoanalyse med risikoidentifisering og evaluering,

	risikobehandling i form av styring og evt. finansiering, samt risikoledelse i form av beslutninger og planlegging (Aarset, 2020).
Sikkerhet	Tilstand med fravær av uønskede hendelser eller frihet fra fare og frykt. Denne tilstanden er imidlertid ikke statisk, men påvirkes av endringer i faktorer som trussel og farer, sårbarhet og verdi (Stranden & Rosvold, 2023).
SMS	Safety Management System, sikkerhetsstyringssystem.
Sårbarhet	Manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin opprinnelige tilstand eller funksjon etter hendelsen (Busmundrud, Maal, & Kiran, 2015).
Tilsiktet	Ønsket.
Tilsiktet uønsket hendelse	En uønsket hendelse som forårsakes av en aktør som handler med hensikt (Norsk Standard, 2012).
TLP	Trafikklysprotokoll.
Trussel	En trussel kan være hva som helst, enten fysisk eller abstrakt, dersom det har potensiale til å negativt påvirke et objekt eller system (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).
Trusselaktør	En entitet som er involvert i utførelsen av et inntrengingsforsøk (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).
Utilsiktet	Ikke ønsket.
Vannhull	I et vannhullsangrep kompromitterer en trusselaktør en internettside som hyppig besøkes av personer i en aktuell målgruppe slik at besøkende på nettsiden serveres skadevare (NSM, 2016).

VHF	Very High Frequency.

INNHOLDSFORTEGNELSE

FIGURLISTE

LISTER OVER TABELLER

1.0 INNLEDNING

Risikostyring er en gammel og innarbeidet øvelse. Historisk sett har trolig en bevisst (eller ubevisst) tilnærming til risiko vært til stede i ulike sivilisasjoner fra «tidenes morgen». Et av formålene med dannelsen av de tidligste sivilisasjoner kan ha vært relatert til temming av vann, først og fremst for å legge til rette for kontrollerte avlinger men også få å redusere risikoen for matmangel og ødeleggelser pga. av ukontrollert vannstrøm.

Den maritime sektoren har gjennom århundrene vært bevisst ulike risikoer det medfører å ferdes på havet. Den Internasjonale Maritime Organisasjon (IMO) ble dannet for å internasjonalisere reguleringen av sikkerhet og trygghet til sjøs. Safety of Life at Sea-konvensjonen (SOLAS) kom i 1914 som en følge av Titanics forlis i 1912 (Wikipedia, 2022).

Risikoområdene i den maritime sektoren har utviklet, og utvidet, seg opp gjennom årene etter hvert som nye aktivitetstyper og operasjonsområder har oppstått, nye fartøytyper har sett dagens lys, og ny teknologi har blitt tatt i bruk.

Med implementering av ny teknologi, innenfor navigasjon, kommunikasjon, lasthåndtering, stabilitet og fremdriftssystemer, fjernaksessering (remote tilgang), etc., har en rekke forbedringer og effektiviseringer blitt oppnådd. I dag innebærer en teknologiutvikling svært ofte nye digitaliserte løsninger, eller remote tilgang til eksisterende digitale løsninger. Digitalisering og remote tilgang innebærer imidlertid også en eksponering for helt nye sårbarheter og risikoområder.

Cyber-begrepet blir brukt om alt som er på internett (gir mulighet for remote tilgang) og er digitalt (Nasjonal Sikkerhetsmyndighet, 2022). Selv om internett ble allment tilgjengelig fra midten på 1990-tallet, tok det noe tid før internett ble tilgjengelig om bord i fartøy i rom sjø og på åpent hav. Parallelt med at teknologiene (databærerne) har utviklet seg slik at internettdekningen, båndbredde og stabilitet har blitt bedre, har stadig flere enheter og systemer blitt tilkoblet internett permanent eller tidvis.

I kjølvannet av den beskrevne teknologiske utviklingen har det fremkommet eksempler på at digitale tekniske løsninger ombord i fartøyer har blitt utsatt for tilsiktede og utilsiktede uønskede hendelser med den følge av at liv, helse, miljø og verdier har gått tapt eller blitt utsatt for skade eller stor fare.

Slike hendelser har skapt en erkjennelse av et behov for å etablere en bevisst håndtering av de nye risikoområdene som har oppstått som følge av den beskrevne utviklingen. IMO`s Maritime Safety Committee kom i 2017 med resolusjon MSC.428(98) hvor de erkjenner det

umiddelbare behovet for å styrke bevisstheten rundt cyber risiko trusler og sårbarheter for å støtte trygg og sikker shipping, som er operasjonelt motstandsdyktig mot cyber risikoer (IMO, 2017).

Med dette som bakgrunn ønsker jeg i dette studiet å forsøke å belyse følgende problemstilling:

1.1 PROBLEMSTILLING

> **«Hvordan utfører rederiene cyber risikovurderingene, hvilke roller er involvert og hvordan oppleves prosessen av de HSEQ-ansatte?»**

Refleksjoner rundt problemstilling og egen forforståelse:

IMO har, gjennom konvensjonen Safety of Life at Sea (SOLAS), etablert et krav om at alle rederier skal etablere et eget sikkerhetsstyringssystem (SMS) for sin virksomhet. For norskregistrerte fartøyer er dette lovregulert gjennom «*Forskrift om sikkerhetsstyringssystem for norske skip og flyttbare innretninger*» (Lovdata, 2022). I forskriftenes kapittel 8 Beredskap, pkt. 8.1 «*Selskapet skal identifisere mulige nødssituasjoner ombord, og innføre framgangsmåter for å reagere på dem*», pkt. 8.2 «*Selskapet skal opprette programmer for trening og øvelser i å forberede seg på handling i nødssituasjoner*» og pkt. 8.3 «*Sikkerhetsstyringssystemet skal omfatte tiltak som sikrer at selskapets organisasjon til enhver tid kan reagere på farer, ulykker og nødssituasjoner der selskapets skip er berørt*» (Lovdata, 2014), pålegges selskapet (rederiet) å gjennomføre en identifisering av trusler og sårbarheter som kan utløse nødsituasjoner. Identifiseringen av egne risikoer og etablering av planverk for håndtering av slike situasjoner er en forutsetning for at nødvendig beredskap mot krisesituasjoner blir ivaretatt og vil kunne være en forutsetning for en vellykket krisehåndtering.

1.2 AVGRENSNING

Ved å avgrense en problemstilling kan man gjøre det enklere å finne relevant litteratur, finne eget perspektiv og ståsted (Dalland, 2017).

I dette studiet tas det utgangspunkt i HSEQ-ansatte ved rederier innenfor ulike typer maritime næringer i Møre og Romsdal (Norge) sin informasjon rundt cyber risikovurderinger. Studiet er derfor ikke avgrenset til en spesifikk maritim næring. Det kan også ligge kulturelle forskjeller til grunn for hvordan cyberrisikoområdet blir behandlet av rederiene. Intervjupersonenes kjennskap til området og deres deltagelse i cyber risikovurderingene er definerende for hvordan og på hvilken måte problemstillingen svares ut.

Problemstillingen er vid i den forstand at den kan omfatte mye. Hele cyberrisikostyringsprosessen ble vurdert som for omfattende for dette studiet og det er derfor fokusert på identifisering av trusler og sårbarheter, egne verdier, risikovurderingene, og behandling av identifiserte risikoer. Etablering av beredskapsplanverk, respons og gjenoppretting er derfor ikke behandlet i dette studiet, til tross for at dette er svært viktige elementer i en helhetlig cyber risikostyringsprosess.

Studiet er videre avgrenset til å omhandle tilsiktede uønskede hendelser. Utilsiktede uønskede hendelser er bevisst utelatt, selv om slike hendelser også representerer cyberrisikoer for rederiene. Bakgrunnen for denne utelatelsen er ønsket om å fokusere på risikovurderinger av hendelser gjennomført med en intensjon om å ramme noen og hva slike problemstillinger kan representere når man velger en tilnærming til eller valg av metode for gjennomføring av risikovurderinger.

1.3 SPRÅK OG OVERSETTELSER

Bakteppet for problemstillingen er IMOs innføring av et krav om gjennomføring av cyber risikovurderinger. IMO, som en internasjonal organisasjon, utsteder alle dokumenter på engelsk. Cybersikkerhetsområdet er preget av en svært rask utvikling, både når det gjelder nye digitale teknologiske løsninger, men også nye sårbarheter og trusler. Litteraturen på området er derfor i stor grad utgitt på engelsk og ikke oversatt til norsk. Metodikken for styringen av cyberrisiko har imidlertid vært noe konsis over tid, noe som har ført til at man der finner en del norsk litteratur. Studiets litteratur er derfor en kombinasjon av engelsk og norsk, med den følge at det også benyttes noen engelske begreper i teksten. Benyttede begreper er forsøkt forklart i kapittelet Begrepsavklaring og definisjoner.

1.4 OPPGAVENS OPPBYGNING

Oppgaven er delt inn i fem kapitler. Første kapittel omhandler de teoretiske perspektiver som danner grunnlaget for drøftingen av resultatene i studiet. I det neste kapittelet gjennomgås relevant litteratur som resultatene blir drøftet mot. Det påfølgende kapittel omhandler studiets metode og det redegjøres for metodiske valg. Resultatene fra den kvalitative undersøkelsen presenteres i kapittel fire, mens drøftingen gjennomføres i kapittel frem. Til slutt blir oppgaven avsluttet med egne betraktninger rundt implikasjoner for videre praksis og forslag til videre forskning på området.

1.5 ETISKE REFLEKSJONER

Intervjupersonenes identitet skal anonymiseres. Det er viktig at ikke intervjupersonene får en følelse av at de har utlevert egen arbeidsgiver og at de forstår at deres svar vil kunne forbedre cybersikkerhetsrisikostyringen i maritim sektor.

Jeg har ikke selv vært ansatt i et rederi eller arbeidet på sjøen og har derfor ingen egne erfaringer om hva som er «normal» risikostyring i rederiene. Sannsynligheten er derfor liten for at jeg vil kunne farge konklusjonen i studiet. Jeg har imidlertid egne erfaringer med cyber risikostyring fra annen virksomhet og disse erfaringene vil kunne påvirke måten jeg utformet intervjuspørsmålene og tolket svarene på. Denne fallgruven har jeg vært bevisst gjennom hele studiet.

2.0 TEORETISK GRUNNLAG

Relevant teori som kan bidra til å belyse problemstillingen vil være tema i dette kapittelet. Ulike teorier vil bli benyttet idet resultatet fra den kvalitative undersøkelsen skal drøftes i kapittel fem.

Første del av teori-kapitlet vil omhandle IMO sin beslutning om å innføre krav om at cyberrisikoer skal inkluderes i rederienes eksisterende sikkerhetsstyringssystemer.

I neste delkapittel vil rammeverk og guidelines som beskriver hvordan cyber risikovurderinger kan gjennomføres og hva som kan være viktig i cyber risikovurderingers ulike faser behandles. Baltic International Maritime Council (BIMCO) sin utgivelse The Guidelines on Cyber Security Onboard Ships version 4 (BIMCO et.al., 2021) vil danne hovedgrunnlaget i dette delkapitlet sammen med Digital Sikkerhet – En innføring (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020), samt Maritime Cybersecurity – A Guide for Leaders and Managers (Kessler & Shepard, 2022).

2.1 KRAV TIL GJENNOMFØRING AV CYBER RISIKOVURDERINGER

IMO er en organisasjon under FN. IMO utvikler regulatoriske rammeverk for internasjonal shipping som adresserer trygghet, miljøforhold, legale forhold, security og internasjonalt teknisk samarbeid (Kessler & Shepard, 2022). SOLAS og konvensjonen om maritim forurensning Maritime Polution (MARPOL) er trolig de konvensjonene IMO er mest kjent for.

2.1.1 IMO 2021

IMO har, som svært mange andre, registrert hvilke sikkerhetsutfordringer digitaliseringen av samfunnet har ført til og på bakgrunn av dette adopterte IMO`s Maritime Safety Committee (MSC) 16.juni 2017 Resolusjon MSC.428(98): MARITIME CYBER RISIK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS hvor de;

> «*erkjenner det umiddelbare behovet for å heve bevisstheten på cyber risiko trusler og sårbarheter for å støtte trygg og sikker shipping, som er operasjonelt motstandsdyktig mot cyber risikoer*», (IMO, 2017).

IMO har ikke selv produsert detaljerte spesifikasjoner for cyberforsvar spesifikt rettet mot den maritime industrien. Generelle guidelines utstedt av IMO har vært ment å støtte trygg og sikker shipping som er operasjonelt motstandsdyktig mot cybertrusler (Kessler & Shepard,

2022). IMO viser til International Safety Management (ISM) koden og dens krav til at sikkerhetsstyringssystemet opprettholder en høy standard for trygghet og beskyttelse av miljøet. ISM-kodens mål er sikre skipsoperasjoner, et trygt arbeidsmiljø, etablering av passende sikringstiltak og kontinuerlig forbedring av sikkerhetsstyringsferdigheter, både på land og på sjø (IMO, 2017). Gjennom Resolusjon MSC.428(98) pålegges rederiene å inkludere cyber risikostyring i sine sikkerhetsstyringssystemer (SMS), i samsvar med de mål og krav som ISM-koden stiller. Administrasjoner, i Norge Sjøfartsdirektoratet, oppfordres til å sikre at cyber risikoer er passende adressert i SMS, senest ved første årlige verifikasjon av rederiets «Document of Compliance» etter 1. januar 2021.

I samme dokument viser MSC til MSC-FAL.1/Circ. «Guidelines on maritime cyber risk management» som ble godkjent i april 2017 (IMO, 2017). I dette dokumentet gir IMO generelle og overordnede anbefalinger for maritim cyber risikostyring som kan inkorporeres i rederienes eksisterende risikohåndteringsprosesser og som er komplementære til den eksisterende trygghets- og sikkerhets-styringspraksis.

MSC

> «*erkjenner også at Administrasjoner, klasseselskaper, rederier, operatører, skipsagenter, utstyrsleverandører, tjenesteleverandører, havner og havnefasiliteter og alle andre maritime industri-interessenter også bør ekspeditt arbeide mot å sikre shipping mot den nåværende og kommende cyber trusler og sårbarheter»* (IMO, 2017).

Videre viser MSC til International Safety Management (ISM) Code og ISMs mål som

> *å etablere trygge praksiser i skipsoperasjoner og et sikkert arbeidsmiljø, vurdering av all identifisert risiko for skip, personell og miljøet, etablering av tilstrekkelige tryggingstiltak, og kontinuerlig forbedring av land- og fartøy-bemanningens evne til trygghetshåndtering*,
>
> *Bekrefter at et godkjent sikkerhetsstyringssystem (SMS) også skal omhandle cyber risk håndtering i overensstemmelse med mål og funksjonskrav for ISM-koden*;
>
> *Oppfordrer Administrasjoner til å sikre at cyber risikoer er tilstrekkelig adressert i SMS ikke senere enn ved den første årlige verifikasjonen av rederiets Document of Compliance etter 1. januar 2021.*

Erkjenner de nødvendige forholdsregler som kan trenges for å bevare konfidensialiteten til visse aspekter ved risikohåndteringen (IMO, 2017).

Som nevnt innledningsvis har det i kjølvannet av den teknologiske utviklingen fremkommet eksempler på at digitale tekniske løsninger ombord i fartøyer har blitt utsatt for tilsiktede og utilsiktede uønskede hendelser med den følge at liv, helse, miljø og verdier har gått tapt eller blitt utsatt for stor fare.

Disse hendelsene har skapt en erkjennelse, hos så vel statlige myndigheter som internasjonale organisasjoner, av et behov for å håndtere de nye risikoområdene. Historiske hendelser som beskriver cyberangrep og statistikk over slike hendelser (IBM Security, 2022), underbygger IMOs krav til en umiddelbar håndtering av cybertruslene.

En rekke internasjonale organisasjoner og kommersielle selskaper har gitt ut og tilbyr sektorgenerelle guidelines og beste praksiser for cyber risiko tilnærming. Det eksisterer også slike guidelines og beste praksiser spesifikt rettet mot den maritime sektoren. De overordnede prinsipper er stort sett allmenngyldige, men den maritime sektorens virksomheter krever i større grad et helhetlig perspektiv på cyber risikoområdet på grunn av sektoren kompleksitet. Dette kan illustreres ved Det Maritime Transportsystemet (MTS) som foruten det enkelte fartøy også består av rederier, havner, passasjerterminaler, verft, cargofasiliteter, logistikkselskaper og andre brukere av de maritime fasilitetene (Kessler & Shepard, 2022). Alle digitale kontaktflater med tilhørende koblinger i MTS kan påvirke, og dermed representere, sårbarheter for hver enkelt aktør eller enheter i MTS eller for systemet som helhet.

Slike «arvede» sårbarheter er veldig godt kjent blant trusselaktørene (TA) og dermed også utnyttet. Fenomenet blir gjerne benevnt som leverandørkjeder og leverandørkjedeangrep. Hovedmålet, gjerne en større organisasjon, for et målrettet cyberangrep kan være godt sikret, med få muligheter for en TA. Et slikt angrep vil kunne kreve en høy grad av intensjon og kapabilitet for å lykkes. Gjennom å angripe og skaffe seg fotfeste hos en dårligere sikret leverandør eller underleverandør, kan TA benytte denne leverandørens legitime og tiltrodde tilgang til hovedmålets enheter. Slik angrep på en leverandør kalles gjerne leverandørkjedeangrep.

Likt en del landbaserte industrier som benytter digitaliserte industrikontrollsystemer (ICS) og systemer for overvåkning og styring av ICS (SCADA) benyttes, foruten

informasjonsteknologisystemer (IT), operasjonelle teknologisystemer (OT) i maritim sektor. Slike OT-systemer kan f.eks. være digitale systemer knyttet til navigasjon, manøvrering, ballastregulering, posisjonering (BIMCO et.al., 2021). OT-systemer benytter gjerne dedikerte digitale kommunikasjonsstandarder og er knyttet til et felles nettverk ombord. Det er vanlig at OT-komponenter benytter informasjon fra hverandre for å gi brukeren den informasjonen hen trenger for å utføre sine oppgaver. En GPS-mottaker ombord sender f.eks. løpende posisjonsinformasjon gjennom OT-nettverket til kartmaskin for navigasjon (f.eks. ECDIS), til VHF for å kunne benytte direktesending av posisjon ved bruk av Digital Selective Calling Capability (DSC) i nødsituasjoner-situasjoner, osv. Hvis en enhet tilknyttet OT-nettverket ombord også har en nettverkstilknytning mot internett, periodevis eller permanent, vil dette kunne medføre utnyttelse av sårbarheter knyttet til alle enheter som er tilkoblet det samme OT-nettverket. Dette illustrerer og underbygger behovet for en helhetlig tilnærming til problemstillingen i dette studiet.

For rederier som er pålagt å ha et sikkerhetsstyringssystem innebærer kravet at de nå må gjennomføre risikovurderinger også på cyberområdet. For en del rederier vil dette medføre noe nytt, mens for andre vil dette kun medføre at risikovurderinger de tidligere har gjennomført «frivillig», nå er blitt et krav. Idet risikoer på cyberområdet ofte er knyttet til tilsiktede uønskede handlinger, vil rederienes innarbeidede tilnærming til vurderingsprosessen og erfaringer med risikovurderinger av utilsiktede uønskede handlinger kunne skape noe forvirring og usikkerhet. Det vil derfor kunne være nyttig å sikre seg støtte gjennom rammeverk og veiledninger.

2.2 RAMMEVERK OG GUIDELINES

IMO gav i juli 2017 ut Guidelines On Maritime Cyber Risk Management. Dette dokumentet gir en veiledning for gjennomføring av cyber risikostyring på et overordnet nivå, områder rederiene bør se på og foreslår en struktur for prosessen. IMO avslutter sin veiledning med å anbefale noen beste praksiser for implementering av cyber risikostyring og trekker frem BIMCO, ISO 27001 og NIST.

En rekke organisasjoner og selskaper har utgitt sektorspesifikke og generelle rammeverk og guidelines for cyber sikkerhet. Internasjonal standard for informasjonssikkerhet (ISO 27001) og NIST er eksempler på organisasjoner og standarder og veiledninger som brukes på tvers av sektorer, og som IMO støtter seg til.

BIMCO er en global shipping-organisasjon som dekker mer enn 60 % av den globale flåten og består av lokale, globale, små og store selskaper (Baltic and International Maritime Council, 2023). Organisasjonen gir ut et bredt spekter av informasjon, veiledere, analyserapporter osv. Innenfor det maritime cybersikkerhetsområdet har BIMCO, sammen med flere andre organisasjoner, gitt ut guidelines for å veilede de maritime aktørene gjennom cybersikkerhetsområdet; «The Guidelines On Cyber Security Onboard Ships» (BIMCO et.al., 2021). Bakgrunnen for utgivelsen av denne veilederen er et erkjent behov for å sette cybersikkerhet på agendaen og støtte medlemmene i arbeidet med cybersikkerhet i maritim sektor.

BIMCOs veileder forklarer hvorfor og hvordan cyber risikoer kan håndteres i en shipping kontekst. Målet med veilederen har vært å utvikle en strategi for å håndtere cyberrisikoene, i tråd med relevante standarder. BIMCO har, i tillegg til IMO 2017, benyttet The U.S. National Institute of Standards and Technology (NIST) sitt Cyber Security Framework som støtte ved utarbeidelsen av veilederen (BIMCO et.al., 2021).

Det har blitt utgitt flere versjonsoppdateringer av The Guidelines On Cyber Security Onboard Ships (BIMCO et.al., 2021) for å hjelpe den internasjonale maritime næringen med å forbedre trygghet og sikkerhet for sjøfolk, miljø, cargo og fartøy (BIMCO et.al., 2021). Når dette studiet gjennomføres er versjon 4 gjeldende og dette studiet tar utgangspunkt i denne versjonen. Veilederen vil i resten av dette studiet benevnes BIMCO og de påfølgende delkapitler vil omhandle deler av denne veilederen.

2.2.1 Forankring og roller

ISO 27001, IMOs guidelines, BIMCO og NIST (NIST, The U.S. National Institute of Standards and Technology, 2018) understreker alle at en cyber risikokultur bør starte på øverste ledernivå og forankres der. Dette for å sikre en helhetlig, fleksibel og kontinuerlig cyber risikotilnærming, at risikotilnærmingen evalueres og kontinuerlig forbedres. Gjennom bruk av NISTs rammeverk utvikles en profil som kan være til hjelp for å identifisere og prioritere tiltak som kreves for å redusere cyber risikoene. Eksempler på slike profiler for ulike maritime sektorer er offentlig tilgjengelige (NIST, The U.S. National Institute of Standards and Technology, 2018).

Å utvikle, implementere, vedlikeholde og kontinuerlig forbedre et system for cyber risikostyring i et rederi innebærer et betydelig arbeid. Det vil være ressurskrevende. Mange rederier mangler ansatte med kompetanse på området og det vil svært ofte medføre vesentlige

kostnader knyttet innhenting av eksterne ressurser siden få rederi selv besitter cybersikkerhetskompetanse. Siden cyber risikoer har et potensiale for svært stor negativ påvirkning, ikke bare for personelltrygghet, og miljø, men også for måloppnåelse og omdømme, vil en cyberhendelse kunne påvirke selskapets overlevelsesevne. En forankring i toppledelsen vil derfor være nødvendig for å sikre en adekvat tilnærming.

Toppledelsen bør legge til rette for en kultur for cyber risikostyring på alle nivå i organisasjonen og sikre en helhetlig og fleksibel tilnærming (BIMCO et.al., 2021).

Arbeidet med en digital sikkerhetskultur er ledelsens ansvar, samtidig som det krever deltagelse fra alle (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020). Ledelsen må sette klare mål for hva som ønskes oppnådd, arbeide målrettet og helhetlig med temaet over tid. Toppledelsen bør kommunisere intern støtte til arbeidet underveis og bidra med kunnskap om egen organisasjon og nødvendige beslutninger (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).

En effektiv cyber risikostyring avhenger av en tydelig plassering av internt ansvar og oppgaver (BIMCO et.al., 2021). Ansvar og oppgaver bør dokumenteres i sikkerhetssystemet og i stillingsbeskrivelser. For enkelte rederier kan det være nødvendig å allokere slikt ansvar og slike oppgaver til en ekstern part (BIMCO et.al., 2021). Dette vil være spesielt aktuelt for rederier med en begrenset landorganisasjon og for rederier som mangler cybersikkerhetskapabiliteter internt. Ofte vil plasseringen av ansvar og oppgaver for cybersikkerhet fungere best om den samsvarer med ansvarsplasseringen for de øvrige risikoområder i rederiet (BIMCO et.al., 2021).

Etter at trusler og sårbarheter er identifisert og risikoene analysert, bør ledelsen involveres i beslutningen om hvorvidt håndteringstiltak skal iverksettes for å redusere (mitigere) risikoene til et akseptabelt nivå for rederiet (BIMCO et.al., 2021).

For å sikre en helhetlig tilnærming til operasjonelle risikoer, bør rederiet etablere et nivå for risikoaksept som er besluttet av styret eller reder / eier. Identifiserte cyber restrisikoer bør ikke ligge over besluttet risiko akseptnivå.

2.2.2 Forholdet mellom Informasjonsteknologi og Operasjonsteknologi

Mens informasjonsteknologisystemer (IT) håndterer data og støtter forretningsfunksjoner, er operasjonsteknologier (OT) hardware (enheter), systemer og programvare som direkte overvåker og kontrollerer fysiske enheter og prosesser. Slike prosesser er direkte integrerte i

et skip og må fungere uavhengig av IT-systemer ombord (BIMCO et.al., 2021). Som den del av IT regnes også de nettverk og nettverkskomponenter som muliggjør en dataflyt mellom land og fartøy.

Eksempler på dette kan være satellittbasert kommunikasjonsløsninger som f.eks. Iridium og VSAT, mobilt bredbåndsløsninger som f.eks. 4G og 5G eller Mobile Broadband Radio (MBR).

Eksempler på OT-systemer kan være ulike brosystemer (GPS, DP, ECDIS, AIS), fremdriftssystemer (motorstyring, kraftproduksjon, utslipps- og forbruks-overvåkning, etc.), lastesystemer, ballaststyring, osv.

Det er viktig at OT-systemenes potensielle sårbarheter blir beskyttet på en tilstrekkelig måte og ikke blir ubeskyttet eksponert i IT-nettverk. Spesielt viktig er dette for eldre fartøyer hvor etablerte OT-systemer aldri var tenkt eksponert mot internett.

2.2.3 Forløpet i en cyber risikostyringsprosess

Figur 1: BIMCO`s tilnærming til cyber risikostyring (BIMCO et.al., 2021)

Dette studiet vil sette fokus på de fire første trinnene i BIMCO`s tilnærming til cyber risikostyring; identifisering av trusler, identifisering av sårbarheter, risikovurdering og utvikling av tiltak og deteksjonsmekanismer. Respons- og beredskapsplaner samt gjenoppretting vil som tidligere nevnt ikke omhandles i dette studiet, selv om dette er en svært viktig del av cyber risikostyringen i rederiene.

I BIMCO`s veiledning følger en opplisting av potensielle sårbare systemer og data om bord. Det synes imidlertid å mangle en uttrykt nødvendighet av å ha gjennomført en verdikartlegging i rederiet, gjerne i forkant av cyber risikovurderingen.

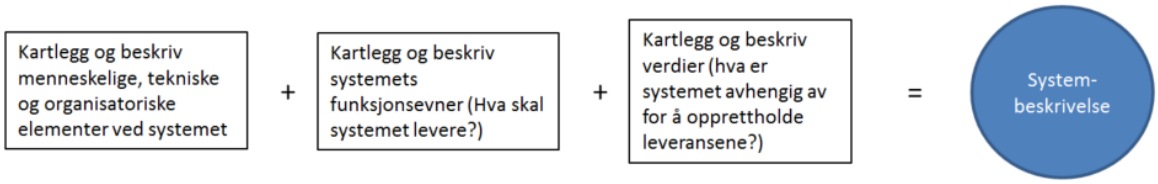
2.2.3.1 Verdier

Identifiseringen av cyber risikoer kan være utfordrende å gjennomføre uten først også å ha et bevisst forhold til hvilke verdier man har et ønske om å beskytte. Det finnes ikke to like rederier med helt like verdier og med det heller ikke to like strategier for styring av cyberrisikoer (Kessler & Shepard, 2022).

Kartlegging av verdier vil være viktig for kunne vurdere konsekvensen av et cyberangrep, men også identifisering av mulig trusselaktører. En verdi kan defineres som en

> «*ressurs som hvis den blir utsatt for en uønsket påvirkning vil medføre negative konsekvens for den som eier, forvalter eller drar fordel av ressursen*»
>
> (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).

I verdikartleggingen er det viktig å vurdere hva virksomheten skal produsere (et produkt eller en tjeneste) og levere for å opprettholde sin misjon (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020). For å produsere benytter de fleste virksomheter et eller flere system. Beskrivelsen av et system forsøkes illustrert gjennom figur 2.



Figur 2 viser sammenhengen mellom en verdivurdering og en systembeskrivelse (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020)

Med andre ord vil organisasjonens systembeskrivelse; egenskaper, formål og funksjon være avgjørende for vurderingen av hvem som kan være en potensiell trusselaktør og hva konsekvensene vil kunne være om systemet blir utilgjengelig, om data endres eller om informasjonen i systemet tilflyter uvedkommende.

Det kan være nyttig å stille seg spørsmålet «Hvilken verdier har vi?», «Er det andre som besitter lignende verdier som oss?». Hvis svaret er ja; «Kan vi opprette et samarbeid om deling av informasjon om kartlegging og forsøk inntrengning med andre som besitter lignende verdier?» (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020). Samarbeid om trusseletterretning vil videre behandles under delkapittelet om trusler.

I Forskrift om sikkerhetsstyringssystem for norske skip og flyttbare innretninger pkt. 10.3 (Lovdata, 2014) stilles det krav til at rederiet skal identifisere utstyr og tekniske systemer som kan forårsake farlige situasjoner i tilfelle av plutselig svikt. Rederiene er gjennom forskrift allerede pålagt å ha identifisert kritisk utstyr som kan føre til farlige situasjoner ved bortfall. Om slikt identifisert utstyr er dokumentert kan det tolkes som at en delvis verdivurdering er gjennomført. I en cybersammenheng vil dette utstyret ofte kunne defineres som operasjonelt

utstyr (OT) og i liten grad IT. Utstyr som ikke er kritisk for sikker operasjon men som kan påvirke en spesifikke operasjons måloppnåelse, trenger nødvendigvis ikke å stå på listen over kritisk utstyr. Slikt utstyr kan likevel inneha sårbarheter som, hvis de blir eksponert for en trusselaktør, igjen kan åpne muligheter (bakdører) hos andre og viktigere enheter.

BIMCO har i sin veileder (BIMCO et.al., 2021) anbefalt å bruke listen over kritisk utstyr og tekniske systemer, pålagt etablert gjennom ISM-koden, samt kritikalitets vurdere enheter på denne listen. I Annex 1 i veiledningen lister BIMCO opp eksempler på systemer potensielt sårbare systemer, kategorisert etter funksjonsområder som f.eks. kommunikasjon, brosystemer, cargo styringssystemer, osv.

Verdielementet i risikovurderinger vil bli ytterligere behandlet under delkapittelet om risikovurderinger.

2.2.3.2 Trusler

Det finnes flere definisjoner av «trussel». Bergsjø, Windvik og Øverlier sammenfatter flere definisjoner av trussel med følgende:

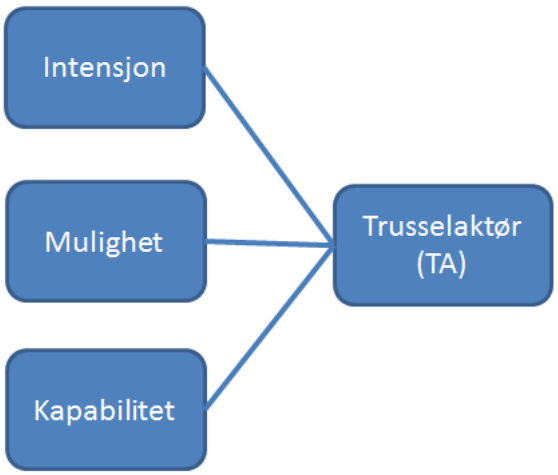
> *«En trussel kan være hva som helst, enten fysisk eller abstrakt, dersom det har potensiale til negativt å påvirke et objekt eller system.»*
>
> (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).

Under arbeidet med cyber risikostyringen og risikovurderingen vil det være nødvendig å identifisere hva, gjennom digitale muligheter, som negativt kan påvirke et system og derigjennom fartøyet; altså potensielle trusler. Truslene er i dette studiet, representert gjennom mennesker (trusselaktører). Det er minst 2 sider ved en trusselaktør som er interessant i en cybersammenheng; hvem trusselaktøren er og hvordan trusselen fra aktøren materialiserer seg (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).

Studiet er, som beskrevet i avgrensningen, begrenset til å omhandle tilsiktede uønskede hendelser. Det vil si at uønskede hendelser som ikke er tilsiktet eller intendert ikke inngår i dette studiet. Utilsiktede uønskede hendelser er imidlertid veldig viktig å ta høyde for i en cyber risikostyring.

Under arbeidet med identifisering av trusselaktører bør man vurdere de ulike spesifikke aspekter ved trusselaktøren`s kapabilitet, mulighet og intensjon for å angripe (BIMCO et.al.,

2021). Det finnes en rekke forskjellige typer trusselaktører. Trusselaktørene har derfor ulike intensjoner, muligheter og kapabiliteter til å gjennomføre cyberangrep mot ulike mål.



Figur 3: Illustrer forholdet mellom intensjon, mulighet og kapabilitet hos en trusselaktør (TA).

En trusselaktørs grad av intensjon, motivasjon eller vilje til å gjennomføre et cyberangrep mot et mål vil også være en vesentlig faktor i vurderingen av hvor sannsynlig det er at et cyberangrep lykkes. Hvis motivasjonen ligger i ren nysgjerrighet i forhold til hva man selv kan få til er det mulig at en trusselaktør gir opp sitt forsøk om vedkommende møter beskyttelsestiltak av en gitt karakter. I den andre enden av skalaen, om motivasjonen ligger i ønske om eller behov for tilgang til sikkerhetspolitisk informasjon av svært høy viktighet er det nærliggende å anta at trusselaktøren ikke gir opp om vedkommende møter beskyttelsestiltak. Trolig vil hen heller forsøke å omgå disse tiltakene.

Gruppe (Trusselaktør)	**Intensjon (motivasjon, vilje)**
Aktivister (inkl. misfornøyde ansatte)	• Hevn • Forstyrrelser av operasjoner • Media-oppmerksomhet • Omdømmetap
Kriminelle	• Finansiell gevinst • Kommersiell spionasje • Industri spionasje
Opportunister	• Utfordringen • Omdømme gevinst • Finansiell gevinst
Stater, statlige støtte organisasjoner, terrorister	• Politisk / ideologisk gevinst, f.eks. (u)kontrollert forstyrrelse av økonomier og kritisk nasjonal infrastruktur • Spionasje

	• Finansiell gevinst • Kommersiell spionasje • Industri spionasje • Kommersiell gevinst

Tabell 1: Grupper av trusselaktører med eksempler på ulike typer intensjoner for å gjennomføre et cyberangrep, relatert til hver enkelt gruppe. Listen er ikke uttømmende, (BIMCO et.al., 2021).

Graden av mulighet for en trusselaktør vil kunne være veldig avhengig av hvem trusselaktøren er. En misfornøyd ansatt vil ha mulighet for fri og direkte legitim tilgang til utstyr, komponenter eller systemer gitt gjennom sin funksjon eller rolle. Avhengig av gitt tilgang vil vedkommende ha mulighet til f.eks. å infisere et system gjennom å kjøre en ondsinnet kode på en datamaskin. En statlig aktør vil høyst sannsynlig ikke ha samme legitime tilgangen til et OT- eller IT-system, men vil ha store muligheter til å erverve eller utvikle ondsinnet kode som kan utnytte en sårbarhet. Stuxnet[1] er et slikt eksempel (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).

Gruppe (Trusselaktør)	Mulighet
Aktivister (inkl. misfornøyde ansatte)	• Fri tilgang til fysiske lokaler • Autorisert nettverkstilgang
Kriminelle	• Tilgang til tilgjengelige verktøy på offentlige og lukkede forum og på det mørke nettet.
Opportunister	• Tilgang til offentlige tilgjengelige verktøy
Stater, statlige støtte organisasjoner, terrorister	• Muligheter gitt under dekke av å være diplomat • Gitt autorisasjon på uriktig grunnlag (illegalist) • Muligheter gitt ved å forlede organisasjonen

Tabell 2: Grupper av trusselaktører med eksempler på ulike typer muligheter for gjennomføring av et cyberangrep relatert til hver enkelt gruppe. Listen er ikke uttømmende.

Kapabiliteten sier noe om trusselaktørens evne, kompetanse og kunnskap. Kapabiliteten vil kunne være avgjørende for å kunne ramme virksomheten med et vellykket cyberangrep. Et slikt angrep kan f.eks. være å plassere en minnepenn med ondsinnet programvare i en pc, sende en phishing epost med et vedlegg inneholdende ondsinnet kode, eller injisere ondsinnet kode inn i et online OT-nettverk. Virksomhetens egne sårbarheter og allerede implementerte beskyttelsestiltak vil kunne være avgjørende for hvor sannsynlig det er at en trusselaktør med en gitt kapabilitet kan lykkes med sitt forsøk på gjennomføring av et cyberangrep.

Gruppe (Trusselaktør)	Kapabilitet (evne)
Aktivister (inkl. misfornøyde ansatte)	• Kunnskap om eget system og hvor organisasjonen kan påføres ønsket skade • Tilgang til enklere og offentlig kjent verktøy for sårbarhetskanninger

[1] Artikkel fra New York Times om Stuxnet, https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

	• Tilgang til enklere og offentlig kjent skadevare
Kriminelle	• Tilgang til medium avansert og offentlig kjent verktøy for sårbarhetscanninger • Tilgang til kriminelle nettverk med medium avansert skadevare • Tilgang til kriminelle cybernettverk med komplementære ferdigheter
Stater, statlige støtte organisasjoner, terrorister	• Tilgang til avanserte og ikke-kjente verktøy for sårbarhetscanninger • Tilgang til 0-dags-sårbarheter • Tilgang til avansert og skreddersydd skadevare (APT) • Tilgang til kriminelle cybernettverk med komplementære ferdigheter

Tabell 3: Grupper av trusselaktører med eksempler på ulike typer kapabiliteter for gjennomføring av cyberangrep, relatert til hver enkelt gruppe. Listen er ikke uttømmende.

Identifiserte trusler bør vurderes sammen med identifiserte sårbarheter for å evaluere sannsynligheten for at angrep skal kunne lykkes. Allerede implementerte sårbarhetsreduserende sikringstiltak bør tas i betraktning når man vurderer hvor sannsynlig det er at en kjent sårbarhet skal utnyttes.

Det kan også være til stor hjelp ved identifisering av trusler å ha kjennskap til hvem som er ute etter å ramme grupper virksomheten selv er en del av. Årlige åpne nasjonale trusselvurderinger fra f.eks. Politiets Sikkerhetstjeneste (PST) og Forsvarets Etterretningstjeneste (E-tjenesten), eller årlige nasjonale sårbarhetsvurderinger som den utgitt av Nasjonal Sikkerhets Myndighet (NSM), kan være til hjelp for å skaffe seg kunnskap om hvilke trusselaktører som har fokus mot ens egen gruppe (f.eks. maritim sektor). I tillegg til disse mer sektorovergripende årlige utgivelsene, utgis det årlige ulike bransjespesifikke trusselvurderinger. Norma Cyber Annual Threat Assessment 2023 er et eksempel på en bransjespesifikk trusselvurdering i maritim sektor (NORMA, 2023).

Gjennom tillitsbaserte samarbeid mellom virksomheter som besitter de samme typer verdier eller som driver innenfor samme bransje kan nødvendig trusselinformasjon deles. En slik deling mellom virksomheter vil kunne øke kvaliteten på virksomhetenes risikovurderinger.

En annen tilnærming eller «angrepsvinkel» for å finne potensielle trusselaktører kan være å gjennomføre en identifisering av egne sårbarheter før arbeidet med å identifisere trusler på startes. Etter at å ha gjennomført kartlagtlegging av egne digitale sårbarheter er det mulig å benytte åpne tilgjengelige databaser som Killchain (Lockheed Martin , 2023) eller Mitre Att@k (MITRE ATT&CK, 2023). Slike databaser kan være til hjelp om det er ønskelig å vite

hvilke hackerverktøy og fremgangsmåter som er assosiert med ens egne sårbarheter. De refererte databaser gir en oversikt over hvilke aktører som er kjente for å benytte seg av de ulike hackerverktøyene og utnyttelse av de kjente sårbarhetene.

Det er vanlig å kategorisere cyber trusler i «ikke målrettede» og «målrettede» angrep. Ved «Ikke målrettede» angrep er offeret bare en av mange potensiell mål. Ulike verktøy og teknikker er offentlig tilgjengelige og de vanligste er malware (ondsinnet programkode) som er laget for å infisere og skade infiserte maskiner, nekte tilgang til infiserte maskiner og/eller hente ut informasjon om brukerne (BIMCO et.al., 2021). Uthenting av personopplysninger, brukernavn og passord på ulike nettsteder gjennom bruk av keyloggere samt utpressing for å sikre en økonomisk gevinst kan være TA`s motivasjon. Det finnes også andre teknikker og verktøy som f.eks. vannhull og sårbarhetsskanning.

«Målrettede angrep» er langt mer sofistikerte og kan benytte verktøy og teknikker spesielt utviklet for å ramme det spesifikke selskapet eller skipet (BIMCO et.al., 2021). Foruten verktøyene og teknikkene er det spesielt kartleggingen og den sosiale manipulasjonen i forkant av et «målrettet angrep» som skiller det fra et «ikke målrettet angrep». Den sosiale manipulasjonen vil øke sannsynligheten for at offeret for angrepet vil forledes til å gjennomføre noe, f.eks. åpning av et epost-vedlegg inneholdende ondsinnet kode.

2.2.3.3 Sårbarheter

En viktig del av en cyber risikovurdering er å identifisere sårbarheter som kan bli kompromittert og resultere i tap av konfidensialitet, integritet eller tilgjengelighet av data og systemer som er nødvendige for å operere hele eller deler av skipet (BIMCO et.al., 2021).

Nasjonal Sikkerhetsmyndighet anbefaler å kategorisere sårbarheter i (NSM, 2020):

- Menneskelige sårbarheter
- Teknologiske sårbarheter
- Organisatoriske sårbarheter

En sårbarhet kan defineres som:

> «*sannsynligheten for at en trusselkapabilitet overgår motstandskapabiliteten*»
>
> (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020)

En rekke sårbarheter, innenfor alle 3 kategoriene på cybersikkerhetsområdet, er vanlige i det maritime domenet, så vel som i samfunnet ellers. Utdaterte og ustøttede operativsystemer, ikke oppdatert programvare, utdatert eller manglende antivirus, ikke adekvate konfigurasjoner, manglende nettverkssegmentering, kontinuerlig internett-tilkoblinger osv. er eksempler på vanlige sårbarheter (BIMCO et.al., 2021).

Ifølge NIST`s National Vulnerability Database (NVD) er det pr 13.april 2023 lagt inn 8271 nye sårbarheter (CVE – Common Vulnerabilities and Exposures) i 2023. Antallet sårbarheter øker raskt etter hvert som digitaliseringen i samfunnet øker. En del eksisterende sårbarheter blir utbedret fra leverandører av produkter og applikasjoner, andre forblir slik de er og må reduseres gjennom alternative tiltak. For at kundene skal oppleve at sårbarheten blir mindre eller borte, krever det at det gjennomføres en oppdatering av applikasjonen eller produktet med den utarbeidede utbedringen.

For å assistere de ulike trinnene i risikovurderingen, og identifiseringen av sårbarheter, bør IT- og OT-systemene identifiseres og systemansvarlige dokumenteres. Innkjøps- og vedlikeholds-kostnadene bør dokumenteres i samme systemoversikt (BIMCO et.al., 2021). For øvrig vises det til delkapittelet om verdier.

Identifiseringen av sårbarheter involverer en analyse av applikasjoner, systemer og prosedyrer for å avdekke sårbarheter som kan utnyttes av en potensiell trusselaktør. Det kan være nødvendig å involvere ekstern ekspertise med kunnskap om maritim industri for å gjennomføre den slik analyse (BIMCO et.al., 2021).

Noen IT- og OT-systemer er gitt fjerntilgang og kan ligge med en kontinuerlig internett-oppkobling for å kunne overvåke, samle data, vedlikeholde, bedre trygghet eller sikkerhet fra en annen lokasjon. Noen av disse systemene er såkalte «tredjepartsystemer» hvor en leverandør er gitt fjerntilgang til systemer de har levert og har ansvaret for å holde i drift (BIMCO et.al., 2021). Systemer med eksponering mot internett er spesielt sårbare når oppkoblingen er aktiv. En legitim remote tilgang vil også gi en mulighet for illegitim remote tilgang for trusselaktører med tilstrekkelig kapabilitet til å utnytte systemet.

Tiltak for å redusere sårbarheter vil beskrives under delkapitlet som omhandler beskyttelsestiltak.

2.2.3.4 Sannsynlighet

Sannsynligheten for at en cybersikkerhetshendelse skal oppstå er et produkt av en trusselfaktor og en sårbarhetsfaktor, noe som betyr at om en av disse faktorene er nær ikke-eksisterende, vil også sannsynligheten være det samme. Det er imidlertid en tendens til å vurdere risiko kun basert på en potensiell konsekvens og en eksisterende sårbarhet. Dette bør tas i betraktning når man skal kvantifisere sannsynligheten (BIMCO et.al., 2021).

Som støtte ved kvantifisering av sannsynlighet er det normalt å benytte en matrise for risikovurdering, hvor det benyttes en 5-trinns skala (BIMCO et.al., 2021), se eksempel tabell 4.

Nivå	Sannsynlighetsbeskrivelse
1	Ikke kjent. Nær utenkt
2	Kjent, men svært sjelden og et resultat av en kjede med uheldige omstendigheter
3	Hendelser har trolig skjedd i eget selskap, men i sammenheng med utstyrsfeil eller ved overraskende menneskelige uhell
4	Skjer av og til i eget selskap, typisk i sammenheng med utstyrsfeil eller menneskelige feil (feil som skjer om bord fra tid til annen)
5	Skjer ofte når den aktuelle oppgaven skal utføres

Tabell 4: Sannsynlighetsmatrise, (BIMCO et.al., 2021).

Ideelt sett burde man hatt tilgang til et tilstrekkelig statistisk grunnlag av shipping-spesifikke cyber hendelsesrapporter for å kunne anslå sannsynlighet for å bli utsatt for tilsiktede uønskede cyberhendelser med størst mulig sikkerhet. Et slikt statistisk grunnlag finnes imidlertid ikke og man blir derfor avhengig av å søke sektorovergripende for å se hvilke teknikker som tidligere er benyttet for å gjennomføre cyberangrep, (BIMCO et.al., 2021).

2.2.3.5 Konsekvens

En modell for konfidensialitet, integritet og tilgjengelighet (confidentiality, integrity, availability, CIA) gir et rammeverk for å vurdere konsekvensen av:

- Tap av konfidensialiteten til informasjonen, f.eks. gjennom uautorisert tilgang eller avsløring
- Tap av integritet, f.eks. gjennom endring av informasjon og data relatert til trygg og effektiv operasjon
- Tap av tilgjengelighet, f.eks. på grunn av destruksjon eller forstyrrelser av tjenester, systemer eller nettverkstrafikk, (BIMCO et.al., 2021).

Se eksempel i tabell 5.

OT-system	Konfidensialitet	Integritet	Tilgjengelighet	Overordnet konsekvens
Sensor data	Lav	Høy	Høy	Høy
Statistiske data	Lav	Lav	Lav	Lav

Tabell 5: Rammeverk for vurdering av konsekvens med sensor data og statistiske data fra et OT-system som eksempel, (BIMCO et.al., 2021).

Graden av hvor kritisk CIA er vil være avhengig av hva informasjonen og dataene blir brukt til. Eksempelvis vil OT-systemer ombord ha større krav til integritet og tilgjengelighet enn konfidensialitet (BIMCO et.al., 2021).

Kvantifisering av konsekvens gjennomføres vanligvis gjennom en matrise for risikovurdering hvor en konsekvens for en gitt hendelse blir angitt på en 5-trinns skala avhengig av hvor alvorlig konsekvensen vil være for ulike kategorier som f.eks. personelltrygghet, miljø, last, forretningen, økonomisk, omdømme osv. (BIMCO et.al., 2021). Tabell 6 gir et eksempel på en enkel konsekvensmatrise.

Nivå	Konsekvensbeskrivelse
1	Ingen helseeffekter / skader. Ingen skader på miljø, enheter, økonomi eller omdømme
2	Svært små helseeffekter / skader. Svært små skader på miljø, enheter, økonomi eller omdømme
3	Små helseeffekter / skader. Små skader på miljø, enheter, økonomi eller omdømme
4	Større helseeffekter / skader. Små skader på miljø, enheter, økonomi eller omdømme
5	Død eller permanente skader. Store og omfattende, signifikante skader på miljø, enheter, økonomi eller omdømme

Tabell 6: Eksempel på en konsekvensmatrise, (BIMCO et.al., 2021).

Konsekvensvurderingen bør utføres for hvert enkelt system ombord, (BIMCO et.al., 2021). I Forskrift om sikkerhetsstyringssystem for norske skip og flyttbare innretninger, Del a – Gjennomføring, pkt. 10.3:

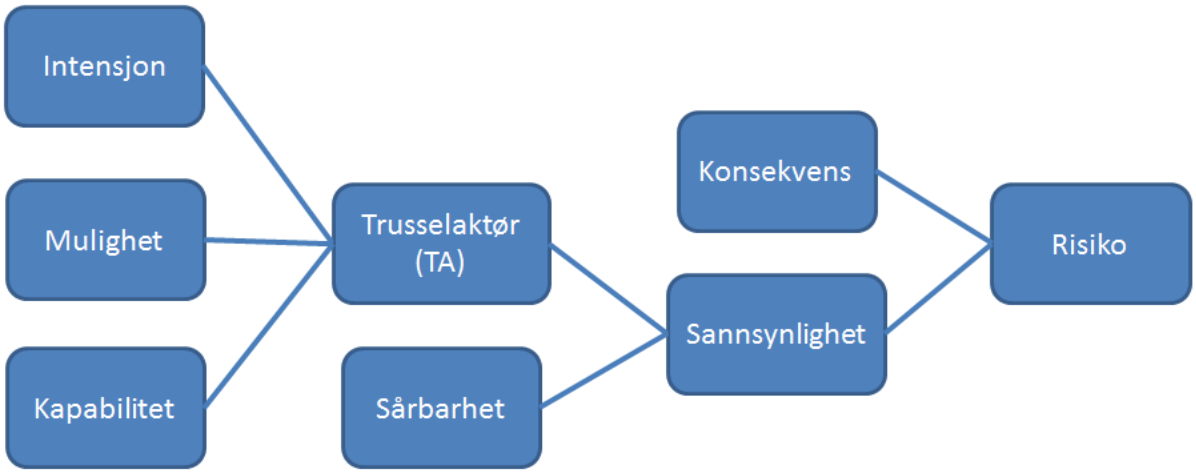
> *«Selskapet skal identifisere utstyr og tekniske systemer som kan forårsake farlige situasjoner i tilfelle av plutselig svikt.»*

En konsekvensvurdering av identifisert utstyr og tekniske systemer som beskrevet i forskriftene bør gjennomføres (BIMCO et.al., 2021).

2.2.3.6 Risikovurdering

Det finnes flere standarder for gjennomføring av risikovurderinger, som f.eks. ISO 31000 som omhandler krav til risikovurderinger. Enkelte standarder, som f.eks. NS 5814, er utviklet for utilsiktede uønskede hendelser. Andre standarder, f.eks. NS 5830, er utviklet for tilsiktede uønskede hendelser. Flere organisasjoner har utviklet veiledere for gjennomføring av risikovurderinger basert på disse standardene. En slik veiledning er BIMCO (BIMCO et.al., 2021) som hevder at en cyber risikovurdering kan kun gjennomføres etter å ha etablert en oversikt over faktorene trusler, sårbarheter, konsekvens og sannsynlighet.

En måte å illustrere faktorenes interne forbindelser på er gjennom et relasjonsdiagram. I et slikt diagram vil boksene representere risikofaktorer og linjene mellom de ulike beskriver hvem som skal multipliseres med hverandre.

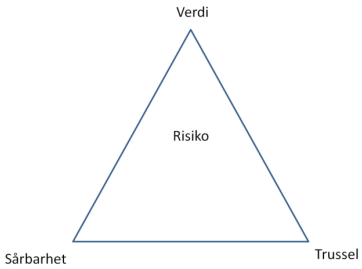


Figur 4: Relasjonen mellom de ulike faktorene som påvirker risikoen, (BIMCO et.al., 2021).

Hvis en av faktorene er null eller svært lav, vil risikoen være det samme.

Faktorer som konsekvens, sannsynlighet, sårbarhet og en trusselaktørs kapabilitet, mulighet og intensjon er alle relevante når en risiko skal vurderes (BIMCO et.al., 2021).

En annen tilnærming til risiko er «Trefaktor» modellen med fokus på verdi, trussel og sårbarhet (VTS). Den er utviklet for å vurdere risiko for tilsiktede uønskede hendelser (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020). I denne modellen defineres risiko som et «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).



Figur 5: Risiko illustrert ved risikotrekanten (VTS).

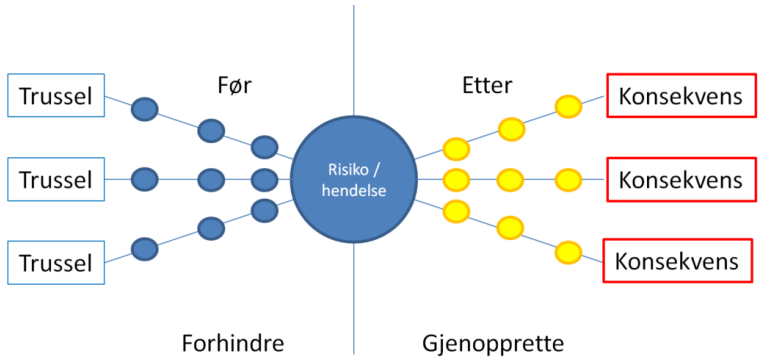
Uavhengig av om risikoene er knyttet til tilsiktede eller utilsiktede hendelser opererer flere av veiledningene for risikovurderinger med 4 faser i vurderingsprosessen. Innholdet i de fire fasene er imidlertid ikke likt. BIMCO (BIMCO et.al., 2021) beskriver innholdet i de 4 fasene som følger; Fase 1 inneholder aktiviteter før selve vurderingen for en gjennomgang av IT- og OT-dokumentasjonen gjennomføres, identifisering av leverandører av kritisk utstyr, inkl. kontaktpersoner, gjennomgang av detaljerte vedlikeholds rapporter og etablering av en oversikt over kontraktkrav og forpliktelser inngår i denne fasen. I fase 2 gjennomføres en vurdering av fartøyet hvor alle faktorer (trusler, sårbarheter, sannsynlighet og konsekvens) vurderes og reduserende tiltak kan utføres. Fase 3 inneholder debrifing og rapportering. For å tilfredsstille kravene i ISM-koden bør risikovurderingene henge sammen i en helhetlig tilnærming, være oppdaterte og med en beskrivelse av hvordan risikoer begrenses. I den fjerde og siste fasen bør funn i risikovurderingene oversendes leverandørene av de påvirkede systemer for å behandle risikoer (BIMCO et.al., 2021).

Ifølge Aarset inneholder en risikovurderingsprosess fire faser; en definisjonsfase hvor scoopet for vurderingen blir bestemt, en fase for risikoanalyse hvor risikoer blir identifisert og evaluert, en risikobehandlingsfase hvor risikostyring og finansiering gjennomføres og til slutt en ledelsesfase hvor det tas beslutninger om hvilke tiltak som skal iverksettes basert på kost-nytte og strategier (Aarset, 2020).

Avhengig av rederiets evne til å gjennomføre egne cyber risikovurderinger, kan rederiet vurdere å be en ekstern ressurs om bistand (BIMCO et.al., 2021). En slik tilnærming til cyber risikovurderinger kan gi en økt verdi om den eksterne parten kan bidra med spesialkompetanse på området. En økt verdi kan også tilføres de selskaper som har få ansatte for å få en mest mulig objektiv og transparent cyber risikovurdering (BIMCO et.al., 2021).

2.2.3.7 Tiltak

Etter at en cyber risikovurdering er gjennomført og cyber risikoer er identifisert bør risikoer som scorer over besluttet risikoaksept nivå behandles (Aarset, 2020). Behandling av risiko kan skje gjennom å avstå fra aktiviteten som påfører virksomheten en risiko, å overføre risikoen til andre, f.eks. gjennom en forsikring, eller å sette inn tiltak som kan redusere risikoen til et akseptabelt nivå (Aarset, 2020). Slike risikoreduserende tiltak kan være organisatoriske, teknologiske eller menneskelige og ha et sannsynlighetsreduserende eller et konsekvensreduserende mål, (Aarset, 2020). Figur 7 illustrerer forskjeller på sannsynlighetsreduserende og konsekvensreduserende tiltak.



Figur 6: En bowtie-modell som illustrerer forholdet mellom trusler, sannsynlighetsreduserende tiltak (blå sirkler) i forkant av en uønsket hendelse, konsekvensreduserende tiltak etter en hendelse og konsekvenser av en hendelse.

Å redusere risikoen til null vil ikke være mulig uten å avstå fra aktiviteten, fjerne systemet eller prosessen hvor risikoen materialiserer seg. En slik tilnærming er svært ofte ikke ønskelig fordi virksomhetens verdi forringes, tiltakene blir for kostbare eller de vil medføre sekundæreffekter som ikke tolereres (Aarset, 2020).

En kombinasjon av teknologiske, menneskelige og organisatoriske tiltak for å redusere sannsynlighet og konsekvens for risikoen er derfor mest benyttet. Slike kombinasjoner kan betegnes som forsvar i dybden («defence in depth).

Beskyttelse i dybden gjennom ulike lag med beskyttelsestiltak, kan være viktig for å oppnå en optimal beskyttelse. Kombinasjoner av sannsynlighetsreduserende beskyttelsestiltak kan være rollebeskrivelser med ansvar og oppgaver (organisatoriske), prosedyrer, sjekklister, retningslinjer og rutiner (organisatoriske), trening, opplæring, øvelser og testing (menneskelige) og brannmurer, IDS, sårbarhetsscanninger, osv. (teknologiske). Slike kombinasjoner av tiltak kan øke muligheten for å avdekke en cyberhendelse, i tillegg til å øke muligheten for å få mest mulig ut av ressursene.

Eksempler på konsekvensreduserende tiltak kan være øvelser, etablering av redundans, backup av data som sikrer tilgjengelighet, avtaler med selskaper som kan bistå virksomheten om en hendelse oppstår, forsikring som reduserer økonomisk tap som følge av hendelsen, osv.

Beskyttelse i dybden vil kun fungere om tekniske- og prosedyre-tiltak er implementert lagvis på tvers av alle sårbare og integrerte systemer. En slik implementering av tiltak kalles forsvar i bredden («defence in breadth»), og har til hensikt å forhindre at en sårbarhet i et system blir brukt til å omgå et beskyttelsestiltak i et annet system (BIMCO et.al., 2021).

Avdekking eller detektering av innbruddsforsøk eller ondsinnede infeksjoner er en sentral del av cyber risikostyringen (BIMCO et.al., 2021). Et bilde av normaltilstanden for nettverkstrafikk og forventet dataflyt for brukere og systemer bør etableres og oppdateres, slik at grenseverdier for varsel av mulig cyberhendelse kan etableres (BIMCO et.al., 2021).

Det eksisterer en rekke tekniske deteksjonsløsninger på markedet, som f.eks. Intrusion Detection System (IDS) og Intrusion Prevention System (IPS), anti-virus og anti-malware. Å avdekke eller avsløre forsøk på, eller et vellykket cyberangrep er viktig av flere grunner. En åpenbar grunn er at forsøket kan avverges eller angrepet begrenses slik at skadene reduseres. En annen viktig grunn er at slike hendelser eller nesten-hendelser gir viktig læring og kan føre til at sannsynlighets- og konsekvens-komponentene ved fremtidige risikovurderinger blir mer presise.

2.3 DIGITAL SIKKERHETSKULTUR

I Norge ble begrepet digital sikkerhetskultur første gang beskrevet og kartlagt av Norsk Senter for Informasjonssikring (NorSIS) tilbake i 2016. Digital sikkerhetskultur har blitt sett på som et verktøy, en organisasjonskultur, for effektivitet og etterlevelse av regler og krav og omhandler beskyttelse av digitale verdier fra trusler mot innebygde sårbarheter (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).

Digital sikkerhetskultur kan forstå som,

> *«De verdier, holdninger, antagelser, normer og kunnskaper som mennesker bruker når de forholder seg til digitale verdier»*
>
> (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020)

NorSIS har pekt ut åtte dimensjoner som de mener beskriver digital sikkerhetskultur; fellesskap, styring og kontroll, tillit, risikooppfattelse, optimisme for teknologi og

digitalisering, kompetanse, interesse for teknologi og IT, samt adferdsmønstre (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020). For en nærmere beskrivelse henvises det til norsis.no.

3.0 METODE

En metode er en fremgangsmåte for å løse problemer og identifisere ny kunnskap, alternativt for å teste allerede etablert kunnskap (Dalland, 2017). Kvalitativ metode er, i flg. Malterud (2013), forskningsstrategier som benyttes for å beskrive, analysere og fortolke karaktertrekk, egenskaper eller kvaliteter ved de fenomener som skal studeres. I denne studien blir, som nevnt i innledningen, kvalitativ metode benyttet som eneste forskningsmetode.

I det følgende vil valget av metode forklares, vitenskapsteoretisk perspektiv beskrives og egen forståelse belyses. Deretter vil planleggingen, utførelsen, analysen og verifiseringen beskrives.

3.1 VALG AV METODE

Før man kan velge metode for å belyse en problemstilling, bør man vite hva målet med studiet er. Problemstillingen, sammen med målet, vil kunne avgjøre hvilke evalueringsmetoder som kan gi relevant kunnskap (Myers, 2019). En tydelig problemstilling kan gjøre valget av metode enklere og styrke studiets interne validitet (Malterud, 2017).

Dette studiets formål er å komme til kunnskap om hvordan rederiene gjennomfører cyberrisikohåndteringen og hvordan de involverte opplever prosessen. Målet vil være å gi rederiene noen råd om hva de bør tenke på når cyber risikovurderinger skal gjennomføres. Det vil være de subjektive oppfatninger av opplevelser og samhandling som skal belyses. På bakgrunn av dette anses en kvalitativ tilnærming som egnet til formålet (Kvale & Brinkmann, 2015).

På bakgrunn av de beskrevne vurderinger av tilnærmingsmåte til kvalitativ metode, er en hermeneutisk fenomenologisk tilnærming med semistruktruerte intervjuer valgt som metode for dette studiet.

Det videre kvalitative metodearbeidet er altså gjennomført med en hermeneutisk fenomenologisk tilnærming, i et fortolkende perspektiv. Dette innebærer en fortolkning av informantens mening, med et mål om å oppnå en gyldig og allmenn forståelse av produktet (Myers, 2020).

3.2 FILOSOFISKE PERSPEKTIVER

Innenfor kvalitativ metode finnes ulike filosofiske perspektiver og paradigmer som benyttes for å klassifisere de ulike metodetilnærmingene. Paradigmene gir oss en indikasjon på hva som anses for å være gyldig kunnskap. Det kan være utfordrende å skille dem, men i hovedsak forholder en seg til tre ulike tilnærminger; en positivistisk, en fortolkende og en kritisk (Myers, 2019).

Den positivistiske tilnærmingen har tradisjonelt vært benyttet innfor naturvitenskapen og søker forklaringer gjennom erfaringsmessige kjensgjerninger og vitenskapelige forklaringer. Man antar at virkeligheten er objektiv, målbar og uavhengig av forskeren. Tanken er at man skal teste teorier for å forutse hvordan et fenomen vil utarte seg (Myers, 2019).

En annen kvalitativ tilnærming er den fortolkende, eller hermeneutiske. Den fortolkende tilnærmingen kan ses på som den motsatte av den positivistiske. Med en slik tilnærming ved kvalitativ forskning antas virkeligheten å kunne beskrives gjennom sosiale konstruksjoner som språk, bevissthet og delte meninger. Fenomener skal forstås gjennom de meninger som mennesker tillegger dem. Mening i en kontekst blir essensielt og man anser det som umulig å forstå meningen av en dataenhet, om man ikke forstår den brede konteksten som innholdet i dataenheten er gitt i. Sosial virkelighet er sosialt konstruert, som M. Myers (2019) skriver.

Det tredje tilnærmingsalternativet er det kritiske paradigmet. Det tar utgangspunkt i at vår sosiale virkelighet er historisk konstruert og reprodusert av mennesker. Hovedoppgaven til en kritisk forsker er å utøve sosial kritikk og målet er endre virkeligheten med en forankring i et etisk grunnlag som demokrati, like muligheter og et bærekraftig miljø (Myers, 2019).

Den positivistiske tilnærmingen med antagelser om at virkeligheten er objektiv, målbar og uavhengig av forskeren kan være utfordrende å benytte og akseptere i en undersøkelse hvor en følelse som *opplevelse av en prosess* er et fenomen som problematiseres. Forståelsen av hva informanten legger i begrepet cybersikkerhetsrisikohåndtering og hvilken kontekst følelsen *opplevelse* oppfattes i kan lett bli marginal om man velger en positivistisk tilnærming til vår problemstilling. Den positivistiske tilnærmingens syn på at fakta er nøytrale og meninger er separate fra fakta og kan oppfattes som direkte motstridende når fenomenet *opplevelse* av en cyber risikohåndteringsprosess skal studeres (Myers, 2019).

Den hermeneutiske tilnærmingen til det innsamlede datamaterialet hvor meningen blir bestemt av konteksten, hvor meningen utgjør fakta og man ønsker å belyse en fremvoksende mening innenfor en gitt kontekst kan oppleves som en mer passende tilnærmingen til dette

studiets problemstilling, idet det, basert på informantenes erfaringer, forsøkes belyst hvordan rederiene håndterer cyberrisikoer internt i rederiene (Myers, 2019).

3.3 AVKLARING AV EGEN FORSTÅELSE

Forskerens eget valg av perspektiv vil kunne påvirke hvordan innsamlingen og analysen av informasjon blir gjennomført. På bakgrunn av den erkjennelsen, er det viktig å tenke over refleksiviteten i studiet. Man må ha et bevisst forhold til egen forståelse og at forskerens forståelse kan påvirke forskningsprosessen (Malterud, 2017). Allerede ved utformingen av problemstilling og intervjuguiden, vil forskerens forforståelse, bakgrunnskunnskaper kunne påvirke resultatet av studiet. Det er viktig å ha et åpent sinn, distansere seg fra forutinntatthet og søke etter funn som motbeviser ens egen aperiori.

I dette studiet er det gitt at en informant skal intervjues om sin opplevelse av cyberrisikohåndteringen i rederiet hen er ansatt i. Den valgte kvalitative metoden vil kunne være en god tilnærming for den gitte problemstillingen. Gjennom åpne spørsmål som kan bevisstgjøre informantens egne opplevelser av håndteringsprosessen i rederiet, ligger det et potensiale for å gi forskeren valid informasjon som kan belyse problemstillingen.

Forskerens egne erfaringer, aperiori, teoretisk grunnlag og perspektiv er alle inkludert i hens forforståelse (Malterud, 2017). Som tidligere beskrevet kan dette påvirke forskningsprosessen. Det er viktig at forskeren er bevisst på dette, slik at ikke forforståelsen påvirker resultatet av studiet.

Min bakgrunn er mer enn 20 års erfaring fra politiet, utdanning og erfaring fra data- og cyberetterforskning, overordnet ansvar for cybersikkerhet i et finanskonsern samt risikohåndtering innenfor ulike krise- og beredskapsområdet i offentlig og privat sektor. Jeg har ingen maritim bakgrunn ut over gjennomføring av studiet Ledelse av maritime operasjoner ved NTNU.

3.4 KVALITATIVE FORSKNINGSINTERVJU

Under et studies planleggingsfase bør spørsmål knyttet til innsamling av data og analysemetoder avklares. I studier med bruk av kvalitativ metode, kan ulike teknikker for datainnsamling benyttes. Eksempler på slike teknikker kan være intervjuer, observasjoner,

feltarbeid eller bruk av dokumenter (Myers, 2019). Man kan også anvende en kombinasjon av teknikker i en kvalitativ studie.

Teknikken intervju er ofte benyttet i kvalitative studier hvor forskeren er ute etter å innta informantens perspektiv på verden. Intervjuets oppbygning og gjennomføring kan deles inn i ustrukturerte, strukturerte, semistrukturerte intervjuer av enkeltpersoner eller intervju av fokusgrupper. Strukturerte intervjuer gjennomføres ved at hele intervjuet planlegges og nedfelles i en strukturert plan. Under intervjuet følger man spørsmålene i intervjuguiden slavisk og dermed minimeres forskerens rolle (Kvale & Brinkmann, 2015).

Semistrukturerte intervjuer er en mellomting mellom de to beskrevne teknikkene. I planleggingsfasen utarbeides en intervjuguide. Guiden følges ikke slavisk og det er viktig med oppfølgingsspørsmål. Her tillates improvisasjon hvis informanten forteller om nye forhold ved fenomenet som forskeren ønsker ytterligere belyst, og nye spørsmål kan bli til underveis i samtalen (M. Myers, 2020).

Forskningsmetoden «semistrukturert intervju» er benyttet som datainnsamlingsteknikk i dette studiet. Hensikten med denne metoden er å få informanten til å berette mest mulig fritt om sine erfaringer og opplevelser rundt de spørsmål som stilles, for på den måten å oppnå tykke beskrivelser (Kvale & Brinkmann, 2015).

Gjennom å benytte innsamlingsteknikken *intervju*, er det innhentet primære data. Primære data er data som ikke er innhentet av andre i en annen sammenheng eller studie, men som er «ny» og upublisert. Et slikt datamateriale kan sies å representere noe nytt og unikt (M. Myers, 2020).

Det eksisterer noen fallgruver når innsamlingsteknikken *intervju* benyttes i kvalitativ forskning. Mangel på tillit, relevant inngangsnivå, påvirkning av informant og situasjon og ulikt språk er eksempler på slike fallgruver som forskeren bør være veldig bevisst og som kan utgjøre feilkilder i forskningsarbeidet.

Metoden «intervju» vil, på en annen side, potensielt gi mer og sterkere data enn en kvantitativ forskningsmetode ville gitt når problemstillingen retter seg mot en følelse som *opplevd* risikostyring.

I dette studiet er det tatt utgangspunkt Kvale og Brinkman (2017) sine sju faser for planlegging og utførelse av en kvalitativ intervjuundersøkelse. De 7 fasene er tematisering, planlegging, gjennomføring av intervju, transkripsjon, analyse, verifikasjon og rapportering. De påfølgende delkapitlene følger disse fasene.

3.4.1 Tematisering

Tematisering er fase 1 i undersøkelsen og formålet med undersøkelsen skal formuleres. Det tas utgangspunkt i problemstillingen og formålet med intervjuundersøkelsen er å avdekke hvordan cyberrisikovurderingene gjennomføres, hvem som er involvert og de rederiansatte opplever cyberrisikostyringen i eget rederi.

Avklaringer av spørsmål rundt studiet; hva, hvorfor og hvordan er viktige for planleggingen, gjennomføringen og valg av metode (Kvale & Brinkmann, 2015). Kunnskap om problemstillingens innhold, fenomenkunnskap og metodikk krever tid. Innsikt i eksisterende forskning og teorier om fenomener som ønskes studert vil være viktig for at kunnskapen som søkes gjennom studiet skal ha vitenskapelig verdi. I tillegg til egen utdanning og erfaring er det medgått mye tid til å sette seg inn i ny metodikk innenfor cyber risikostyringsområdet, men også kunnskapservervelse fra andre sektorer innenfor samme tematikk. Dette arbeidet ble gjennomført for også å sikre en best mulig forutsetning for å forstå de ulike informantenes tilnærming til området.

En *prosessopplevelse* og *forståelse av området* kan innbefatte flere komponenter. Erfaring, fenomenkunnskap, tillit, kommunikasjon og en felles forståelse er eksempler på slike komponenter. Selve opplevelsen vil også kunne være forankret og forklart ved de deltagende enkeltindividers egenskaper. Bronstein (2003) presenterer 4 påvirkende faktorer for tverrfaglig samarbeid. Disse 4 faktorene er personlige egenskaper, samarbeidshistorie, strukturelle kjennetegn og faglig rolle. Bronsteins teori er ikke den del av det gitte teorirammeverket, men det er viktig å forstå disse faktorenes betydning for informantenes svar.

3.4.2 Planlegging

Alle 7 fasene må planlegges før intervjuarbeidet igangsettes, for å sikre høyest mulig grad av validitet og reliabilitet. I tillegg vil planleggingen ha mye å si i forhold til hvor godt man klarer å svare på problemstillingen.

Som et ledd i å verifisere at personvernet er i varetatt i denne studien er det sendt en søknad til Norsk Senter for Forskningsdata (NSD). NSD har godkjent studiet og godkjenningen forelå da det første intervjuet ble gjennomført, (vedlegg 1). Informasjonsskriv og samtykkeerklæring er sendt ut til informantene da de ble spurt om å delta, slik at personvern og formelle krav til undersøkelsen er fulgt. Alle informantene som har blitt intervjuet har underskrevet samtykkeerklæring.

3.4.3 Utvalgsbeskrivelse

Ideelt sett burde, som tidligere nevnt, utvalget vært noe større. Selv om utvalg i slike studier sjelden består av mange informanter, blir overførbarheten påvirket i negativ retning når utvalget er begrenset.

I utvelgelsen av rederier og intervjupersoners rolle i rederiene ble det gjennomført en vurdering av hvilke(n) bransje innenfor maritim sektor som skulle undersøkes. Valget stod mellom rederier fra en og samme bransje, f.eks. fiskeri eller offshore, eller rederier som representanter fra ulike bransjer. Valget falt ned på det sistnevnte. Bakgrunnen for utvalget er at IMO ikke stiller spesifikke krav til bestemte bransjer, men det aktuelle IMO kravet som er tema i dette studiet er gjeldende for samtlige rederier, uavhengig av type operasjoner de bedriver. Så lenge de har et krav om å ha et sikkerhetsstyringssystem skal de kunne legge frem en dokumentert cyberrisikovurdering i første revisjon etter 1.januar 2021. Det ble i tillegg sett på som interessant å tilnærme seg rederier fra ulike bransjer for å se om det var en forskjell på hvordan man tilnærmer seg det studerte temaet, uten å tillegge svarene noen overførbarhet til øvrige rederier innenfor samme bransje.

HSSEQ rollen ble valgt fordi BIMCO anbefaler at cyber risikostyringen bør legges til de funksjoner som har ansvaret for sikkerhet i rederiene. En rekke rederier har definert denne rollen som ansvarlig også for cybersikkerhet. Tilgjengelighet til aktuelle HSEQ-ansatte var også viktig for å få gjennomført intervjuene og denne rollen ble vurdert som mer tilgjengelig enn f.eks. daglig leder.

Utvalget i studiet består av 5 informanter med rollen HSEQ i sine respektive rederier og bransjene offshore, vind, passasjer, fiskeri og brønnbåt representert i utvalget.

Et representativt utvalg av ansatte med HESQ-ansvar, gjerne med en spredning i alder, ansenitet i rederiet, utdanning / profesjon og rolle, vil kunne gi forskeren det informasjonsgrunnlaget hen trenger for å gi studiet nødvendig tyngde, sett i forhold til validitet og reliabilitet. På den annen side kan også likhet blant informantenes funksjon eller rolle i rederiene legge til rette for at informantenes kunnskap om praksis og modenhet i sine respektive rederier og derigjennom svar på intervjuspørsmål blir forstått på tilnærmet samme måte.

I dette studiet er fem ansatte stilt spørsmål innenfor fire kategorier og intervjuene hadde en varighet på ca. en time. Det er ikke benyttet noen spørreundersøkelse som grunnlag for utformingen av intervjuspørsmålene, men det ble gjennomført ett dybdeintervju forkant med

en informant som kjenner den maritime næringen godt og som har inngående kunnskap om cyber risikostyringen i næringen.

3.4.4 Intervjuguide

Det ble utarbeidet en intervjuguide (vedlegg 2) basert på Tjora (2018). Intervjuguiden ble fordelt over tre faser; oppvarming, refleksjon og oppsummering. Guiden ble satt opp med emner som skulle dekkes, med tilhørende spørsmålsforslag. Det ble gjort et skille mellom forskningsspørsmål (de spørsmål jeg ønsket svar på) og de spørsmålene som ble stilt til informanten. Spørsmålene rettet til informanten var åpne.

Det meste av tiden ble benyttet til fase to; refleksjonsfasen. Majoriteten av intervjuene var ca. 60 minutter i total lengde. I fase to ble spørsmålene som belyser tematikken stilt. Det er ønskelig at informanten bruker litt tid og reflekterer over sine svar i fase to. Det er også viktig i et semistrukturert intervju at forskeren følger opp med utdypende spørsmål hvis det er nødvendig for å belyse fenomenet best mulig.

Under oppsummeringen ble informantene blant annet spurt om det var noen de hadde tenkt på under intervjuet som var relevant for temaet og som jeg ikke hadde spurt om. Flere av informantene kom med egne betraktninger som var høyst relevant for temaet, og som ikke hadde vært nevnt tidligere i intervjuet.

Det ble gjennomført lydopptak av intervjuene. Opptakene er lagret på et eksternt medium som ikke er koblet til internett og utilgjengelig for andre enn forskeren.

I dette studiet ble det ble ikke kjør pilotundersøkelser etter at intervjuguiden ble utarbeidet og før intervjuene ble gjennomført. En pilotundersøkelse kan imidlertid gjennomføres for å gi en pekepinn på om de formulerte spørsmålene blir oppfattet og besvart på en slik måte at de treffer problemstillingen og fenomenet som søkes studert. Forskeren ser i etter tid at en pilotundersøkelse burde vært gjennomført.

3.5 GJENNOMFØRING AV INTERVJU

Første kontakten med informantene ble opprettet gjennom telefonoppringning, hvor informantene ble informert om det studiet og spurt om de var villige til å motta informasjonsskriv og samtykkeerklæring. Samtlige informanter sa seg villig til å delta under telefonsamtalen.

Informantene mottok eposten med vedlagt informasjonsskriv og det ble i påfølgende korrespondanse avtalt tid og sted for intervjuene.

Informantene ble rekruttert delvis gjennom bruk av eget nettverk og delvis gjennom bruk av Google.

Trygghet i intervjusituasjonen kan være med å legge grunnlaget for vellykkede intervjuer (Tjora, 2018). Fire av fem intervju ble gjennomført på informantenes arbeidssted, mens det femte intervjuet ble gjennomført hjemme hos forskeren. Bakgrunnen for dette valget var ønske om gjennomføring informantenes kjente omgivelser. Man kan imidlertid også argumentere for at informantene kanskje ikke opplever det like trygt å skulle fortelle om negative følelser eller opplevelser knyttet til temaet for studiet samtidig som de sitter på sitt eget arbeidssted. For at rammene i intervjusituasjonen skulle oppleves mest mulig likt av informantene, falt valget ned på den gjennomførte varianten.

De 3 første intervjuene ble gjennomført før jul 2022 og de 2 siste intervjuene ble gjennomført i januar/februar 2023.

Intervjuene ble gjennomført etter intervjuguiden (Kvale, 2017) som ble utarbeidet i oktober 2022. Informantene valgte rom for gjennomføring av intervjuene hos egen arbeidsgiver. Det er ikke kjent for forskeren om informantene hadde informert egen arbeidsgiver om egen deltagelse i studiet. Intervjuene startet med at jeg forklarte litt om bakgrunnen for hvorfor jeg ønsket å gjennomføre et intervju med nettopp hen. Etter at vi hadde snakket litt om temaet, ble lydopptaket startet.

Oppvarmingsfasen ble forholdsvis kort. Informantene fortalte om seg selv, sin bakgrunn og relevant erfaring. Jeg understreket at informasjonen hen fortalte i intervjuet ville bli anonymisert slik at det ikke skulle la seg gjøre å identifisere hen i den endelige rapporten og at ingen andre ville få tilgang til arbeidsdokumentene.

Dialogene ble oppfattet som gode og det ble stilte noen oppfølgingsspørsmål underveis som ikke var nedfelt i intervjuguiden. Det ble etterstrebet å stille åpne spørsmål og la informantene snakke. Siden intervjuene ble tatt opp på lyd, ble det ikke tatt notater underveis. Forskerens oppmerksomhet ble brukt på informantene under intervjuet. For å sikre god flyt gjennom intervjuene, ble det prioritert å la informanten snakke fritt fremfor å styre rekkefølgen på spørsmålene i intervjuguiden slavisk. Intervjuguiden ble derfor benyttet som en sjekkliste, mer enn et manus.

3.6 TRANSKRIPSJON OG ANALYSE

For å gjøre informasjonen som kom frem under intervjuene tilgjengelig for analyse, ble innholdet i lydopptakene nedskrevet. Allerede i denne fasen forringes kvaliteten i informasjonen, idet et nedskrevet intervju ikke klarer å skildre stemning og følelser som oppstår mellom forskeren og informanten (Kvale, 2017). Fenomener studeres i sin egen kontekst, og noe av konteksten kan sies å forsvinne idet et intervju blir transkribert (nedskrevet). Transkriberingen av intervjuene ble gjennomført samme dag, eller i de påfølgende dagene etter at intervjuene ble tatt, noe som kan sies å være en fordel. Ved å gjennomføre transkriberingen kort tid etter intervjuet, kan forskeren fortsatt inneha en hukommelse av noe av den stemningen som var tilstede under intervjuet. Teksten ble skrevet på bokmål og lyder som ikke var meningsbærende ord ble ikke nedskrevet.

Analysemetoden legger grunnlaget for hvordan informasjonsinnsamlingen; intervjuplanleggingen, gjennomføringen og transkriberingen, skal gjennomføres (Kvale, 2017). Det er derfor viktig at valget av analysemetode er godt gjennomtenkt i planleggingsfasen.

I dette studiet er det valgt en hermeneutisk metode; tverrgående systematisk tekstkondensering. Metoden har en fokus på informantens mening med det vedkommende sier og den fungerer godt sammen med egen forforståelse. Tidligere kunnskap skal bygges på, ikke unngås. I en hermeneutisk analyse oppstår kunnskapen gjennom samtalen. Dette er en godt etablert analysemetode innenfor kvalitativ forskning, men det kan være en utfordring å vite når man skal avslutte analyseprosessen.
I en tverrgående analyse blir likhetstrekk, forskjeller og variasjoner i erfaringer, følelser og holdninger fortolket og sammenfattet. Informasjonen blir strukturert i tema og underkategorier som kan beskrive fenomenet. Dette studiet baserer seg på fem informanter. En tverrgående analyse egner seg imidlertid for nye beskrivelser og begreper (Malterud, 2017).

Malterud (2013) foreslår fire trinn i utførelsen av en systematisk tekstkondensering. De fire trinnene er; få et helhetsinntrykk, identifiser meningsbærende enheter (ME), kondensere innholdet i de meningsbærende enhetene og sammenfatte betydningen av dette (Malterud, 2013).

Jeg vil videre beskrive det arbeidet jeg gjorde med den informasjonen jeg hadde etter å ha gjennomført transkriberingen av intervjuet.

3.6.1 Helhetsinntrykk

Jeg startet med å få et helhetsinntrykk av materialet ved å lese gjennom og notere meg stikkord basert på egen forståelse av hva informantene hadde fortalt. Ut fra mine stikkord, satt jeg igjen med fire temaer som kunne knyttes opp mot problemstillingen i oppgaven. De fire temaene var; ressursinvolvering, kartlegging og vurdering, prosesshåndtering og prosessopplevelse.

3.6.2 Identifisering av meningsbærende enheter

I denne delen av analysen skal den relevante delen av teksten skilles fra den irrelevante. De relevante delene i teksten skal kodes til temaene fra forrige trinn i analysen. Gjennom kodingen hentes deler av teksten ut og settes sammen med tekst fra andre deler av dokumentet som omhandler det samme temaet (Malterud, 2017). Jeg jobbet induktivt ved å identifisere de åtte kodene for deretter å se hva disse resulterte i.

Teksten fra transkripsjonen ble nøye gjennomgått på nytt og de meningsbærende enhetene, i form av hele eller deler av setninger, ble strukturert under hver sin passende kode. Kodene ble identifisert til å være intern og ekstern involvering, identifisering av verdier, trusler og sårbarheter, rammeverk og analyseprosess, sannsynlighet, konsekvenser og tiltak, ulike perspektiver / opplevelser, status og modenhet.

3.6.3 Kondensering

Under kondenseringen skal det systematiske hentes ut mening ved å kondensere innholdet i de meningsbærende enhetene som er kodet sammen. Materialet ble fordelt i to sub-grupper for hver kode og de meningsbærende enhetene ble skrevet i en mer generell «jeg-form». De samme uttrykkene som informantene hadde benyttet i sine beskrivelser i intervjuene, ble videreført i nedskrivingen av innholdet i sub-gruppene. Innholdet i sub-gruppene kondenserte jeg ned i et notat som blir brukt i underkapitlet «Sammenfatning». Som et ledd i metodikken, ble det laget «Gullsitater» som illustrerer innholdet i de kondenserte kodegruppene (Malterud, 2013).

3.6.4 Sammenfatning

Kondensatene fra forrige trinn ble skrevet om til en analytisk tekst, i 3.persons-form. Det ble fokusert på at den analytiske teksten skulle være en gjenfortelling fra informanten. Teksten ble vurdert mot «Gullsitatene», og resultatkategoriene fikk sitt endelige navn.

Til slutt ble de analytiske tekstene rekontekstualisert mot transkripsjonen. Dette arbeidet ble gjennomført for å sikre sammenheng mellom funn og de sammenhenger som kom frem under intervjuet (Malterud, 2017).

3.7 VERIFIKASJON – ETIKK, FEILKILDER, VALIDITET OG RELIABILITET

3.7.1 Etikk

Fokus på etiske prinsipper er viktig i all forskning, men kanskje spesielt viktig i bruk av kvalitative metoder. Etisk praksis innenfor kvalitativ forskning blir gjerne definert som den moralske holdningen som involverer respekt og beskyttelse av personer som aktivt samtykker til å bli studert (Myers, 2019).

Det kan tenkes at man kan komme opp i konflikt mellom de respektive rederiene hvor informantene er ansatt på den ene siden og informantens anonymitet på den andre siden, om informantene blir identifisert. Hvis informanten er veldig kritisk til rederiets ledelse og utvalget er begrenset, som i dette studiet, vil en slik risiko kunne være tilstede.

Informantens identitet bør derfor anonymiseres. Det er viktig at informanten ikke får en følelse av at hen har utlevert egen arbeidsgiver men at hen forstår at hens svar vil kunne forbedre rederienes cyberrisikostyring.

3.7.2 Feilkilder

Forskeren vil alltid påvirke prosessen (Malterud, 2017). På den måten kan forskeren også påvirke reliabiliteten i studiet. Vil informanten ha gitt andre svar om forskeren hadde vært en annen, eller om spørsmålene hadde blitt stilt på en litt annen måte, eller med andre ord og begreper? Vil stedet intervjuet gjennomføres på kunne påvirke svarene? Når studiets utvalg er relativt begrenset som her, vil slike potensielle feilkilder kunne bli desto større. Jeg vil tro, uten å ha vitenskapelig belegg for det, at tidsbegrensningene også kan påvirke relasjonen mellom forsker og informant. Dette kan påvirke muligheten for å reprodusere de samme svarene i en lik undersøkelse på et senere tidspunkt. På den andre siden kan tidsbegrensningen også medføre en mindre sannsynlighet for en påvirkning av informanten, sett i lys av at det vil ta noe tid å opparbeide en relasjon. Samtidig er det mulig at en bedre relasjon og kjemi i intervjusituasjonen vil kunne gi informanten den tryggheten vedkommende trenger for å fortelle om hvilke opplevelser hen egentlig har av samarbeidet.

Studiets sårbarhet for feilkilder er til stede. Med informasjon basert på fem informanter, er det en mulighet for at enkelte informanter ikke kjenner rederiets risikostyringsprosess godt. Erfaring i rollen vil her kunne være avgjørende for hvilke svar informanten gir.

3.7.3 Validitet og reliabilitet

Både validiteten og reliabiliteten i studiet kan påvirkes av at utvalget er svakt. Reliabiliteten (reproduksjonsmuligheten av resultatene) kan svekkes når studiet består av informasjon fra fem informanter, alle med samme rolle. Muligheten er til stede for at den enkelte informant lar seg påvirke av forskeren, men sannsynligheten for at fem informanter lar seg påvirke på samme måte av den samme forskeren, er betydelig mindre. Reproduksjonsmuligheten av resultatene, og reliabiliteten, vil derfor kunne være sterkere med et større utvalg av informanter.

Kvale og Brinkmann (2017) skriver at valideringsprosessen må foregå gjennom hele forskningsarbeidet. Det er derfor viktig at forskeren, ikke bare knytter spørsmålet om validitet til et enkelt steg i arbeidet, men under hele arbeidet fra A til Å og har fokus på å sikre så høy validitet som mulig.

Valg av metode som passer problemstillingen er også viktig for validiteten. Dette viser at validitet må være i fokus fra den tidligste fasen i arbeidet. Metodikken ble bestemt tidlig i dette studiet og det må derfor antas at validiteten knyttet til metodikk var ivaretatt. Likevel er det viktig å ha fokus på validitet som en kvalitet ved studiet.

Jeg har ikke selv arbeidet i et rederi eller på sjøen og har derfor ingen egne erfaringer om hva som er «normalt» ved risikovurderinger i maritim sektor. Sannsynligheten er derfor liten for at jeg vil kunne farge konklusjonen i rapporten. Men med erfaring innenfor IKT-sikkerhetsarbeid og data- og nettverksetterforskning, har jeg imidlertid erfaringer som vil kunne påvirke meg i måten intervjuspørsmålene blir utformet på og svarene tolket på.

3.7.4 Generaliserbarhet

Generaliserbarhet, eller overførbarhet, omhandler muligheten for at resultatet av studien kan overføres til andre relevante situasjoner eller organisasjoner Kvale og Brinkmann, 2017). Dette momentet kan, som validiteten og reliabiliteten, påvirkes av flere forhold. Et eksempel på et slikt forhold kan være det noe svake utvalget i studiet. Andre eksempler kan være størrelsen på rederiet, kompleksiteten og oppdragsporteføljen til rederiet osv.

Relevansen i studiet er også viktig å ha et bevisst forhold til. Forskeren må stille seg spørsmål om hva resultatet av arbeidet skal brukes til, hva som er kjent om emnet fra tidligere forskning og om resultatene vil være overførbare til andre interessenter utenfor det utvalget man har benyttet (Malterud, 2017).

Forskeren bør også stilles seg spørsmål om den valgte metoden er relevant i forhold til det fenomen som skal studeres og i hvilken grad den er egnet til å gi svar på de spørsmål som reises i problemstillingen (Kvale & Brinkmann, 2015). Slike spørsmål berører vurderingen av validiteten i studiet. Når disse spørsmål skal besvares under forskerens planlegging av studiet, bør hen ha tilstrekkelig med forhåndskunnskap til å sikre at hen velger den mest optimale metoden. Som tidligere diskutert, vil samtidig denne forhåndskunnskapen også påvirke selve studiet (Malterud, 2017). Forforståelse, selve utvalget i studiet og formuleringen av intervjuspørsmål, er feilkilder som kan påvirke validiteten.

Dette viser hvor viktig planlegging av studiet, bevissthet rundt egen forståelse og feilkilder er for studiets kvalitet.

Når studiets resultat er klart og andre skal vurdere dets viktighet og holdbarhet, er det viktig at studiet skal kunne reproduseres av andre. De metodiske valgene må derfor være synlige og komme frem i avhandlingen (Kvale & Brinkmann, 2015).

4.0 RESULTATER

I dette kapittelet presenteres resultater fra intervju-undersøkelsen. Gjennom analysen av det innsamlede datamaterialet, med problemstillingen som definerende, ble det identifisert fire kategorier med tilhørende subgrupper.

KATEGORIER	SUBGRUPPER
Ressursinvolvering	Intern involvering Ekstern involvering
Kartlegging og vurdering	Identifisering av verdier Trusler og sårbarheter
Prosesshåndtering	Rammeverk og analyseprosess Sannsynlighet, konsekvenser og tiltak
Prosessopplevelse	Ulike perspektiver/opplevelser Status og modenhet

4.1 INVOLVERING

Denne kategorien handler om hvilke roller og funksjoner rederiene har valgt å involvere i cyber risikovurderingsprosessen, både innad i rederiene og av eksterne ressurser. Kategorien er tatt med for å få et bilde av en eventuell fordeling mellom interne og eksterne ressurser.

4.1.1 Intern involvering

Flere intervjupersoner har beskrevet involvering i cyberrisikovurderingene fra øverste ledelsen i rederiet, dog på et overordnet nivå. En HSEQ-ansatt forteller at daglig leder har det overordnede ansvaret. Alle intervjupersonene har HSEQ roller i sine respektive rederier og samtlige forteller at de er involvert i cyber risikovurderingsprosessen. De beskriver videre at operasjonssjefer eller ansatte med lignende roller er med i prosessen med cyberrisikovurderinger, sammen med flere fra landorganisasjonen, blant annet intern IT-avdeling. Flere intervjupersoner anslår at ca. ti intern ansatte er med i cyber risikovurderingsprosessene.

Flere nevner at teknisk sjef, nautikere og maskinsjefer involveres. Noen forteller at HR-avdelingen er involvert, med tanke på behandling av personopplysninger (GDPR).

Gullsitat:

> *Vi har jo en Operasjonssjef og så er det meg som HSEQ manager da, så det er de 2 mest relevante posisjonene men vi diskuterer og snakker med teknisk som er involvert, Technical Manager, og likedan den øverste ledelsen er jo veldig interessert i at vi skal*

ha gjort de riktige vurderingene og selvfølgelig ha en tjeneste som blir levert som er tilstrekkelig.

4.1.2 Ekstern involvering

Alle intervjupersonene forteller at rederiene, dog i ulik grad, har involvert eksterne ressurser som støtte på cyberområdet. En av de intervjuede forteller at rederiet har inngått en avtale om bistand til håndtering av mulige fremtidige cyberrelaterte hendelser. Flere forteller at de mottar trusseletterretning i form av rapporter fra sine respektive eksterne parter. Slike rapporter kan omhandle nettverkstrafikk på fartøyenes nettverk, eventuell mistenkelig aktivitet og eventuelle nye kjente sårbarheter.

Intervjupersoner forteller også at de eksterne partene er involvert på teknisk side, gjennom nettverksskanninger, teknisk identifisering av sårbarheter (sårbarhetsskanning), osv. Flere HSEQ-ansatte beskriver at ekstern part tilbyr ferdige tekniske løsninger og kommer med anbefalinger om etablering av ulike tekniske sikkerhetsløsninger. Slike tekniske sikkerhetsløsninger kan eksempelvis være brannmurer, oppsett og segmentering av nettverk og backup-løsninger.

Noen beskriver at de er helt avhengige av ekstern bistand til gjennomføring av cyberrisikovurderinger. Den eksterne parten er med i hele eller deler av selve cyber risikovurderingsprosessen og den eksterne part blir brukt som en sparringspartner og sikrer kvaliteten på vurderingsresultatene.

Alle som oppgir at de involverer ekstern part i sin cyberrisikostyring forteller at de er fornøyde med tjenestene de får levert.

Gullsitat:

> *Alt IT-oppsett og administrasjon har vi satt vekk til en ekstern part fordi vi ikke har kompetansen her på huset. Vi har satt vekk det som går på brannmur og oppsett av nettverk ombord og sånn.*

En av intervjupersonene opplyser at den eksterne parten ikke berører eller er involvert i de operasjonsteknologiske systemene ombord i fartøyene og at dette ikke inngår i avtalen eller leveransen som de har kjøpt. En annen forteller at rederiet har tatt den eksterne parten inn i organisasjonsbeskrivelsen i rederiets ISM som supporting. Den eksterne parten er altså en del av organiseringen i rederiets sikkerhetsstyringssystem. Siden de setter ut deler av rederiet sikkerhetsorganisasjon kjører de revisjoner hos den eksterne part.

4.2 KARTLEGGING OG VURDERING

Denne kategorien omhandler hvordan rederiene i praksis kartlegger enheter ombord som de mener kan bli rammet av en cyberhendelse og hvordan de blir kjent med trusler og sårbarheter knyttet til de enhetene de identifiserer.

4.2.1 Identifisering av verdier

En av de HSEQ-ansatte forteller at rederiet har en generell asset-liste over alle komponenter og at mye er likt på fartøyene. Listen blir sendt ut til fartøyene sammen med en fartøyspesifikk oversikt. Hvis det for eksempel er gjennomført endringer i serveroppsett ombord siden forrige identifisering, blir de ansvarlige ombord bedt om å gå gjennom oppsettet en ekstra gang for å være sikker på at de har fått med seg alt.

Andre HSEQ-ansatte forteller at de har identifisert de utstyrskomponentene som er knyttet opp mot nettverk og som er mulige å logge seg på. Identifiseringsarbeidet er gjennomført av ekstern part. Enkelte intervjupersoner beskriver det som vanskelig å identifisere OT-komponenter som f.eks. ECDIS ved nettverkssøk. Noen av de intervjuede beskriver at meste av OT-komponenter ble identifisert da fartøyet ble bygd gjennom kravspesifikasjoner og utstyret er verifisert og testet mot klasseregler. Det beskrives videre at rederi nå har startet med å identifisere hvilke komponenter som er i bruk ved de ulike operasjonene fartøyene er involvert i. Hensikten er å forsøke å avdekke hva som er oppkoblet og gitt remote tilgang, med eventuelle eksponerte cyberrisikoer, under de enkelte operasjonene fartøyene gjennomfører.

En annen HSEQ-ansatt forteller at rederiet har benyttet IT-leverandører og OT-leverandører for det utstyret som står ombord, sammen med spesifikasjonslistene som er ombord på fartøyene, for å få en oversikt over digitalt utstyr, både på IT og på OT. Spesifikasjonslistene ble opprettet da de kjøpte båtene, men ble laget først og fremst for å få en oversikt abonnement og leverandører for de ulike særsystemene. Hver enkelte båt er kartlagt i detalj for å få en oversikt over leverandører og systemer.

Gullsitat:

> *Vi har kjøpt båter med systemer så vi må kartlegge hva vi kjøper. Det er abonnement og det er koblinger mot leverandører av de ulike sær-systemene, så det er naturlig at det i en slik prosess blir en bevisstgjøring.*

En av intervjuperson forteller at de benytter en nettverksskanning for å se hva som er online. Hen er fornøyd med resultatene fordi de også viser hvilke komponenter som tidligere har vært koblet til nettverket. På den måten får rederiet identifisert noen sårbarheter. Den HSEQ-ansatte vurderer denne metoden som reaktiv.

En av de intervjuede beskriver at rederiet har utarbeidet prosedyrer for identifisering av enheter, basert på BIMCO Guidelines. Rederiet har benyttet utstyrskategoriene som BIMCO har anbefalt for å få en oversikt over OT komponenter ombord i fartøyene. Grunnen til at de har kategorisert komponentene er at de har ønsket å gjøre arbeidet mer forståelig for de som skal gjennomføre cyberrisikovurderingsprosessen. De involverte har gått gjennom alle komponenter de kan finne ombord innenfor hver kategori, identifisert kjente sårbarheter og eksisterende barrierer. Det er også kartlagt hvem som har tilganger til de ulike systemene, både interne, eksterne og remote. Den intervjuede har en oppfatning av at IT-delen er mye vanskeligere fordi det der trengs mer spesifikk kompetanse. Resultatet har blitt at rederiet har en separat IT-risikovurdering.

4.2.2 Trusler og sårbarheter

En av de HSEQ-ansatte beskriver at den interne trusselen kanskje er den største for dem, og å avdekke utro tjenere derfor er viktig. De er redde for alt som kan forstyrre operasjonene og stanse utstyr ombord som er operasjonskritisk. Løsepenge-trusselen er noe de også er bekymret for i dette rederiet.

En av de andre intervjuede forteller at de i snitt har 60-70 mann ombord på de enkelte fartøyene til enhver tid. Hen forteller at de ikke har hatt noen konkrete cyberrelaterte hendelser, men beskriver at de opplever utfordringer med minnepinner og andre lagringsenheter.

En annen HSEQ-ansatt forteller at de ikke har definert noen trusler på cyberområdet, fordi de har lite følte trusler. Trusler om økonomisk vinning eller folk som bare vil lage faenskap beskriver hen som konstant. Industrielle trusler mot egen informasjon har ikke rederiet ansett som veldig stor. Hen beskriver en tendens til å tegne et skremselsbilde.

Gullsitat:

Jeg hadde nylig en skipper som, der ene plottersystemet var gått ned uforklarlig, med en gang fikk en mistanke om at noen hadde vært ombord og tappet informasjon og satt systemet i en mode der det ikke var brukelig lenger.

En av de andre intervjupersonene forteller at det er mannskapet som eksponerer fartøyet når de åpner for remote tilgang for eksterne brukere med lovlig tilgang. Samtidig forteller hen at det er aktivister mot den næringen de driver service for som også er den største trusselen mot deres egen næring. Pr. i dag driver disse aktivistene ikke med voldelige eller sabotasjeaktiviteter, men de jobber mer mot det politiske nivået.

En intervjuperson forteller at trusler kan være enkeltpersoner, det kan være nasjoner eller leverandører. Truslene finnes der ute, men de vet egentlig ikke så mye om dem og rederiet har ingen indikasjon på direkte trusler i dag. Trusler kan også være en enkelt kunde som kommer ombord i båten og logger seg på det offentlige nettverksområdet. Kunden kan laste ned ondsinnet programvare som igjen kan forsøke å koble seg opp på skipets systemer. Intervjupersonen forteller at de mottar trusselinformasjon fra ekstern part som er gitt en TLP-verdi («trafikklys»-verdi). De deler informasjonen bredt internt i rederiet, men er den gradert rødt er det kun enkelte interne som får tilgang til informasjonen.

Flere av intervjupersonene trekker frem at utstyr med remote tilgang er det mest sårbare utstyret som er ombord. En HSEQ-ansatt forteller at mulighetene for feilsøking og endringer eller oppdateringer av programvare kan være årsaken til at det gis remote tilgang. En annen av intervjupersonene forteller at de har hatt en runde med oppgraderinger av ECDIS, men mener det ikke har relatert til cybersikkerhet men mest navigasjonssikkerhet.

Andre intervjupersoner forteller at de ser at kritikaliteten knyttet til OT-systemene er ganske stor, men at de er veldig avhengige av leverandører som til stadighet skal inne eller ombord. Rederiet har innført en rekke kontrolltiltak for å være i mål på dette området. De har identifisert sårbarheter i systemer og vurdert eksisterende barrierer. Interne diskusjoner har oppstått i den delen av vurderingsprosessen som har omhandlet identifisering av sårbarheter. Intervjupersonen forteller at rederiet har hatt nytte av at ansatte har stilt kritiske spørsmål etter at de har opplevd hendelser eller avdekket potensielle sårbarheter. Flere ganger har dette medført forbedringsforslag som er innsendt til vurdering.

En av intervjupersonene forteller at datakommunikasjonen blir bedre og bedre, med stadig høyere hastigheter og mer stabil levering. Følgen av bedre nettverkstjenester er at rederiene kan lene seg mer på onlinebaserte tjenester som igjen fører til at de kan sette bort ansvaret. Det samme rederiet har definert dataflyten til og fra fartøyet som noe av det mest sårbare. Hvis forbindelsene faller ut, vil de miste tilgang til de ulike onlinebaserte tjenestene. En av de andre intervjupersonene forteller at de kun har en enkelt datakommunikasjonslinje inn til fartøyet og at de derfor er sårbare for jamming.

En HSEQ-ansatt angir mangfoldigheten i systemene både som en styrke, idet det er vanskelig å slå ut en alt på en gang, men at dette også innebærer en sårbarhet. Det er flere proprietære systemer ombord, og det er ikke alltid at de på land får vite at en ny funksjonalitet blir aktivert og tatt i bruk. Leverandører kommer ombord og gjør arbeid på systemer. Etter endt arbeid mottar besetningen eller landorganisasjonen bare en melding om at maskina er oppgradert og «up to date». Siden det er så mange leverandører og så mange dippedutter, har de sett på dette som en av de største sårbarhetene.

Brukergrensesnittene og de ulike systemenes koblinger og avhengigheter blir av et intervjuobjekt påpekt som en sårbarhet i seg selv. De ansvarlige mister overblikket og vet ikke hva som henger sammen med hva.

En av de andre intervjupersonene beskriver at de får overlevert en statusliste over sårbarheter fra den eksterne parten og at de på den måte mener å ha en oversikt over de kjente sårbarhetene.

Noen av intervjupersonene beskriver at IT- og OT-systemene ombord henger sammen og at det er mulig for rederiet, servicepersonell og leverandører å fjernstyre en masse ting ombord i båtene. Hensikten er at de hurtig skal kunne koble seg på remote og gjøre endringer i programvare og slike ting.

En HSEQ-ansatt forteller at de har sett på IT- og OT-utstyr for å se hvor risikoene ligger og at de har vurdert OT-systemet som avskjermet. Rett nok er det et IT-nettverk som også gjør det mulig å hacke OT-systemer. Den intervjuede mener rederiet har god kontroll på leverandører som logger seg på og hva leverandørene gjør gjennom den tjenesten de leverer. IT-nettverket oppleves derimot som vanskeligere å kontrollere, siden mange flere er involverte der.

En HSEQ-ansatt beskriver det som litt vanskelig å se hvordan det ene systemet kan påvirke det andre. På OT-siden har de hatt med teknisk og operasjonelt personell i sårbarhetskartleggingen men på IT-siden er det overlatt til IT-avdelingen, både på setup og på hardware.

Gullsitat:

> *Det er produsenter som logger seg på, men vi mener at vi har relativt god kontroll gjennom den tjenesten den eksterne parten leverer. Gjennom deres tjeneste har vi full oversikt over hvem som logger seg på, hvem som er inne og hva de gjør. Det er kanskje litt vanskeligere å kontrollere IT. Der er det mange flere involvert.*

4.3 PROSESSHÅNDTERING

Denne kategorien forsøker å belyse hvilke hjelpemidler eller rammeverk rederier benytter som støtte, for å sikre at cyberrisikovurderingene blir gjennomført på en metodisk og strukturert måte. Videre omhandler kategorien konsekvensvurderinger og hvordan rederiene kommer frem til hvilke tiltak som skal implementeres for å redusere identifiserte cyberrisikoer til akseptable risikonivåer.

4.3.1 Rammeverk og analyseprosess

Noen av de HSEQ-ansatte forteller at de har benyttet BIMCO (BIMCO et.al., 2021) som et rammeverk for å ha en struktur på cyber risikovurderingsarbeidet i rederiet. Tre av intervjupersonene opplyser at de støtter seg til klasseselskapenes veiledninger og regler. En av dem forteller at de også har benyttet IMOs guidelines (IMO, 2017) men at klienter og kunder har egne krav som indirekte påvirker rederiets arbeid på området. Klienter og kunder har vist til BIMCO sine guidelines.

Gullsitat:

> V*i har jo IMO sine guidelines, kanskje de som ligger mest i bunnen for disse tingene her da, og så blir vi konfrontert med kundene sine systemer og krav så de er jo medvirkende her til å danne et kravsett som vi forholder oss til. Noen kunder bruker fra BIMCO…*

En av intervjupersonene forteller at cyberrisikovurderingene startes av nautikere og chief ombord på det enkelte fartøy og at de sender vurderingene til landorganisasjonen med forslag

tiltak. På land blir vurderingene gjennomgått og om nødvendig blir vurderingene justert og nye forslag til tiltak kan bli tilføyd. Cyber risikovurderingen blir deretter sendt ombord til de respektive fartøyene igjen for kommentarer før den er komplett. Vurderingene blir så lagret ned i et elektronisk system og alle vurderingene deles mellom fartøyene i rederiet. På den måte fasiliterer rederiet for erfaringslæring mellom fartøyene. Rederiet har definert et akseptnivå for risikoer og de benytter fargekoder for å visualisere risikonivåer. Cyberrisikovurderinger blir gjennomført en gang pr. år om det ikke oppstår endringer som krever en umiddelbar revurdering.

En annen intervjuperson påpeker at gjennomføring av risikovurderinger går på kompetanse. Når de har gjennomført cyberrisikovurderinger har det vært på et overordnet nivå. De har fått innspill fra en ekstern part på sin vurdering av behandlingen av identifiserte cyberrisikoer. Intervjupersonen forteller at de har benyttet frekvens og konsekvens for å regne seg ut til en risiko og at det er den økonomiske konsekvensen som er den verste for dem. Rederiet har etablert en policy for cybersikkerhet, hvor de har nedfelt hva som er viktig for rederiet og noen mål på cybersikkerhetsområdet. Intervjupersonen forteller at de fortsatt har en del gule cyberrisikoer, til tross for at de har satt inn tiltak for å redusere risikoene. Cyberrisikovurderingen ble gjennomført før tjenestene fra ekstern part ble kjøpt inn, men vurderingen ble ikke dokumentert på en god måte. Risikovurderingen var mer basert på samtaler internt før de kjøpte inn en pakke med tekniske løsninger fra den eksterne parten.

En tredje intervjuperson beskriver at de har startet på en dokumentert risikovurdering, men at den ikke er fullstendig. På landsiden føler de ansvarlige at de er ivaretatt gjennom en innkjøpt skybasert tjeneste fra en ekstern part. Intervjupersonen forteller at rederiet har en plan på hvordan de vil legge opp arbeidet på cybersikkerhetsområdet og at de ønsker å definere dette inn i eksisterende rutinebeskrivelser.

Gullsitat:

> *Det som i bunn og grunn ligger i de skybaserte tjenestene er det at du kjøper en slags total driftsgarantipakke på et eller annet.*

En av de intervjuede forteller at de har hatt med ekstern part i selve risikovurderingsprosessen. Den eksterne parten har kartlagt farene og beskrevet risikoer med farer basert på sannsynlighet og konsekvens. Kartlegging har foregått ved hjelp av en

nettverksskanning for å se hva som er online på det respektive nettet og deretter scoret funnene (komponentene) basert på en 5 ganger 5 matrise. Komponenter knyttet til navigasjonssystemet (f.eks. ECDIS) er scoret høyt på konsekvens fordi det er kritisk i forhold til å kunne navigere trygt. De har så lagt inn en sannsynlighet for at komponenten skal bli utnyttet. Internt i rederiet har de gjennomgått den eksterne cyberrisikovurderingen og justert den basert på egen kjennskap til systemene og redundansmuligheter. Rederiet har sagt at de skal gjennomføre skanning med en påfølgende risikovurdering årlig.

Den femte intervjupersonen beskriver at de har en filosofi i bunn som har gitt bakgrunn for den digitale sikkerhetspolitikken. De har ikke kvantifisert cyberrisikoene sine, men vurderer sannsynlighet og konsekvens og ender opp med en risiko basert på det. Risikoen beskrives som grønn, gul eller rød. De ansvarlige har sett på ulike tilnærminger til cyberrisikovurderingen og tatt kontakt med en ekstern part for å få innspill til hvordan de burde gå frem. De ble anbefalt å splitte trusseldelen i sannsynligheten opp i intensjon, kapabilitet og mulighet. Denne tilnærmingen ble opplevd som vanskelig å benytte for de ansatte som skulle gjennomføre vurderingene. Rederiet benytter en 1-5 og A-E gradering for å beskrive sine identifiserte cyberrisikoer.

4.3.2 Sannsynlighet, konsekvenser og tiltak

Noen HSEQ-ansatte beskriver at de benytter en matrise med forhåndsinnlagte sannsynligheter. De henter et tall fra denne matrisen som skal representere sannsynlighet og legger ganger denne sammen med en konsekvensfaktor for å få frem risikoverdien.

En HSEQ-ansatte forteller at konsekvensen av en cyberhendelse kan være stor selv om de i utgangspunktet ikke vurdere seg selv til å være i målgruppa for en trusselaktør. Hen forteller at de ikke har så mange forretningshemmeligheter som f.eks. skipsdesignere eller verft har. Rederiet er mest engstelig for at den operasjonelle driften skal stanse. Hvis noen kommer fra utsiden og kan manipulere data eller informasjon er de «ute og kjøre».

En av intervjupersonene forteller at de økonomiske konsekvensene kan bli veldig store om en kritisk enkeltkomponent i produksjonssystemet ombord blir slått ut, pga. en feil eller med vilje. Om enkeltkomponenter på navigasjonssiden blir slått ut trenger ikke konsekvensen å bli like alvorlig fordi de har manuelle alternativer. Hen beskriver at hele næringen, fra myndighetenes side, er bestemt å være transparent og at svært mye informasjon derfor er gjort tilgjengelig.

To av de HSEQ-ansatte forteller at deres rederier ikke gjennomfører en konfidensialitets-, integritets- eller tilgjengelighetsvurdering når de gjennomfører cyberrisikovurderinger.

En av intervjupersonene forteller at Vesselmanagere på land skal være involvert før eksterne får remote tilgang ombord i båtene. Ansatte ombord kan ikke selv ta beslutningen og gi eksterne remote tilgang. Samtidig er systemene satt opp slik at kun et fåtall ombord i båtene har tilgang. Underleverandører varsles når det er åpnet for remote tilgang for dem. Tilgangene er fysisk stengt når det ikke er behov for remote tilgang og passordbeskyttet når de er åpne. Ingen systemer står permanent oppkoblet for remote tilgang. IT-nettverkene ombord er segmentert. Maritimt crew, fartøy og klienter har hver sine egne nettverk. Hen forteller at de har innført pålegg om utlogging av systemer, låsing av pc når man forlater dem, forbud mot deling av passord, forbud mot bruk av ukjente minnepinner, og rederiet presiserer viktigheten av at alle forstår mulige konsekvenser av ikke å gjøre det de er pålagt.

En HSEQ-ansatt forteller at den eksterne parten leverer dedikerte sikkerhetssystemer, tilhørende programvare, backup-løsninger og brannmurer. Hen forteller at de tekniske løsningene er ekstremt viktige men at også den interne opplæringen for å vekke oppmerksomhet på at det er den som trykker på tastaturet som gjerne åpner døren inn. Intervjupersonen forteller at rederiet har innført tilgangsstyring, hvor enkelte har endringstilganger mens andre kun har lesetilganger. De har laget en cyber security guideline som sier noe om hvordan folk skal forholde seg til påloggінger og tilgang. Man skal ikke forlate pc fritt tilgjengelig, men logge av. Rederiet har også lagt inn en ti-punkts Cyber Security tips i tillegg til å ha segmentert nettverk. Rederiet må imidlertid overlate til den eksterne parten å bestemme eller vurdere om dette er tilstrekkelig, basert på det rederiet har angitt som kritisk. Intervjupersonen beskriver at det er her de er i ferd med å glippe, fordi de ikke kan vurdere kvaliteten i leveransen. Den eksterne parten må komme med innspill på relevante ting som de kan levere, blant annet gjelder dette OT og sikringer av påloggінger. Skulle de bli utsatt for et cyberangrep kan det være at rederiet må gjøre noe, men inntil den tid får de tro at det den eksterne parten gjør er tilstrekkelig for at unngå at rederiet blir offer for et cyberangrep.

En av de andre intervjupersonene forteller at de har gått for anerkjente skybaserte løsninger fra dag en som et tiltak mot uønskede hendelser.

Gullsitat:

Lykkepillen her er skybaserte løsninger, jeg vet ikke hva de gjør oppi skyen der jeg, he he he!

Den intervjuede forteller at rederiet har vært veldig opptatt av at de valgte skyløsningene skal være fra norske leverandører for å være ganske trygge på at dataoppbevaringen skjer i kontrollerte former. Unntaket er Microsoft som har en dominant posisjon og som det derfor er vanskelig å komme utenom.

Ombord har de en rekke tekniske sikringstiltak og prosedyrer for hvem som skal ha tilgang til kritiske drifts- og styringssystem ombord. Det foreligger veldig strenge brannmurregler for nettverkstrafikken. Prosedyrene beskriver på rollenivå hvem som er gitt hvilke tilganger, hvem som kan koble seg remote til båten, osv. Prosedyrene beskriver også kontroll av redundans og backup-rutiner.

Gullsitat:

Det skal gå kortest mulig tid fra plunder og heft til at vi er oppe og gå igjen på et godt nivå

Skipperne mottar hvert døgn en oversikt over hvilket nettverksutstyr som har vært tilkoblet nettverket ombord, bruk av datamengder osv. Det er et veldig strengt regime på databruk. Mange praktiske ting er på plass, men fra rederiets side mangler den enhetlige felles dokumenterte tilnærmingen.

En HSEQ-ansatte forteller at de har valgt å sette ut arbeidet. Nettverkssegmentering, backup-rutiner og monitorering er eksempler på tiltak som den eksterne parten var valgt å implementere. Klientene ombord benytter stort sett eget 4G-nett. I tillegg har den eksterne parten valgt å kode software killswitcher slik at de kan stenge av internett til de forskjellige enhetene, i tillegg til fysiske nøkler som bryter koblinger på eldre nett.

En av de intervjuede forteller at rederiet har valgt å benytte inngåelse av arbeidskontrakter som et sikringstiltak. Alt arbeid som medfører et behov for tilgang er inkludert og beskrevet i en kontakt. Svært mye av vedlikeholds- og servicearbeid krever tilkobling, og dette har vært et diskusjonstema internt. Hvis noen skal ha remote tilgang skal det også gis beskjed om at de er innlogget på nettverket ombord. For øvrig beskrives bruken av remote tilgang som svært begrenset. Siden det meste av tilgangen krever fysisk tilstedeværelse, anser intervjupersonen tilgang etter at ansettelsesforhold er avsluttet å være godt håndtert.

Servicepersonell kan komme ombord når de ligger i en havn. De styrter rett inn, kobler fra osv. Kontrakten, eller arbeidstillatelsen, krever at intet arbeid skal foregå uten at kapteinen eller maskinsjefen har fått beskjed. Rederiet har opplevd at det er blitt gjort endringer som har fått konsekvenser for propulsjon som kapteinen ikke var klar over. Intervjupersonen beskriver det som en stor risiko for drift og at denne hendelsen medførte et stort fokus på dette risikoområdet.

Den HSEQ-ansatte forteller også om nettverkssegmentering og stort fokus fra IT-avdelingen på å skille IT-nettverk fra OT-systemene.

I tillegg til tekniske og prosedyremessige tiltak har rederiet innført Nanolearning for ansatte med informasjonssikkerhetsopplæring og GDPR-krav.

4.4 PROSESSOPPLEVELSE

I denne kategorien blir intervjupersonenes subjektive opplevelse av cyber sikkerhetsområdet belyst. De HSEQ ansatte sine perspektiver på temaet, opplevelser av prosessen med cyber risikovurderinger samt deres egen oppfatning av rederienes status og modenhet i forhold til de krav IMO har stilt på cyberområdet.

4.4.1 Ulike perspektiver / opplevelser

Noen intervjupersoner opplever at rederiets håndtering av cyberrisikovurderinger er god. De forteller at rederiene har et system som er godt innarbeidet, samtidig som at de er helt avhengige av eksterne ressurser. Cyberrisikoområdet blir tatt på alvor i hele rederiet og ledelsen legger til rette for at cyberrisikoene kan reduseres. Hendelser i Europa det siste året har bidratt til økt fokus på cyberområdet og det kommer høyere og høyere på agendaen. Det er ingen som sier imot hvis man i dag argumenterer med sikkerhet. Samtidig ønsker flere HSEQ-ansatte å ha enda mer ressurser tilgjengelig for å håndtere cyberrisikoer.

Gullsitat:

> *Det er et stadig fokus på det, men så er det jo sånn med oss mennesker at så lenge du ikke har opplevd noe, ikke sant, så føler du deg kanskje sånn nogen lunde trygg da*

En av de intervjuede beskriver at det er ukomfortabelt på den måten at verden har blitt ganske uoversiktlig. En annen har en opplevelse av at det bremser en masse utvikling fordi rederiet blir avhengige av å ha, eller få inn, ny kompetanse. I mellomtiden står leverandører på vent for å få inn sine system, fordi de må i gjennom en protokoll slik at de ikke blir sperret ute.

En HSEQ-ansatt opplever cyberrisikoområdet som ekstremt omfattende. De er vant med å risikovurdere, implementere og sjekke alt av operasjoner, men dette feltet er ekstremt avansert, både på IT-siden og på de tilfeldige faktorene med folk, vilje og det der. Intervjupersonen beskriver en følelse av ikke å ha kontroll.

Gullsitat:

> *Så det å føle at vi har kontroll på dette her, det tror jeg ikke. Kanskje noen føler at de har kontroll, men jeg føler det ikke.*

4.4.2 Status og modenhet

En av de HSEQ-ansatte forteller at rederiet laget en cyber security prosedyre tilbake i 2018 og at den har vært revidert flere ganger. Den har vært gjenstand for revisjoner av klasseselskapet under den årlige gjennomgangen. Revisjonene har ført til ytterligere forbedringer.

En av de andre intervjupersonene forteller at det har vært et ganske høyt fokus på cyberrisikoområdet ved klasse- og system-revisjoner. De retningslinjer og guidelines som kom fra IMO tilbake i 2017 var i hovedsak rettet mot at det skulle gjennomføres cyber risikovurderinger og at man skulle gjøre sårbarhetsanalyser for å finne ut hvor man stod. Disse retningslinjene og guidelines var ikke veldig spesifikke og man ble ikke pålagt å gjøre veldig mange tiltak. Dette var for å vekke oppmerksomhet på cyberutfordringene. Hen forteller at rederiet har gjort en overordnet vurdering av hva de trenger. Siden de ikke har intern kompetanse på området, har de satt det ut til en ekstern part. Den eksterne parten har kommet med en pakke, basert på sine erfaringer og rederiets ønsker.

En intervjuperson forteller at de har startet på arbeidet med cyberrisikovurderinger. De har en plan for hvordan de skal gå frem og har etablert en policy, men de har ikke kommet i mål.

Andre HSEQ-ansatte forteller at ISM krever at man skal identifiserer trusler. De har en sikkerhetspolitikk og har definert cyber security som en fare. Det er etablert prosedyrer om digital sikkerhet som spesifiserer ansvar på land og på sjø og hvordan disse risikoene skal håndteres. Prosedyrene inkluderer seilende personell, ledelse og funksjoner i land og leverandører.

En intervjuperson forteller at klasseselskapet har bekreftet at cyberrisikohåndteringen innad i rederiet er ganske godt innarbeidet. Samtidig opplever de at mange kunder og større, spesielt internasjonale, klienter har strengere krav til cybersikkerhet enn IMO. Kundene forventer at dette er på plass, og derfor går rederiets prosedyrer lengre enn det som står i IMO.

Noen av intervjupersonene forteller at de har kommet i gang og fått cyberrisikovurderinger inn i styringssystemet, i tillegg til å ha koblet på ansvarlige. En beskriver at det er utfordrende å få kunnskap og drift til å henge sammen.

Gullsitat:

> *Det er der utfordringen ligger, i det å koble hele veien, kunnskap og drift. Alt skal henge i hop.*

4.5 OPPSUMMERING

I dette kapittelet har det blitt presentert fire kategorier, med til sammen åtte subkategorier. Resultatene som her er presentert forsøker å belyse problemstillingen:

«*Hvordan utfører rederiene cyber risikovurderingene, hvilke roller er involvert og hvordan oppleves prosessen av de HSEQ-ansatte?*»

Resultatet fra undersøkelsen viser at rederiene har litt ulik tilnærming til selve utførelse av cyber risikovurderinger. Enkelte rederier har et bevisst forhold til et rammeverk og støtter seg til guidelines, mens andre har en litt mer tilfeldig utførelse og ikke innehar ikke det samme fokuset på en strukturert tilnærming til cyber risikovurderinger.

De HSEQ-ansatte som er intervjuet i dette studiet har opplyst at det i stor grad er involvert både interne og eksterne ressurser når det utføres cyber risikovurderinger i rederiene. Bakgrunnen for denne ressurskombinasjonen er en manglende intern kompetanse på cyberområdet i flere rederier. Den eksterne ressursen involveres gjerne inn mot den tekniske tilnærmingen til sårbarhetskartlegging, identifisering av enheter og systemer og implementeringen av tekniske sikringstiltak.

De HSEQ-ansatte er litt delt i opplevelsen av cyber risikovurderingsprosessen. Flere av de intervjuede forteller at de er usikre, at cybersikkerhetsområdet føles ukjent og komplisert. Andre har fått eksterne bekreftelser på at rederiet er på riktig vei, kanskje fått noe økt selvtillit og motivasjon.

5.0 DRØFTING

I dette kapittelet drøftes resultatene fra den gjennomførte undersøkelsen mot teorier beskrevet i teorikapittelet. Delkapitlene her tilsvarer subkategoriene under ressursinvolvering, kartlegging og vurdering, prosesshåndtering og prosessopplevelse. Avslutningsvis blir det presentert en oppsummering.

5.1 INTERN INVOLVERING

Funn i studiet viser at alle HSEQ-ansatte forskeren har hatt kontakt med, kjenner til IMO`s krav til cybersikkerhet som kom i 2017, med virkning fra 2021 (IMO, 2017). Samtlige intervjupersoner oppgir at de selv, som følge av sin rolle i rederiet, er involvert i arbeidet med cyber risikovurderinger.

I følge BIMCO (BIMCO et.al., 2021) vil en effektiv cyber risikostyring hvile på en tydelig fordeling av ansvar og oppgaver internt. Plassering av ansvar og oppgaver knyttet til cyber risikostyringen vil fungere best om den samsvarer med det vanlige kommando-hierarkiet (BIMCO et.al., 2021). Rederiene har utpekt ansvarlige for å sikre at kravene til cyber risikovurderinger blir fulgt og dette ansvaret har blitt lagt til HSEQ-rollen i rederiene. Antallet internt ansatte som er involvert i arbeidet med cyber risikovurderinger varierer mellom rederiene, og er gjerne avhengig av rederienes størrelse. Hos flere av rederiene er daglig leder, teknisk ledelse, IT og HR involvert.

Risikovurderinger knyttet til operative virksomhet er noe den maritime næringen har bedrevet veldig lenge. Historisk kan risikovurderingene gjerne være knyttet til vurderinger av utilsiktede uønskede hendelser. Utfordringene med cyber risikovurderinger kan være at man skal vurdere sannsynligheten for at noen med viten og vilje utsetter et fartøy for en uønsket hendelse.

Resultatet fra undersøkelsene i dette studiet viser at cyberområdet kan være utfordrende og virke komplisert for de som har ansvaret for å gjennomføre slike risikovurderinger. Den interne cybersikkerhetskompetansen i rederiene er begrenset idet det digitale cyberdomenet er relativt nytt og domenet bærer preg av høy kompleksitet. Flere av intervjupersonene beskriver at risikoarbeidet på dette området oppleves som krevende, noe som vil ytterligere behandlet senere i dette kapittelet.

På bakgrunn av i funn som er gjort i dette studiet er det grunn til å tro at flere velger å plassere ansvaret for cyber risikostyring i rederiet til HSEQ-rollen. Mange rederier mangler intern cybersikkerhetskompetanse og har, på bakgrunn av krav i IMO 2021, ikke annet valg enn å søke bistand hos eksterne parter for å tilfredsstille kravene. Det er grunn til å tro at dette er gjeldende på tvers av områder som fiskeri, supply, osv.

5.2 EKSTERN INVOLVERING

Resultatene viser at alle rederiene i undersøkelsen har involvert eksterne ressurser i arbeidet med cybersikkerhet. Graden av ekstern involvering varierer imidlertid rederier imellom. Enkelte HSEQ-ansatte beskriver at deres rederi er helt avhengige av ekstern bistand for å kunne gjennomføre cyber risikovurderinger, mens andre oppgir at de kun mottar trusselinformasjon fra en ekstern part.

BIMCO (BIMCO et.al., 2021) beskriver at, avhengig av rederiets kapabilitet til å gjennomføre cyberrisikovurderinger selv, involvering av tredjepart kan vurderes. Noen intervjupersoner forteller at de har involvert ekstern part ved teknisk identifisering av sårbarheter, gjennomføring av cyber risikovurderinger men også ved utvelgelse og implementering av sikringstiltak. På bakgrunn av dette er det grunn til å tro at identifiserte tekniske sårbarheter er redusert gjennom implementering av adekvate tiltak. En slik tilnærming kan innebære noen utfordringer for rederiene.

Avhengigheten av ekstern part på grunn av mangel på intern kompetanse *kan* sette rederiene i en posisjon hvor de er prisgitt kompetansen og kunnskapen til den eksterne parten. De foreslåtte løsninger (tiltak) kan være redusert til de tjenestene den eksterne parten kan levere per tiden. Det vil kunne være en reell risiko for at rederiet ikke får informasjon fra den eksterne parten om mulige risikoreduserende løsninger som kunne tatt ned identifiserte risikoer på en mer effektiv om kostnadsbesparende måte fordi den eksterne parten ikke har den aktuelle løsningen i sin produkt- eller tjenesteportefølje. På den annen side kan involvering av eksterne ressurser ved gjennomføring av cyber risikovurderinger gi rederiene en merverdi i form av spesialkompetanse på cyber risikoområdet og en økt grad av objektivitet i vurderingene (BIMCO et.al., 2021).

En annen utfordring ved en stor grad av ekstern involvering vil kunne være at fokuset vil være rettet mot tekniske sikringstiltak alene. Organisatoriske og menneskelige tiltak *kan* helt eller

delvis bli utelatt. Behovet for en helhetlig tilnærming til cyber risikostyring vil behandles senere i kapittelet.

Studiet har ikke sett på hvilke kriterier som ligger til grunn når rederiene velger ekstern leverandør av cyber sikkerhetsløsninger, hvem leverandørene er eller hva de leverer. Bergsjø, Windvik og Øverlier beskriver en verdi-trussel-sårbarhets-tilnærming ved gjennomføring av cyber risikovurderinger, hvor verdivurderinger danner grunnlaget og er utgangspunktet når trusler og sårbarheter skal kartlegges (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020).

Ved utsetting av cyber risikovurderinger til ekstern part risikerer rederiene at virksomhetens verdier blir unøyaktig eller feil vurdert om den eksterne part ikke kjenner rederiet godt. I verste fall blir ikke virksomhetens verdier eller funksjoner tatt i betraktning i det hele tatt, noe som kan resultere i at også trusselbildet heller ikke blir riktig. En delt dokumentert verdikartlegging hvor rederiets formål, funksjon og systemer fremkommer vil kunne legge forholdene bedre rette og redusere mulighetene for unøyaktigheter eller feil. Dokumenterte verdikartlegginger kan være særdeles bedriftssensitiv informasjon. Deling av denne typen informasjon med eksterne parter krever tillit, at taushetserklæringer er på plass og at mottakeren har et sikkert system for å besitte denne typen informasjon.

En av de HSEQ-ansatte forteller at rederiet har valgt å ta den eksterne parten inn i organisasjonsbeskrivelsen i rederiet ISM som støttende. Den eksterne parten blir dermed et ledd i rederiets sikkerhetsstyringssystem. En slik løsning kan fungere om den eksterne parten kan få tilgang til verdikartlegginger og rederiinformasjon som vil kunne danne tilstrekkelig bakgrunnsinformasjon for å gjennomføre cyber risikovurderinger. Det er grunn til å anta at om slik informasjon *ikke* tilflyter den eksterne part kan en løsning hvor den eksterne parten inngår i rederiets ISM uten å besitte nødvendig informasjon medføre en risiko for både rederiet og den eksterne part.

5.3 IDENTIFISERING AV VERDIER

Funn i undersøkelsen viser at prosessen med kartlegging av de digitale enheter ombord som kan være utsatt for cyberangrep varierer. Enkelte opererer med en generell liste over enheter som blir distribuert ut til samtlige fartøy, i tillegg til fartøyspesifikke oversikter. Kartlegging av fartøyers enheter kan foregå gjennom nettverksskanning. Undersøkelsen viser at denne

typen tilnærming til kartleggingen av enheter kan innebære utfordringer knyttet til identifiseringen av enkelte typer OT-komponenter. Det må tas høyde for at de intervjuede har HSEQ-roller i sine rederier og ikke nødvendigvis teknisk kompetanse. Undersøkelsen tar ikke høyde for at teknisk personell i rederiene kan ha en annen oppfatning om identifiseringen av OT-komponenter.

Gjennomføring av en risikovurdering, innenfor cybersikkerhetsområde eller på andre områder, kan være utfordrende uten å ha en god forståelse for virksomheten, dens prosesser og systemer (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020). Kunnskap om rederiets formål, hva det produserer av tjenester, hvilke fartøy rederiet har, hvilke kritiske systemer fartøyene er avhengige av for å kunne gjennomføre sine ulike operasjoner, hvilke prosesser som kjører på disse systemene, hvilket personell systemene og prosessene er avhengige av, hvilket teknisk utstyr osv. vil være svært nyttig i en risikostyringsprosess og ved utvelgelsen av selve risikovurderingsprosessen.

Ensrettet fokus på IT-enheter (rutere, switcher, PC`er osv.) og de OT-enheter som har remote tilgang *og* som det er mulig å logge seg på vil kunne resultere i at kritiske OT-komponenter ikke blir identifisert. Eksempelvis vil enheter som gir grunnlagsdata (f.eks. GPS enheter) kunne bli utelatt. Om dette skjer vil det kunne resultere i at sårbarheter som ellers ville ha blitt avdekket og mitigert forblir åpne og fartøyet kan være utsatt for f.eks. spoofing av GPS-signaler. Mange fartøyer har i dag ECDIS kartmaskin som erstatning for oppdaterte sjøkart på papir. Forsøk har vist at det er mulig å manipulere GPS-signaler som går til ECDIS med den følge at operatører blir forledet til å tro at fartøyet befinner seg på en annen posisjon enn det i realiteten er, noe som kan føre til grunnstøting med de konsekvenser det kan resultere i.

Funn i studiet viser at kravspesifikasjoner og komponentlister fra fartøyenes byggeprosess eller eierskifter også kan bli benyttet for å identifisere digitale enheter om bord. Ved en slik tilnærming kan også en oversikt over leverandører av ulike enheter og systemer dokumenteres. Denne dokumentasjonen kan være nyttig i det videre arbeidet med de ulike enhetenes sårbarheter, idet leverandørene besitter kunnskap om de enheter de leverer og hvordan de tilhørende sårbarhetene best kan reduseres.

Funn i studiet viser at BIMCO`s veileder kan bli benyttet for å tilegne seg en oversikt over enheter basert på utstyrskategoriene. En metodikk for kartlegging av digitale enheter om bord, som beskrevet av BIMCO, vil understøtte behovet for en systematisk gjennomgang og bruk av en slik kategorisering vil kunne forenkle prosessen med senere oppdateringer av listen over

enheter om bord. Endringshåndtering (Management of Change) er ikke spesifikt omhandlet i dette studiet, men systematisk dokumenterte oversikter over enheter vil kunne være viktige forutsetninger for å se hvordan ønskede endringer kan påvirke andre enheter og systemer. I et cybersikkerhetsperspektiv vil sekundæreffekter av endringer av en enhet eller i et system kunne være nye eller økte sårbarheter i andre enheter eller systemer. Et eksempel på en slik sekundæreffekt kan være at eldre fartøyer med digitale enheter og systemer som aldri var tiltenkt en internett-tilknytning besluttes å utrustes med internettilgang fordi det oppstår et ønske eller et pålegg om å kunne monitorer prosesser ombord fra landsiden. Innføring av krav om digital fangstrapportering fra myndighetene kan bakgrunnen for en slik beslutning.

Ingen fartøy er helt like med tanke på hvilke digitale utstyrskomponenter som befinner seg om bord. Resultatet av kartleggingen av digitale enheter vil derfor være unik (Kessler & Shepard, 2022). Identifiseringen av enheter (verdier) er viktig av flere grunner. For at redere og eiere skal kunne ta gode beslutninger knyttet til redusering av risiko trenger de å vite hvilke enheter som det er knyttet risikoer til, hva konsekvensene av et cyberangrep kan være, osv., men verdikartleggingen er også viktig for valget av, og for implementeringen av sikringstiltak. Hvilke typer tiltak som bør implementeres og justeringer av tiltakene avhenger av hvilke enheter de skal beskytte. Graden av forskjeller mellom rederier, fartøyer, operasjonsområder og næringer underbygger behovet for gode kartlegginger, spesielt der eksterne ressurser står for majoriteten av cybersikkerhetsarbeidet.

5.4 TRUSLER OG SÅRBARHETER

Funn i dette studiet viser at forståelse og oppfatningen av maritime cyber trusler og sårbarheter samt vurderinger av deres alvorlighetsgrad varierer. Opplevelsen av trusler varierer fra fraværende, via ansatte med utilsiktede handlinger som åpner for ytre trusselaktører som f.eks. aktivister og opportunister til kriminelle med økonomiske motiver.

Ved identifiseringen av cybertrusler bør potensielle trusselaktører sine kapabiliteter, intensjoner og muligheter til å angripe vurderes (BIMCO et.al., 2021). Funn i undersøkelsen kan tolkes som at noen rederier ikke har et bevisst forhold til hvilke typer trusselaktører som kan utgjøre en potensiell trussel mot deres fartøyer. En manglende eller svak bevissthet til hvordan rederiets egne verdier understøtter virksomhetens mål *kan* være en medvirkende faktor til en svak oppfattelse av det trussellandskap man opererer i. Mangler denne bevisstheten kan det være utfordrende å skulle kunne vurdere potensielle aktørers kapabilitet,

intensjon og mulighet på en strukturert måte. Resultatet *kan* bli en unøyaktig eller feil sannsynlighetsfaktor som igjen vil kunne føre til feil i en risikovurdering med påfølgende uadekvat bruk av ressurser på anskaffelser, implementering og håndtering av cyber sikringstiltak.

Enkelte rederier mottar trusseletterretning fra ekstern leverandør av cyberetterretning og studiet viser at denne etterretningsinformasjonen blir distribuert ut i rederiet om dette tillates av utgiveren. Trusseletterretning, som produkt av en styrt prosess med systematisk innsamling av informasjon, analyse og vurdering av denne informasjonen som en del av et beslutningsgrunnlag, er viktig også i cyberdomenet. Trusseletterretningen skal predikere fremtiden, med en kommunisert usikkerhetsfaktor. Gjennom digital trusseletterretning vil rederiene kunne prioritere tid og ressurser på å oppdage og motvirke det som er mest relevante og sannsynlig for rederienes verdier (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020). Relevant og tidsriktig cyber trusseletterretning av god kvalitet vil kunne være en viktig faktor i rederienes arbeid med å få, og vedlikeholde, en cyber risikoforståelsen og redusere usikkerhetselementer i sine cyber risikovurderinger.

Samtidig er det under risikovurderinger viktig å bruke tid på det vi faktisk vet noe om; egne verdier og sårbarheter (Busmundrud, Maal, & Kiran, 2015). Rederiene må forsøke å skaffe seg informasjon om trusselen og hvordan den kan påvirke deres verdier, men på et tidspunkt må de sette strek. Uavhengig av hvem trusselaktøren er og deres motivasjon for å gjøre gjennomføre et cyberangrep, så vil det medføre skade på rederienes verdier om de lykkes. Derfor må de sikre seg. Det viktigste vil da bli å finne det som er viktigst å sikre seg mot og på hvilken måte (Busmundrud, Maal, & Kiran, 2015).

Funn i studiet viser at noen rederier har fokus på digitale og fysiske sårbarheter som kan påvirke cybersikkerheten om bord. De HSEQ-ansatte er bevisst sårbarheter som knytter seg til remote tilgang til digitale enheter, systemer og nettverk om bord i fartøy. Ved vurdering av sårbarheter bør nettverkstilknytning, direkte eller indirekte eksponering mot internett, implementerte (eksisterende) sikringstiltak, nødvendighet av programvareoppdateringer, bruk av flyttbare enheter som f.eks. minnepinner og fysisk adgangskontroll tas i betraktning (BIMCO et.al., 2021). I identifiseringen av sårbarheter om bord inngår en analyse av applikasjoner, systemer og prosedyrer for å avdekke svakheter som kan utnyttes av en potensiell trusselaktør (BIMCO et.al., 2021).

Hva som i praksis utgjør en sårbarhet vil være avhengig av hvilke trusselaktører rederiene realistisk sett står overfor (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020). Sett i lys av funn knyttet til enkelte rederiers vurdering av potensielle trusselaktører kan det være utfordrende å benytte Bergsjø, Windvik, & Øverlier sin tilnærming. En alternativ tilnærming for identifisering av cyber sårbarheter vil da kunne være en kartlegging av alle idenfiserte enheters offentlig kjente sårbarheter gjennom f.eks. National Vulnerability Database (NVD). Utfordringene knyttet til en slik tilnærming vil kunne være stor fokus på tekniske sårbarheter og at sårbarheter knyttet til egne menneskelige, organisatoriske og fysiske sikringstiltak går under radaren om rederiene ikke er bevisst dette forholdet. En slik tilnærming vil også sette krav til at en god dokumentert og systematisk kartlegging av digitale enheter (verdier) foreligger.

5.5 RAMMEVERK OG ANALYSEPROSESS

Funn i studiet viser at rederier benytter veiledninger for cybersikkerhet utgitt av klasseselskaper, BIMCO og IMO guidelines for gjennomføring av cyber risikostyringen. Samtidig viser funn at noen vurderinger kan ligge på et overordnet nivå og at ikke alle vurderinger blir dokumentert. I enkelte maritime bransjer som f.eks. servicefartøyer i olje- og gass-næringen kan klienter og kunders krav til cyber risikostyring være strengere enn omtalte veiledninger og guidelines. For rederier som har slike klient- og kundekrav vil disse kravene kunne påvirke cyber risikotilnærmingen i de respektive rederiene på en positiv måte. Grunnen til større klientkrav kan være at rederiene inngår i klientenes verdikjede og at kjeden ikke er sterkere enn det svakeste ledd. Verdikjedeangrep har blitt en kjent angrepsmetode ved målrettede cyberangrep de siste årene (NorSIS, 2023).

Cyber risikostyring vil kreve en helhetlig, strukturert og systematisk tilnærming på grunn av dens kompleksitet (BIMCO et.al., 2021). En helhetlig tilnærming vil kunne sikre at risikoreduserende tiltak vil bli valgt på bakgrunn av deres positive påvirkning på de ulike systemer om bord og deres kostnadseffektivitet (BIMCO et.al., 2021). BIMCO sin veiledning er basert på NIST Cyber Security Framework (NIST, The U.S. National Institute of Standards and Technology, 2018) og den internasjonale standarden for styringssystem for informasjonssikkerhet, ISO 27000-serien. Rammeverket kan brukes som maler for et cyber risiko styringssystem.

Styring av cyber risiko kan fremstå som en svært komplisert aktivitet. Kompleksiteten på området med store og avanserte digitale systemene om bord, ulike IT- og OT-nettverk samt risikovurderinger av tilsiktede uønskede hendelser, kan resultere i at mange rederier kun gjennomfører en dokumentert forenklet risikovurdering for å kunne fremvise dette overfor en assessor. Et bevisst forhold til valg av rammeverk som passer rederiets virksomhet vil kunne gjøre cyber risikostyringen mer overkommelig og resultatet etter en strukturert og systematisk gjennomgang vil kunne gjøre det lettere for rederiene å opprettholde en oppdatert oversikt egen cyber risikostyring. Ved å være strukturert og konkret blir det også enklere for beslutningstakeren å følge resonnementene i vurderingene og det blir lettere å fatte beslutninger om behandling av risikoene.

Sett i lys av utfordringer knyttet til verdikjedeangrep, vil det trolig bli et enda større fokus på bruk av standardiserte rammeverk for cyber risikostyring. Ved bruk av et kjent rammeverk, med en vurdering av tilstanden i rederiet basert på dette rammeverket og et verktøy for måling av modenhet, vil rederier kunne dokumentere sitt cyber sikkerhetsnivå overfor sine kunder og samarbeidspartnere. I tillegg til å redusere de faktiske cyberrisikoene for rederiene, vil dette også kunne være et salgsargument ved inngåelse av fremtidige kontrakter.

Funn viser at prosessen med gjennomføring av cyber risikoanalyser kan være forskjellig fra rederi til rederi. Enkelte rederier starter prosessen om bord og resultatet fra den innledende risikovurderingen sendes til landorganisasjonen. Vurderingene gjennomgås og justeringene kan bli gjennomført før de returneres fartøyene for kommentarer.

Flere rederier kvantifiserer risikoer gjennom bruk av sannsynlighet og konsekvens i en fem ganger fem-matrise, hvor det blir benyttet fargekoder for å visualisere risikonivåer. Andre rederier gjennomfører en overordnet cyber risikovurdering internt og involverer deretter ekstern part for behandling av identifiserte cyberrisikoer. Involvering av mannskap på alle nivåer, spesielt kaptein og maskinsjef og overstyrmann, for å få en forståelse av implementeringen av IT- og OT-systemer om bord og hvordan eventuelle avvik mellom den faktiske implementeringen og den dokumenterte, er et aspekt ved cyber risikovurderinger (BIMCO et.al., 2021). Mindre endringer i oppsett av systemer og nettverkstilknytninger vil, som tidligere nevnt, potensielt kunne medføre uønskede eksponeringer av sårbarheter. Slike endringer kan bli gjennomført uten at disse blir dokumentert i fartøyets dokumentasjon. Om slike endringer ikke blir hensyntatt under risikovurderinger vil man kunne sitte igjen med en feil forståelse av egen risikoeksponering.

Andre rederier benytter kvalitative vurderinger for sine cyberrisikoer og risikoen beskrives med grønn, gul og rød. Ved kvalitative cyber risikovurderinger har rederier benyttet 1-5 og A-F graderinger av sannsynlighet og konsekvens. BIMCOs (BIMCO et.al., 2021) fire faser er et eksempel på strukturering av risikovurderingsprosessen. For å oppnå en helhetlig og sammenhengende risikovurdering vil en strukturert prosessen som beskrevet av BIMCO kunne være til god hjelp.

På bakgrunn av dette er det grunn til å anta at det benyttes både kvantitative og kvalitative cyber risikovurderinger blant rederiene. En kvantitativ tilnærming vil være gjenkjennbart for de fleste rederier og det vil kunne oppfattes som enklere å gjennomføre men også lettere å sammenholde resultatene (risikoverdiene) mellom de ulike identifiserte risikoene i sikkerhetsstyringssystemet. Utfordringen med den kvantitative tilnærmingen vil kunne være å kommunisere usikkerhetselementer i vurderingen av de ulike faktorene. Trolig vil en kvalitativ tilnærming til risikovurderinger gjøre det lettere for en beslutningstaker å forstå hva som ligger til grunn for vurderingene og at vurderingene innebærer ulike grader av usikkerhet. Siden risikovurderinger i bunn og grunn handler om å predikere sannsynligheten for at noe galt skal skje og hva en mulig konsekvensen av dette kan bli, vil en beskrivelse av usikkerhet i vurderinger være til hjelp når ledelsen skal fatte beslutninger om hvilke tiltak som skal iverksettes.

Enkelte rederier har også benyttet ekstern part for gjennomføring av selve risikovurderingsprosessen. Den eksterne part har gjennomført nettverksskanning og deretter gjennomført en sårbarhetsvurdering av de digitale komponentene som ble kartlagt i nettverksskanningen. Kvantitative risikovurdering basert på sannsynlighet og konsekvens i fem ganger fem matriser har blitt utarbeidet og overlevert rederiet. Rederiet har deretter gjennomgått vurderingene og justert konsekvensfaktorene basert på egen kunnskap. Avhengig av rederiets interne ressurser kan gjennomføringen av cyber risikovurderinger assisteres av en tredjepart (BIMCO et.al., 2021).

Eksternes cyber risikovurderinger bør gjennomføres av personell med spesialkompetanse på området slik at det helhetlige ressurspådraget ved cyber risikostyringen og reduksjon av cyber risikoer kan bli best mulig. En annen fordel med å involvere ekstern part i gjennomføring av risikovurderingene er en større mulighet for objektiv vurdering og læring i rederiet (BIMCO et.al., 2021). For å få et optimalt resultat av en ekstern risikovurdering er det nødvendig at den eksterne part har god innsikt i det maritime cyberdomenet, trusselbildet og inngående

kunnskap om rederiet. Mangler en slik bakgrunnskunnskap hos den eksterne parten kan en ekstern cyber risikovurdering føre til at man implementerer feil eller uhensiktsmessige tiltak.

«Konsulenter kan benyttes, men ansatte bør ha ansvaret»

(Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020)

Det eksisterer i dag ingen internasjonal enighet om hva som er beste praksis for gjennomføring av risikovurderinger for tilsiktede uønskede hendelser. Det kan imidlertid være avgjørende at den tilnærmingen man velger å benytte er tilpasset risikovurderingens formål (Busmundrud, Maal, & Kiran, 2015). Hensikten med risikovurderinger er:

«*Å gi beslutningsstøtte vedrørende valg av løsning og tiltak»*

(Busmundrud, Maal, & Kiran, 2015)

For rederiene vil det derfor kunne være nyttig å gjennomføre en diskusjon om valg av tilnærming for cyber risikovurderinger. Skal man benytte en kvantitativ tilnærming som man er kjent med fra andre områder innad i rederiet og som kanskje vil gjøre det enklere å sammenligne risikoer fra ulike områder? Man bør da være klar over at en slik tilnærming vil kunne gjøre det vanskeligere å beskrive graden av usikkerhet som ligger i vurderingene og at sannsynlighetsfaktoren ofte blir vurdert for høyt, noe som vil resultere i at risikoen kanskje blir vurdert noe for høyt. Et annet alternativ kan være å velge en kvalitativ tilnærming som beskriver risikoene bedre hvor usikkerheten kan kommuniseres beslutningstakere på en bedre måte. En slik tilnærming vil sette større krav til beslutningstakerne når det gjelder å kunne sammenligne cyberrisikoene mot øvrige risikoer fra kvantitative risikovurderinger.

5.6 SANNSYNLIGHET, KONSEKVENS OG TILTAK

Beskrivelser av hvordan rederiene anslår sannsynligheten for at cyberhendelser skal finne sted hos dem kommer ikke godt frem i dette studiet. Flere HSEQ-ansatte oppgir at de benytter en matrise for å angi sannsynlighet og konsekvens. Ingen av intervjupersonene oppgir at de gjennomfører noen vurderinger av sannsynlighetskomponenter som BIMCO anbefaler. Sannsynlighetskomponentene er egne sårbarheter og trusselaktørens intensjon, kapabilitet og mulighet (BIMCO et.al., 2021).

Funn i studiet viser at HSEQ-ansatte vurderer den økonomiske konsekvensen av cyberhendelser som den alvorligste og kravet til systemers tilgjengelighet for å kunne

opprettholde den operasjonelle driften av fartøyene som det viktigste. Intervjupersoner beskriver i mindre grad et bevisst forhold til kvantifiseringen av konsekvensene ved vellykkede cyberangrep. Flere oppgir at de benytter en risikomatrise med sannsynlighet og konsekvensfaktorer. Uten en kvantifisert konsekvens kan det bli utfordrende, eller umulig å ha en kvantifisert risikotilnærming som de beskriver at de har. Svakheter i den kvalitative undersøkelsen kan være årsaken til at konsekvensvurderingene ikke har kommet godt nok frem i dette studiet. Med utgangspunkt i at rederiene har lang erfaring med gjennomføring av risikovurderinger på ulike områder, er det grunn til å anta at de allerede har etablerte og dokumenterte oversikter med kvantifiserte konsekvenser ved uønskede hendelser. For å kunne etablere og vedlikeholde en helhetlig og konsistent risikostyring på tvers av ulike områder i rederiet vil det kunne være nyttig å benytte den samme konsekvensmatrisen på de ulike områdene. En slik tilnærming vil også gjøre det lettere for ledelsen å sammenligne risikoer på tvers av risikoområder i egen organisasjon.

Flere intervjupersoner oppgir at de ikke har et bevisst forhold til konfidensialitets-, integritets- og tilgjengelighets-krav når de gjennomfører cyber risikovurderinger. Ifølge BIMCO (BIMCO et.al., 2021) gir en modell for konfidensialitet, integritet og tilgjengelighet (CIA) et rammeverk ved konsekvensvurderinger. Samtidig representerer CIA sikringsmål knyttet til de ulike enheter og systemer, og inngår gjerne som en del av en fullstendig verdikartlegging. Det kan derfor være vanskelig å ha et forhold til CIA uten å ha gjennomført en grundig verdikartlegging og vurdering i forkant av risikovurderingen. En naturlig del av verdivurderingen vil kunne være å definere sikringsmålene til de ulike verdiene. Sikringsmålene vil da være knyttet til hvor viktig konfidensialiteten, integriteten og tilgjengeligheten til de ulike systemer er. Å unnlate å forholde seg til CIA ved risikovurderingen vil potensielt kunne føre til sekundæreffekter som at feil risikoreduserende tiltak blir implementert, at tekniske tiltak ikke blir parametersatt riktig eller at tiltak blir en unødvendig begrensning på f.eks. tilgjengelighet.

Resultater fra studiet viser at rederiene har etablert teknologiske, menneskelige og organisatoriske sikringstiltak. Funn viser at flere rederier har etablert prosedyrer for remote og fysisk tilgang til fartøyer. Administrasjon av tilgangsrettigheter for remote tilgang til fartøyene hos noen rederier blir gjennomført av fartøyansvarlige. Kun et fåtall ansatte har tilgang til kritiske systemer og remote tilgang er passordbelagt. Tilgang gis kun når spesifikt arbeid som krever remote tilgang skal utføres. BIMCO (BIMCO et.al., 2021) beskriver nødvendigheten av å etablere policyer og prosedyrer for slike tilganger. Tilgang via fartøyers

internett-oppkoblinger (remote tilgang) vil kunne være en vesentlig sårbarhet for de fleste rederier. Alle de HSEQ-ansatte har fortalt at de hadde identifisert remote tilgang som et kritisk punkt. Sett i forhold til å ta seg fysisk om bord eller å benytte en innsider, vil et cyberangrep via en internett-tilkobling trolig være den angrepsmåten som representerer minst fare for å bli oppdaget, bli tatt og stilt til ansvar for handlingen. Samtidig vil et nettverksangrep trolig være den billigste angrepsmetoden for en ekstern trusselaktør.

Fysisk tilgangskontroll som et sikringstiltak mot cyberrisikoer på fartøyer er beskrevet av HSEQ-ansatte i dette studiet. Fysisk tilgangskontroll er gjerne allerede gjennomført som et ledd i trygghetsarbeidet om bord og også forankret i sikkerhetsstyringssystemet. Identifiseringen av eksisterende tiltak underbygger behovet og nytten av å ha en helhetlig tilnærming til risikoområdet. En helhetlig tilnærming kan være nyttig for å få en best mulig utnyttelse av de tiltakene man allerede har implementert, men også for å kunne være i stand til å forstå at endringer eller fjerning av et etablert tiltak vil kunne få en negativ eller positiv påvirkning på andre risikoområder. Slike effekter beskrives gjerne som sekundæreffekter, og er tidligere beskrevet.

Segmentering av nett, brannmurer og brannmurregler, antivirus og oppdatert programvare, skybaserte løsninger og kodede killswitcher er eksempler på tekniske sannsynlighetsreduserende tiltak HSEQ-ansatte beskriver som implementert hos dem. BIMCO (BIMCO et.al., 2021) skisserer en rekke mulige tekniske sikringstiltak for å redusere sannsynligheten for å bli utsatt for et vellykket cyberangrep. Tiltakene beskrevet av de HSEQ-ansatte er alle nevnt av BIMCO.

Det tidligere nevnte begrepet «forsvar i dybden», kan illustreres gjennom de ulike tiltakene de HSEQ-ansatte har beskrevet. De prosedyremessige tiltakene er viktige, men vil ikke fungere like godt uten at de tekniske sikringstiltakene er på plass og fungerer etter hensikten. De tekniske tiltakene hadde heller ikke fungert på ønsket måte om man ikke hadde hatt, og etterlevd, de policyer og prosedyrer som beskriver hvordan bl.a. tilganger skal gis, når nettverkstilkoblinger skal være aktive, osv. Fysisk tilgangskontroll skal hindre at uvedkommende kan komme i kontakt med sårbare IT- og OT-komponenter som kan utnyttes. Idet det eksisterer en kobling mellom internett og IT- og OT-komponenter om bord, vil disse enhetene i seg selv være like sårbare som lignende enheter på land, og dermed også like utsatt for målrettede og ikke-målrettede angrep.

Følgende maritime eksempler kan illustrere sårbarhet for cyberangrep. I 2010 ble en ny oljerigg på vei fra Sør-Korea til sitt operasjonsområde infisert av, trolig ikke-målrettet, skadevare-angrep. Skadevaren spredte seg blant digitale nettverksenheter om bord og infiserte også en «Blowout Preventer» (BOP) (Kessler & Shepard, 2022). Arbeidet med fjerningen av skadevaren fra riggen tok 19 dager. 19 dager som kunne vært benyttet til produksjon. Denne hendelsen illustrerer at cyberangrep ment for «det brede lag» og som ikke nødvendigvis er rettet mot den maritime næringen, likevel kan få store konsekvenser for den som blir rammet. Digitaliseringen av fartøyene har satt disse i den tilnærmet samme situasjonen som digital infrastruktur og digitale enheter på land.

I 2011 ble et iransk rederi utsatt for et målrettet cyberangrep hvor deres nettverk ble hacket, logistikksystemer tatt ned og hele flåten på ca. 170 fartøyer ble kompromittert. Angriperne la inn uriktig informasjon som bl.a. førte til at sporingen av fartøyene ikke fungerte, fartøy ble sendt til feil havn og cargo forsvant (Kessler & Shepard, 2022). Denne hendelsen viser at konsekvensene av målrettet angrep kan bli enorme og kan ha svært store følgeeffekter siden den maritime verdikjeden er tett sammenflettet.

Skadevare kan infisere digitale enheter om bord ved å bli lastet ned fra en internettkilde som en funksjonalitet i en datafil (f.eks. en kjørbar multimedia-fil), et vedlegg mottatt på epost, ligge som en fil på en minnepenn som stikkes inn i en USB-kontakt, osv. Svært ofte vil et vellykket cyberangrep initialt kreve en aktiv handling fra offerets side. Dette er bakgrunnen for at prosedyremessige og tekniske tiltak må understøttes av menneskelighet tiltak. Eksempler på slike menneskelige tiltak kan være opplæring av ansatte som øker deres bevissthet om cybertrusler og hvordan de fungerer, trening på gjenkjennelse og håndtering av cyberangrep hvis de skulle komme, osv. Funn i studiet viser at rederier har tatt i bruk ulike tiltak for å heve de ansattes bevissthet og kompetanse på cyberområdet.

Det fremstår som uklart om rederiene har en bevisst strategi for utvikling av «forsvar i dybden», eller om de ulike tiltakenes sammensetning tilfeldigvis har blitt slik. Flere av rederiene har beskrevet at de kjøper inn tjenester fra eksterne leverandører og at leverandørene kommer med forslag til hvordan rederiene skal sikre seg. En slik tilnærming kan fungere og være en alternativ tilnærming, noe BIMCO (BIMCO et.al., 2021) også skisserer, men tilnærmingen har også noen vesentlige utfordringer.

Hvordan kan rederiene vite hvilke løsninger som er gode og hvilke som er mindre gode hvis de selv ikke har tilstrekkelig kunnskap om cybersikkerhet? Denne problemstillingen ble

beskrevet av George A. Akerlof og han belyste den i «The Market for «Lemons»: Quality Uncertainty and the Market Mechanism» (Bergsjø & Windvik, 2018). Akerlof satte søkelyset på informasjonsasymmetrien mellom selger og kjøper. Innenfor cyber sikkerhetstjenester kjenner tjenesteleverandørene cyberdomenets utfordringer, eksisterende produkter og tjenester samt feltets høye endringstakt mye bedre enn rederiene. Rederiene har ingen mulighet til å evaluere tjenestenes kvalitet og kan ikke vite sikkert om de fungerer etter hensikten. Om rederiene benytter de samme leverandørene til sine sikringstiltak som for etterretningsprodukter, eksisterer det en mulighet for at noen beskriver et «sykdomsbilde» og kommer med en diagnose i den ene omgangen for deretter å presentere medisinen i form av egne tjenester og produkter i den neste. Funn i studiet viser at HSEQ-ansatte opplever det som vanskelig å vurdere kvaliteten i sikkerhetsleveransen fra den eksterne parten.

For å redusere sannsynligheten for å havne i et «Lemon market» kan det være en mulig tilnærming å benytte en leverandør av trusseletterretning og cyber risikovurderinger og en annen leverandør av ulike typer sikringstiltak (menneskelige, teknologiske og prosedyremessige).

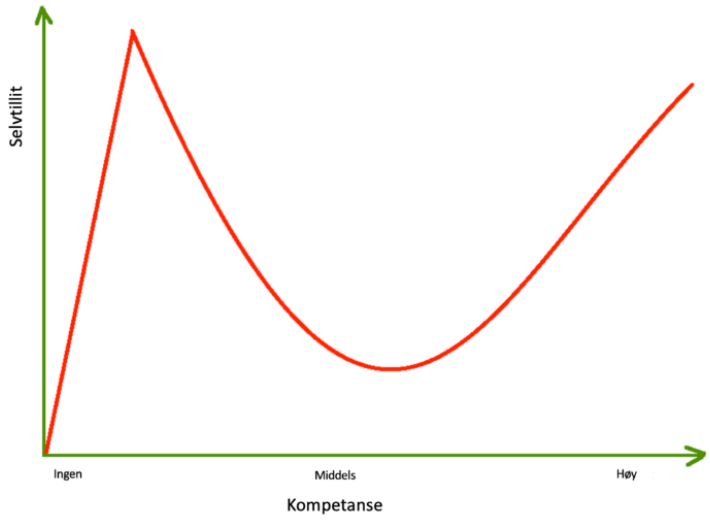
5.7 ULIKE PERSPEKTIVER OG OPPLEVELSER

Funn i studiet viser at opplevelsen av cybersikkerhetsområdet er litt forskjellig blant de HSEQ-ansatte. Noen har fått bekreftet av klasseselskapet at det arbeidet de gjør på området er bra. En bekreftelse på at det du gjør er riktig, vil trolig også gi en positiv opplevelse. Støtte og tilrettelegging fra ledelsen og en økt offentlig oppmerksomhet på cybersikkerhetsområdet generelt kan være en medvirkende faktor for at den enkelte opplever arbeidet med cybersikkerhet som meningsfylt og motiverende. Samtidig er det andre intervjupersoner som oppgir at de er ukomfortable og at verden oppleves som uoversiktlig på dette området. Cyber risikoområdet kan oppleves som ekstremt omfattende og avansert. Resultatet kan bli en følelse av mangel på kontroll. Denne følelsen trenger nødvendigvis ikke å være negativ, men kan kanskje i stede være en indikasjon på at man er på rett vei.

Psykologene David Dunning og Justin Kruger har presentert en mulig forklaringsmodell for de variasjonene som funnene beskriver. Forklaringsmodellen blir kalt Dunning-Kruger-effekten (Svartdal, 2022) og kan beskrives som;

Økende kompetanse ledsages gjerne av en økende forståelse av hvor lite man kan, men med ytterligere erfaring øker igjen opplevelsen av forståelse.

Dunning-Kruger effekten (Svartdal, 2022)



Figur 7 Dunning-Kruger effekten. Kilde: snl.no / Salgo60/Line Marie Berteussen/Shutterstock.

Det kan være en tendens hos enkelte til innta en for positiv holdning til rederiets status på cyber risikoområdet, basert på tilbakemeldinger fra revisjoner gjennomført av klasseselskap og måten den eksterne parten (tjenesteleverandøren) har solgt inn sine produkter og tjenester på. De HSEQ-ansatte som uttrykte en følelse av mangel på kontroll kan, i flg. Dunning-Kruger, befinne seg på et middels kompetansenivå og i bunnen av grafen i figur 8. Et fortsatt fokus på cyberområdet vil, i flg. Dunning-Kruger, kunne føre til en bedre følelse og selvtillit som en følge av økt kompetanse på området. En reell test av rederiets sikkerhetstilstand oppnås kanskje ikke før man har opplevd hvordan et skarpt cyberangrep blir håndtert av rederiet selv og av leverandøren man har inngått en avtale med. Et bedre alternativ er trolig en større øvelse regissert av andre med den riktige kompetansen. Et massivt cyberangrep som reduserer tilgjengelighet på kritiske innsatsfaktorer (enheter, systemer og nettverk), endrer data i databaser og truer med å lekke sensitiv informasjon vil stresse mange avdelinger og enkeltpersoner over en lengre periode og vil i ytterste konsekvens kunne resultere i tap av menneskeliv og konkurs.

På bakgrunn av dette kan det være grunn til å anta at de intervjupersoner som har uttrykt en følelse av å ikke ha kontroll og at cybersikkerhetsområdet er krevende, har forstått kompleksiteten i temaet og hvor utfordrende det vil være for rederiet å håndtere en cyberhendelse.

En etablert digital sikkerhetskultur hvor NorSIS 8 dimensjoner (Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse, 2020) oppleves å være tilstede, kan være en årsak til at enkelte HSEQ-ansatte opplever cyberrisikoområdet som overkommelig og motiverende.

5.8 STATUS OG MODENHET

Alle rederier med krav om å ha etablert et sikkerhetsstyringssystem skal gjennomføre en cyberrisikovurdering i henhold til IMO 2021-kravene (IMO, 2017). Fristen for å ha gjennomført den første cyber risikovurderingen har gått ut. De HSEQ-ansatte som har bidratt i dette studiet har alle bekreftet at de har gjennomført en cyber risikovurdering, eller er i gang med en slik vurdering.

HSEQ-ansatte forteller at tilbakemeldingene etter revisjonene i 2021 og 2022 har ført til økt fokus på cyberrisikoer som igjen har gitt forbedringer. Disse observasjonene kan sies å være helt i tråd med hvordan man ønsker at den kontinuerlige forbedringsprosessen skal være. Sikkerhetsarbeidet er en reise uten en endelig destinasjon. Denne påstanden kan sies å være ekstra gyldig innenfor cyberområdet hvor teknologien utvikler seg stadig raskere og hvor nye sårbarheter oppstår på løpende bånd.

En HSEQ-ansatt peker på at IMOs krav om at det skal gjennomføres en cyber risikovurdering og kartlegging av egne sårbarheter for å finne ut av hva egen status er.

Alder, størrelse (antall ansatte og antall fartøyer), intern kompetanse og driftsområde det respektive rederiet arbeider innenfor *kan* påvirke både kapabiliteten og kapasiteten det enkelte rederi har til å gjennomføre risikovurderinger på dette området og dermed også status på rederiets cybersikkerhetsarbeid i dag. Som tidligere nevnt er bevissthet rundt risikoer innenfor cyberdomenet relativt nytt for flere rederier. Antallet sårbarheter, og dermed risikoene, har økt i takt med digitaliseringen den maritime næringen. Graden av bevissthet rundt de «nye» risikoene har vært varierende og det kan kanskje hevdes at de for enkelte tidvis har vært ubevisste. Cybersikkerhetsområdet er noe forskjellig fra øvrige risikoområder rederiene har erfaringer med å navigere i, noe som kan forklare at alle rederier ikke har kommet like langt.

De største forskjellene fra andre risikoområder kan være at vi har med tilsiktede uønskede handlinger å gjøre og at cyberdomenet fremstår som uoversiktlig og ekstremt komplisert. Det vil kreve en modning blant beslutningstakere, HSEQ-ansatte og redere å erkjenne at cyberrisikoer i maritim sektor må tas på det største alvor.

En testcase hvor et virtuelt fartøy ble hacket idet det var i ferd med å legge til kai i Spania, har vist at potensiale for store materielle skader på fartøy, kai, personell og miljø gjennom mulige utslipp, samt store økonomiske kostnader knyttet til forsinkelser av lasting og lossing ved havna viser alvoret i og hva som kan være reelle konsekvenser ved et maritimt cyberangrep (Tam, 2021).

Modenhet kan ofte henge sammen med erfaring, på individnivå så vel som på organisasjonsnivå. Hva man erfarer på organisasjonsnivå kan være en utfordring å få en oversikt over, idet de faktiske erfaringer skjer hos det enkelte individ. For å få en dokumentert oversikt over et rederi sin modenhet kan man benytte ulike kartleggingsverktøy. Det eksisterer verktøy for å kartlegge egen organisasjon sin modenhet på cybersikkerhetsområdet.

Et eksempel på et slikt verktøy er NIST Cybersecurity Framework (CSF) som består av fasene identifisering, beskyttelse, detektering, håndtering og gjenoppretting (NIST, The U.S. National Institute of Standards and Technology, 2018). BIMCO (BIMCO et.al., 2021) har støttet seg på NIST i utarbeidelse av sin veiledning og benytter grovt sett de samme fasene. Sammen med CSF kan det gjennomføres en kartlegging av rederiets status gjennom bruk av Capability Maturity Model (CMM). Modellen består av tilstandsnivåene initialt, gjentagende, definert, håndtert og optimalisert. Ved å vurdere nivået på rederiets eksisterende tiltak i dag i de ulike CSF-fasene kan modenheten på cyber sikkerhetsområdet kartlegges og dokumenteres. Resultatet av en slik kartlegging vil kunne være et godt grunnlag for det videre arbeidet med å behandle de identifiserte risikoene på cyberområdet.

5.9 OPPSUMMERING

I dette delkapittelet oppsummeres de foregående drøftingskapitlene.

Dette studiet har vist at tilnærmingen til selve utføringen av cyberrisikovurderinger varierer noe rederiene i mellom. Langt de fleste har valgt en kvantitativ tilnærming med bruk av sannsynlighet ganger konsekvens og benyttet en 5 ganger 5 matrise. Fordelene med en slik tilnærming er at den allerede er kjent å benyttet i rederiene. Utfordringen med en kvantitativ

tilnærming i cyberrisikovurderinger der man skal vurdere risikoer for tilsiktede uønskede hendelser kan ligge i at vurderingene blir for «smale». Trusselaktørens komponenter (mulighet, intensjon og kapabilitet), eksisterende sårbarheter og allerede implementerte sikringstiltak kan være utforende å belyse i tillegg til at usikkerhetsmomentet likeså.

Alternativet til en kvantitativ tilnærming er en kvalitativ cyber risikovurdering. En kvalitativ tilnærming tar inn over seg side ved trusselaktøren, sårbarheter og eksisterende sikringstiltak, men setter større krav til den som skal gjennomføre vurderingene. En annen fordel med en kvalitativ tilnærming kan være dens potensiale til å kommunisere usikkerhetselementet på en bedre måte.

De rederiene som har bidratt i denne undersøkelsen har lagt ansvaret for oppgavene knyttet til de IMO pålagte cyberrisikovurderinger til HSEQ-rollen. Denne løsningen oppfattes å være i tråd med BIMCO`s anbefalinger. Undersøkelsen har vist at de fleste rederiene har en bred intern involvering i arbeidet med cyber risikovurderinger, noe som også inkluderer ledelsesnivået. Teori på området understreker ledelsens deltakelse og støtte som en viktig premiss for god cyberrisikostyring. Gjennom kommunisert støtte til risikoarbeidet kan ledelsen også legge til rette for en bred intern involvering.

Involvering av leverandører av cybersikkerhetstjenester er vanlig blant de rederiene som inngår i dette studiet. Hvor i cyberrisikostyringen, og i hvilket omfang, varierer imidlertid i en viss grad. Leveransene varierer fra kun trusseletterretning til å være en del av den formelle sikkerhetsorganisasjonen i rederiet. Omhandlet teori viser at dette kan være en god løsning for enkelte rederier, men at det er noen fallgroper i en slik tilnærming som man bør være bevisst.

Nødvendig teknisk kunnskap om sikringstiltak og sårbarhetskartlegging fører også til at de fleste rederiene i undersøkelsen velger å sette ut sårbarhetskartlegginger og sikringstiltak til eksterne parter. Flere av de intervjuede har opplyst at rederiene har inngått avtaler om håndtering cyberhendelser om slike skulle oppstå. Også dette er i tråd med anbefalinger, gitt av blant annet Nasjonal Sikkerhetsmyndighet (NSM). NSM har en godkjenningsordning for leverandører av slike tjenester.

Det kan vise seg å være nyttig å benytte seg av eksterne leverandører av cybersikkerhetstjenester om leverandøren har et dokumentert tilstrekkelig kunnskapsnivå og innsikt i gitt tilstrekkelig informasjon om det foretaket de skal tjene. I sammenheng med innkjøp av cybersikkerhetstjenester kan det også være nyttig å være bevisst

informasjonsasymmetrien mellom leverandør og kunde. Risikoen for å få et mindre godt produkt kan reduseres om rederiene setter krav til dokumentert kvalitet hos leverandørene.

Undersøkelsen har vist at bevisstheten rundt hvilke systemer og applikasjoner som støtter opp under rederienes kritiske funksjoner kunne vært bedre. I et tillegg til BIMCOs veileder, opplistes en rekke kategorier med underliggende systemer som kan være relevante å risikovurdere. Ikke to rederier og fartøyer er like. Derfor kan en verdikartlegging som grunnlag for risikovurderinger være nyttig.

De intervjuede er noe delt i opplevelsene knyttet til cyberrisikovurderinger spesielt og cybersikkerhetsområdet generelt. Enkelte beskriver kontroll, noe erfaring på området og grunngir det med gode tilbakemeldinger etter revisjoner og at dette er noe de har bedrevet i noen år nå. Andre oppgir et inntrykk av en uoversiktlig verden og at cyberområdet er komplisert og avansert. Dette kan gi en følelse av at man ikke strekker til og at man ikke har kontroll. Denne følelsen er ikke god, men trenger nødvendigvis ikke være bare negativ. Tilstanden kan være en indikasjon på at man har kommet til en videre situasjonsforståelse og at man er på vei inn i en dypere forståelse og erverv av en høyere kompetanse. Om dette er tilfellet kan selvtilliten på området øke, ref. Dunning-Kruger effekten.

6.0 AVSLUTNING

I dette kapittelet vil mulig implikasjoner for praksis diskuteres, samt forslag til videre forskning.

6.1 IMPLIKASJONER FOR PRAKSIS

Dette studiet har vist at rederienes cyber risikovurderinger og cyber risikostyring kan utføres av deres HSEQ-ansatte, men med støtte fra eksterne tjenesteleverandører i større eller mindre grad. Studiet viser også at rederier kan ha et noe ubevisst forhold til hvilke digitaliserte enheter som befinner seg om bord og konsekvensene vil kunne være om disse blir utsatt for et cyberangrep. Det vil kunne være utfordrende for en tjenesteleverandør å skreddersy cybersikkerhetsleveranse til fartøyet om leverandøren ikke kjenner til fartøyets særegenheter, og for rederiet å vurdere kvaliteten i leveransen. Det kan derfor argumenteres for at rederiene gjennom økt fokus på egne verdier og en heving av bestiller-kompetansen på cybersikkerhet kan redusere egne cyberrisikoer ytterligere.

6.2 VIDERE FORSKNING

Det er gjennomført forskning på gjennomføring av risikovurderinger innenfor området tilsiktede uønskede hendelser (Busmundrud, Maal, & Kiran, 2015), og det er utarbeidet en norsk standard som beskriver hvordan slike risikovurderinger kan gjennomføres. Maritim sektor er en næring som har en tradisjon for gjennomføring av risikovurderinger av utilsiktede uønskede hendelser.

Selv om cyberrisikoområdet også kan omfatte utilsiktede uønskede hendelser, vil rederienes pålagte risikovurderinger av slike uønskede hendelser sette større krav til rederienes egen kompetanse på området. Om cyberrisikovurderinger skal settes ut til eksterne parter, vil en inngående kunnskap om det enkelte rederi sine verdier kunne være nødvendig for at tiltakene skal bli optimale.

Det kan derfor være hensiktsmessig å forske nærmere på rederienes egne verdikartlegginger og konsekvensanalyser, samt hvordan slik dokumentasjon etableres og vedlikeholdes.

En slik kunnskap vil kunne bidra til at rederier øker sannsynligheten for optimal bruk av menneskelige og finansielle ressurser på cybersikkerhetsområdet.

REFERANSER

Aarset, M. (2020). *Håndtering av risiko.* Ålesund: Terp.

Andresen, M. E. (2023, 05 23). *asymmetrisk informasjon i Store norske leksikon*. Hentet 05 23, 2023 fra snl.no: https://snl.no/asymmetrisk_informasjon

Baltic and International Maritime Council. (2023, 04 10). *bimco.org*. Hentet fra https://www.bimco.org/

Bergsjø, H., & Windvik, R. (2018). *Datasikkerhet for ledere - hvordan beskytte din virksomhet.* Oslo: Universitetsforlaget.

Bergsjø, Håkon; Windvik, Ronny; Øverlier, Lasse. (2020). *Digital Sikkerhet - En innføring.* Oslo: Universitetsforlaget.

BIMCO et.al. (2021). *The Guidelines on Cyber Security Onboad Ships version 4.* Hentet fra https://www.bimco.org/: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Busmundrud, O., Maal, M., & Kiran, J. H. (2015). *Tilnærminger til risikovurderinger for tilsiktede, FFI-rapport 2015/00923.* Lillestrøm: FFI (Forsvarets Forskningsinstitutt).

Dalland, O. (2017). *Metode og Oppgaveskriving, 6. utg.* Oslo: Gyldendal Akademisk.

Dvergsdal, H. (2023, 05 03). *digitalisering i Store norske leksikon*. Hentet 05 23, 23 fra snl.no: https://snl.no/digitalisering

Engerengen, L. (2023, 05 23). *jamming i Store norske leksikon*. Hentet 05 23, 2023 fra snl.no: http://snl.no/jamming

IBM Security. (2022). *Cost of a Data Breach Report 2022.* Armonk, NY 10504: IBM Corporation.

IMO. (2017, 7 5). Guidelines on Martime Cyber Risk Management. London, UK: International Maritime Organization.

IMO. (2017, juni 16). MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS. *Resolution MSC.428(98)*. London, UK: Inernational Maritime Organization.

Kessler, G., & Shepard, S. (2022). *Maritime Cybersecurity - A Guide for Leaders and Managers.* Great Britain: Amazon.

Kvale, S., & Brinkmann, S. (2015). *Det kvalitative forskningsintervju, 3.utg.* Oslo: Gyldendal akademisk.

Lockheed Martin . (2023, April 13). *lockheedmartin.com*. Hentet fra https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Lovdata. (2014, 09 05). *Lovdata.no*. Hentet fra Forskrift om sikkerhetsstyringssystem for norske skip og flyttbare innretninger: https://lovdata.no/dokument/SF/forskrift/2014-09-05-1191

Lovdata. (2022, 10 01). *Lovdata.no*. Hentet fra https://lovdata.no/forskrift/2014-09-05-1191

Malterud, K. (2017). *Kvalitative forskningsmetoder for medisin og helsefag, 4.utgave.* Oslo: Universitetsforlaget.

MITRE ATT&CK. (2023, April 13). *attack.mitre.org*. Hentet fra https://attack.mitre.org/

Myers, M. D. (2019). *Qualitative Reseach in Business & Management 3.Edition.* London: Sage.

Nasjonal Sikkerhetsmyndighet. (2022, 10 05). *nsm.no*. Hentet fra https://nsm.no/sok/?categoryID=14&tileInstanceId=2597&q=definisjon+cyber

NIST, The U.S. National Institute of Standards and Technology. (2018, April). *Cybersecurity Framework Version 1.1.* Hentet fra https://www.nist.gov/cyberframework

NORMA. (2023). *2023 Annual Threat Assessment.* Oslo: NORMA.

NorSIS. (2023, 04 30). *Norsk senter for informasjonssikring*. Hentet fra https://norsis.no/fakta/verdikjedeangrep/

Norsk Standard. (2012). *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi NS 5830:2012.* Oslo: Norsk Standard.

NSM. (2016). *Helhetlig IKT-risikobilde 2016.* Oslo: Nasjonal Sikkerhetsmyndighet.

NSM. (2020). *Grunnprinsipper for IKT-sikkerhet v2.0.* Oslo: Nasjonal Sikkerhetsmyndighet.

Nätt, T. H. (2022, 01 21). *tastaturlogger i Store norske leksikon*. Hentet 05 23, 2023 fra snl.no: https://snl.no/tastaturlogger

Nätt, T. H. (2023, 05 23). *dataangrep i Store norske leksikon*. Hentet 05 23, 2023 fra snl.no: https://snl.no/dataangrep

Stranden, R., & Rosvold, K. A. (2023, 02 23). *sikkerhet i Store norske leksikon*. Hentet 05 23, 2023 fra snl.no: https://snl.no/sikkerhet

Svartdal, F. (2022, 06 13). *Dunning-Kruger-effekten i Store norske leksikon*. Hentet 05 23, 2023 fra snl.no: https://snl.no/Dunning-Kruger-effekten

Tam, K. H.-N. (2021). *Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. Journal of Transportation Technologies* . Plymouth: Scientific Research Publishing Inc.

Tjora, A. (2018). *Qualitative Research as Stepwise-Deductive Induction, 1.utg.* London: Routledge.

Wikipedia. (2022, 10 05). *Wikipedia.org*. Hentet fra https://no.wikipedia.org/wiki/Den_internasjonale_sj%C3%B8fartsorganisasjonen#Historie

VEDLEGG 1: NSD SIN VURDERING

Referansenummer

168640

Vurderingstype

Standard

Dato

25.10.2022

Prosjekttittel

Master i Maritim Operativ Ledelse - NTNU

Behandlingsansvarlig institusjon

Norges teknisk-naturvitenskapelige universitet / Fakultet for ingeniørvitenskap / Institutt for havromsoperasjoner og byggteknikk

Prosjektansvarlig

Marie Haugli-Sandvik

Student

Arnt Rennan

Prosjektperiode

10.11.2022 - 30.06.2023

Kategorier personopplysninger

- Alminnelige

Lovlig grunnlag

- Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet.

Det lovlige grunnlaget gjelder til 30.06.2023.

OM VURDERINGEN
Personverntjenester har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket. Personverntjenester har nå vurdert den planlagte behandlingen av personopplysninger. Vår vurdering er at behandlingen er lovlig, hvis den gjennomføres slik den er beskrevet i meldeskjemaet med dialog og vedlegg.

VIKTIG INFORMASJON TIL DEG
Du må lagre, sende og sikre dataene i tråd med retningslinjene til din institusjon. Dette betyr at du må bruke leverandører for spørreskjema, skylagring, videosamtale o.l. som institusjonen din har avtale med. Vi gir generelle råd rundt dette, men det er institusjonens egne retningslinjer for informasjonssikkerhet som gjelder.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til den datoen som er oppgitt i meldeskjemaet.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
Personverntjenester vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om: - lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen - formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål - dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet - lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), og dataportabilitet (art. 20). Personverntjenester vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13. Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32). Ved bruk av databehandler (spørreskjemaleverandør, skylagring eller videosamtale) må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29. Bruk leverandører som din institusjon har avtale med. For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema Du må vente på svar fra oss før endringen gjennomføres.

OPPFØLGING AV PROSJEKTET
Personverntjenester vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

VEDLEGG 2: INTERVJUGUIDE

Hva jeg ønsker å vite noe om	Forslag til spørsmål (Intervjuguide)
Informasjon før opptak	Fortell litt om temaet for samtalen (bakgrunn, formål) Forklar hva intervjuet skal brukes til, og forklar taushetsplikt og anonymitet Spør om noe er uklart og om intervjupersonen har noen spørsmål Informer, få samtykke til og start opptak
Personalia	Utdanning Nåværende stilling Erfaring i nåværende stilling og evt relevant tidligere erfaring
Cyber risikohåndtering på overordnet nivå	Hva er status på implementeringen av IMO2021 i rederiet pr dd? Hvilken tilnærmingsmåte har dere valgt (inhouse, konsulenter, kombinasjon)? Hvilke roller/funksjoner hos dere er med i cyberriskhåndteringsprosessen? Hvordan ser dere på relasjonen IT – OT? Kan du fortelle noe om analysetilnærmingen? (bruker dere sannsynlighet x konsekvens, eller vurderer dere verdi, kritikalitet, sårbarhet, kapasitet og intensjon?) Hvis dere gjennomfører en IKT-ROS, hvor ofte gjør dere det? Hvis dere støtter dere til et rammeverk, hvilket rammeverk?
Identifisering av egne cybersikkerhetsrisikoer	**IDENTIFISERING AV ENHETER:** Hvordan identifiserer rederiet egne enheter? Hvordan gjennomføres identifiseringsprosessen? Hvordan innhenter du informasjon du trenger? - Hva er enheter/verdier for dere? - Hvor ofte henter dere inn enhetsoversikten? o Hvordan sikrer dere endringshåndteringen? (Kommer nye enheter inn i oversikten?) **SÅRBARHETER:** Hvordan finner dere sårbarheter som er knyttet til enhetene/verdiene vi har snakket om? **TRUSSEL:** Med utgangspunkt i enhetene/verdiene og de sårbarhetene dere har; hvordan ser trussel-landskapet deres ut?

	Hvordan er bevisstheten rundt Tilgjengelighet, Integritet og Konfidensialitet? - Hvordan er bevisstheten til CIA for de ulike enhetene - Interne / eksterne trusler?
Håndtering av identifiserte cybersikkerhetsrisikoer	Hvordan foregår den videre prosessen med analyse og håndtering? Beskriv. - Hvordan utbedrer dere identifiserte sårbarheter? - Eksterne / interne aktører involvert? - Hvordan er tilnærmingen? o TEKNISK vs ORGANISASTORISK eller begge deler? (teknisk utbedring eller prosessendringer, opplæring osv?)
Opplevelsen	Hvordan oppleves prosessen med cyberrisikohåndteringen? (nytt, ukjent, eller bare nye risikoområder som må håndteres?) Hvordan opplever du kompetansen innad i rederiet?
Cyberrisiko- modenheten	Hvor moden er rederiet i forhold til IMO 2021? Hva er dine største bekymringer på dette området? Har dere det dere trenger for å tilfredsstille kravene i IMO 2021? Hvis nei, hva mangler?
Oppsummering	Er det noe du er spesielt opptatt av i forhold til det vi har snakket om? Hvorfor er dette viktig? Hva kan/burde gjøres? Oppsummere hva som er gjennomgått Har jeg forstått deg riktig? Er det noe du vil tilføye?

VEDLEGG 3: INFORMASJONSSKRIV OG SAMTYKKEERKLÆRING

Forespørsel om deltakelse i forskningsprosjektet:

«MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS»

Dette er en henvendelse til deg om å delta i et forskningsprosjekt for å fortelle om dine erfaringer med overstående tema. Dette skrivet gir deg informasjon om målet for prosjektet, og hva deltakelse vil innebære for deg.

Bakgrunn og formål
I dette studiet ønsker jeg å finne ut av hvordan rederiet utfører cyberrisikohåndteringen i sikkerhetsstyringssystemet, hvilke funksjoner/roller i rederiet som er involvert i risikohåndteringen og hvordan de involverte opplever håndteringsprosessen.

På bakgrunn av formålet med studiet ønsker jeg å intervjue 6-8 COO eller HSQE for å få kunnskap om erfaringer med overstående tema. Du kan delta i studien om du innehar en slik funksjon/rolle i dag i et rederi.

Prosjektet er en masteroppgave, som er en del av masteren i ledelse av maritime operasjoner, ved institutt for havromsoperasjoner og byggteknikk ved NTNU i Ålesund.

Hvem er ansvarlig for forskningsprosjektet?
NTNU i Ålesund er ansvarlig for prosjektet.

Hva innebærer det for deg å delta?
Jeg vil gjennomføre et intervju med deg som tar ca. 60 minutter. Dette er tenkt som en samtale der du kan fortelle fritt om dine erfaringer vedrørende overstående tema. Spørsmålene har fokus på din erfaring i forhold til tema, og hva du er opptatt av. Vår samtale vil bli tatt opp med lydopptaker.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke ditt samtykke tilbake uten å oppgi noen grunn. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan jeg oppbevarer og bruker dine opplysninger
Jeg vil bare bruke opplysningene om deg til formålene jeg har fortalt om i dette skrivet. Jeg behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Opplysningene fra deg, samt andre intervjupersoner, skal kun benyttes som grunnlagsmateriale i min mastergradsoppgave. Personopplysninger vil holdes adskilt fra øvrige data, og det er kun jeg som vil ha tilgang til disse. Lydopptaket og transkriberingen vil bli lagret passordbeskyttet på en ekstern harddisk som oppbevares innelåst. I arbeidet med datamaterialet vil jeg anvende fiktive navn på intervjupersoner. Det skal ikke være mulig å gjenkjenne deg i den ferdige publikasjonen.

Hva skjer med opplysningene dine når jeg avslutter forskningsprosjektet?
Prosjektet skal etter planen avsluttes innen utgangen av juni 20239. Da vil alt datamaterialet bli slettet, og utskrevne intervju bli makulert.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Hva gir meg rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan du finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- NTNU i Ålesund ved Marie Haugli-Sandvik (veileder), telefon: 45061300 eller epost: marie.h.sandvik@ntnu.no.
- Arnt H Rennan (student), telefon: 40084661 eller epost: arnt.h.rennan@gmail.com
- Vårt personvernombud: Thomas Helgesen, telefon: 93079038
- NSD – Norsk senter for forskningsdata AS, på epost (personvernombudet@nsd.no) eller telefon: 55 58 21 17.

Med vennlig hilsen

Arnt Holm Rennan

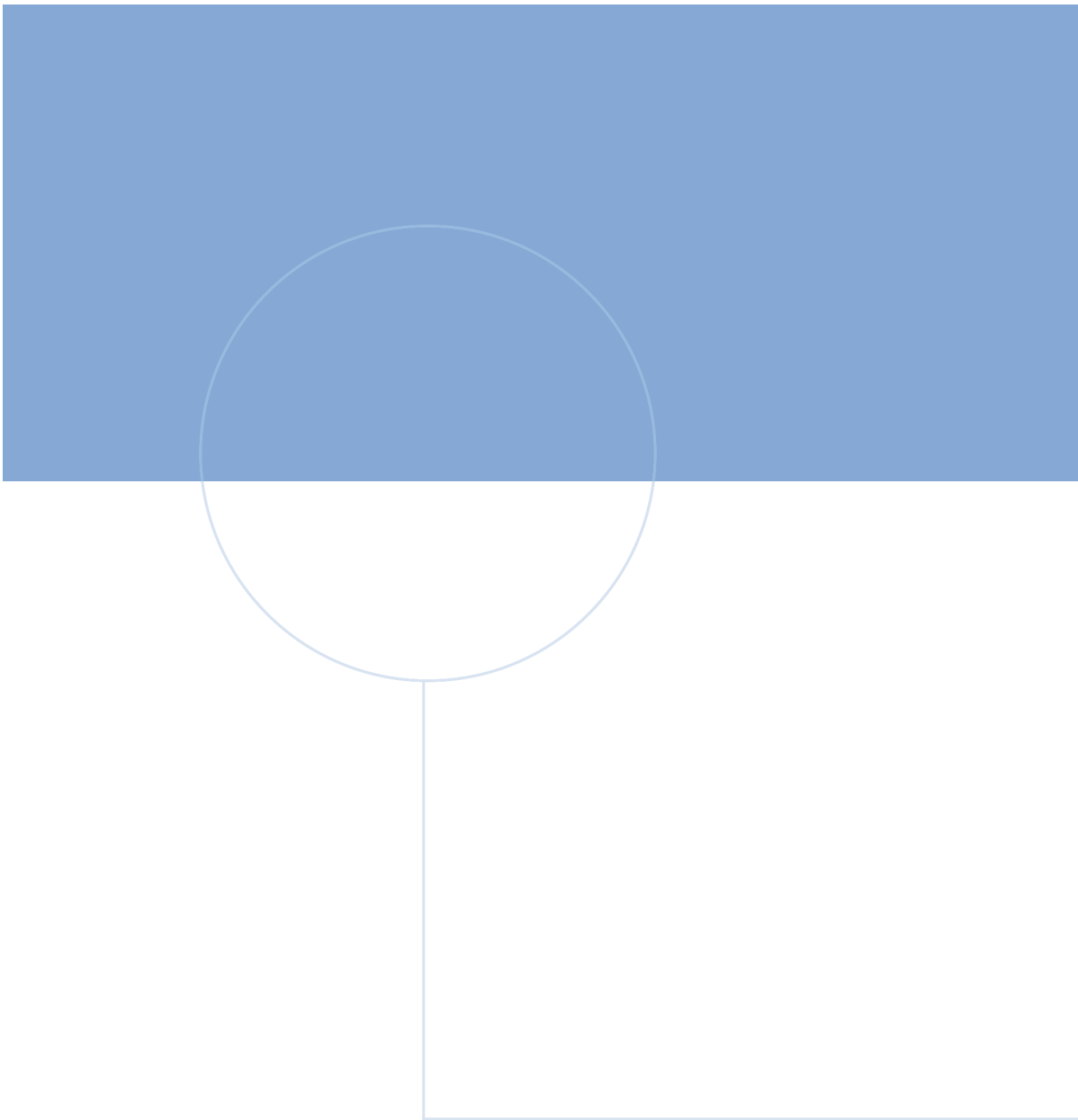
Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS», og har fått anledning til å stille spørsmål. Jeg samtykker til:

☐ å delta i intervjuundersøkelsen

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. slutten av juni 2023.

(Signert av prosjektdeltaker, dato)



NTNU

Kunnskap for en bedre verden