Emilie B. Stang, Henrik N. Vatle og Pål Utslottøy

Cybersikkerheit i maritim industri

Korleis opplever ulike aktørar innan maritim industri handteringa av cyberrisiko om bord på skip?

Bacheloroppgåve i Nautikk

Rettleiar: Marie Haugli Larsen

Juni 2021

Bacheloroppgåve

NTNU
Noregs teknisk-naturvitskaplege universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk

NTNU
Norwegian University of
Science and Technology

Emilie B. Stang, Henrik N. Vatle og Pål Utslottøy

Cybersikkerheit i maritim industri

Korleis opplever ulike aktørar innan maritim industri handteringa av cyberrisiko om bord på skip?

Bacheloroppgåve i Nautikk
Rettleiar: Marie Haugli Larsen
Juni 2021

Noregs teknisk-naturvitskaplege universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk

NTNU
Kunnskap for ei betre verd

FORORD

Denne oppgåva er det avsluttande arbeidet for tre studentar etter tre år på studieprogrammet «Bachelor i nautikk» ved NTNU i Ålesund, Institutt for havromsoperasjonar og byggteknikk.

Me vil først og fremst rette ein stor takk til rettleiar Marie Haugli Larsen. Gjennom heile prosjektet har ho vore tilgjengeleg og kome med gode tilbakemeldingar, noko som har vore av stor betydning for oppgåva. Vidare vil me takke respondentane for deira tid, slik at me kunne fullføre oppgåva.

Me tok fatt på oppgåva med lite kunnskap om maritim cybersikkerheit og om akademisk oppgåveskriving, og kan difor sjå attende på prosjektet som svært lærerikt. Valet av tema, cybersikkerheit i den maritime industrien, fall oss naturleg. Dette er eit særs aktuelt og viktig tema, noko som dei nye IMO-krava syner. Me vonar at oppgåva vil vidare belyse og understreke viktigheita av god cybersikkerheit, og at andre vil dra nytte av oppgåva i seinare tid.

Emilie B. Stang, Henrik N. Vatle og Pål Utslottøy

SAMANDRAG

Bakgrunn: IMO-resolusjon MSC.428(98) stiller krav til innføring av cyberrisiko i sikkerheitsstyringssystem om bord innan første «Document of Compliance»-revisjon i 2021. Kombinert med eit auka tal cyberåtak, har dette gjort cybersikkerheit særs relevant i den maritime industrien dei siste åra.

Formål: Formålet med studien er å avdekkje det potensielle nedslaget av dei nye IMO-krava, og undersøkje korleis dei eventuelt har hjelpt til auka medvit i den maritime industrien. Studien vil også sjå på kva for tiltak industrien har gjennomført for å imøtekome krava, og korleis cyberrisiko vert handtert om bord.

Problemstilling: Korleis opplever ulike aktørar innan maritim industri handteringa av cyberrisiko om bord på skip?

Teori: Først vert teori knytt til IMO-resolusjonen teke føre seg, etterfølgt av teori om cybersikkerheit og forskjellige typar åtak. Vidare vert IT- og OT-system teke føre seg. Deretter kjem teori om cyberrisikostyring og ei tilnærming til dette, etterfølgt av teori knytt til menneskelege faktorar. Til slutt kjem teori om opplæring om bord.

Metode: Kvalitativ metode med djupneintervju har vorte nytta. Studien sitt utval består av to dekksoffiserar, to reiarlagstilsette og éin tilsett i eit klasseselskap. Systematisk tekstkondensering er nytta i analysen av dei transkriberte intervjua.

Resultat: Funna i denne studien kan tyde på at det er varierande medvit kring cyberrisiko, men at merksemda kring temaet har auka som følgje av IMO-krava. Reiarlaga vurderer og handterer også cyberrisiko i større grad no enn før. Funna tyder likevel også på at industrien har betringspotensiale på fleire områder, som til dømes opplæring og bevisstgjering.

Konklusjon: IMO-resolusjonen har bidrege positivt for cybersikkerheita i industrien, men industrien har likevel har betringspotensiale. Industrien vil tene godt på ein ytterlegare auke av medvit kring cyberrisiko i dei komande åra, i takt med auken i talet cyberåtak.

Nøkkelord: Cyberrisiko, cyberåtak, opplæring, menneskelege faktorar, risikohandtering og medvit.

SUMMARY

Background: The IMO-resolution MSC.428(98) demands the implementation of cyber risk in safety management systems within the first "Document of Compliance" audit in 2021. Combined with an increased number of cyber attacks, this has made cyber security particularly relevant in the maritime industry in later years.

Purpose: The purpose of the study is to reveal the potential impact of the new IMO-requirements, and explore how they have eventually led to increased consciousness in the maritime industry. The study will also take a look at what measures the industry has implemented in order to meet the requirements, and how cyber risk is managed on board.

Research question: How do different stakeholders within the maritime industry experience the management of cyber risk on board ships?

Theory: Firstly, theory related to the IMO-resolution is presented, followed by theory related to cyber security and different kinds of attacks. Theory related to IT and OT systems will be presented afterwards. The study will then introduce theory related to cyber risk management and an approach to this, followed by theory related to human factors. The chapter will end with theory related to on-board training.

Method: Qualitative method using in-depth interviews has been used. This study's selection consists of two deck officers, two shipping company employees and one employee in a classification society. The analytical method used is systematic text condensation.

Findings: The findings in this study indicate that there is a variety of levels of awareness concerning cyber risk, but that the attention given to the subject has increased following the IMO-requirements. The shipping companies also have a greater focus on cyber risk than before. The findings indicate, however, that the industry has potential for improvement on several areas, such as training and raising awareness.

Conclusion: The IMO-resolution has made a positive impact on cyber security in the industry, but there is still potential for improvement. Over the next few years the industry will benefit from raising awareness related to cyber risk, in line with the increasing number of cyber attacks.

Key words: Cyber risk, cyber attacks, training, human factors, risk management and consciousness.

OMGREPSLISTE

Charter-krav	Krav i ein befraktingsavtale.
Digitalisering	Konvertering av analoge data til digitale, samt effektivisering av prosessar ved hjelp av digital teknologi (Nätt og Heide, 2015).
DOC	Document of Compliance
DP	Dynamic Positioning – Eit system som held fartøyet i ein bestemt posisjon ved hjelp av propellar (Kjerstad, 2019).
ECDIS	Electronic Chart Display and Information System
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite Systems
Hackar	Ein person som nyttar ein datamaskin til å få uautorisert tilgang til data (Nätt og Heide, 2015).
Hacktivist	Ein person som nyttar ein datamaskin til å få uautorisert tilgang til data for å fremje sosiale eller politiske føremål (Inmarsat, 2020).
HMI	Human-Machine Interaction
IAS	Integrated Automation System
IMO	International Maritime Organization
Integritet	At informasjon i IT-system alltid føreblir korrekt med omsyn til korleis den vart lagra eller sendt (Hareide *et al.*, 2018).
IT	Informasjonsteknologi – Omfattar teknologi for innsamling, lagring, behandling, overføring og presentasjon av informasjon (BIMCO et al., 2018).
MSC	Maritime Safety Committee
Multifaktor-autentisering	Ein metode for tilgangskontroll, om ein brukar ynskjer tilgang må det presenterast fleire separerte bevis for ein identitet (Braathe Gruppen, 2020).
OT	Operasjonsteknologi – Omfattar teknologi for overvaking og kontroll over utstyr, prosessar og hendingar (BIMCO et al., 2018).
SSO	Ship Security Officer
STCW	International Convention on Standards of Training, Certification and Watchkeeping for Seafarers

Tabletop-øving	Ein diskusjonsbasert øving som tek for seg ulike problemstillingar og uynskte hendingar, der ein gjennom diskusjon kjem fram til ei løysing (ESC, 2017).
TEMPEST	Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions; Elektromagnetisk stråling frå elektronisk utstyr som utilsikta kan forårsake at uvedkommande kan få tilgang til sikkerheitsgradert informasjon, samt undersøkingar og analysar knytt til slike fenomen (Forskrift om endring i Forskrift om Informasjonssikkerhet, 2012).
UNCTAD	United Nations Conference on Trade And Development.
Verdsveven	World Wide Web – Eit nettverk av websider på internett (Bergami *et al.*, 2012).

INNHALDSLISTE

FIGURLISTE

LISTE OVER TABELLAR

1.0 INNLEIING

I ei tid kor fokuset på digitalisering og bruk av nettbaserte tenester aukar, aukar også risikoen for misbruk av dette. Eit åtak mot datasystema i eit reiarlag kan resultere i store tap av både pengar og omdøme. Datakriminalitet er eit omgrep som stadig vert meir omtalt, og motiv som økonomisk gevinst, hemn, status og utpressing er like gjeldande for datakriminalitet som for kriminalitet elles (Nätt og Heide, 2015, s. 18).

Den maritime industrien er ikkje friteke frå å rette fokus mot dette, med meir teknologi om bord, og fleire applikasjonar og mediekanalar i bruk enn nokon gong før. Somme skip har dobla databruken sin kvar 6. månad. Behovet for cyber-motstandsdugleik har difor aldri vore større (Inmarsat, 2020). Risikoen relatert til cybersikkerheit vil mest sannsynleg fortsette å auke betrakteleg som eit resultat av større tillit til elektronisk handel og eit skifte mot virtuelle samhandlingar på alle plan. Dette gjev eit større spekter av sårbarheiter over heile verda, med eit potensiale til å gjere store skadar på kritiske forsyningskjeder og tenester (FN, 2020).

FN (2020) viser i rapporten «Review of Maritime Transport 2020» at over 80% av alt gods globalt, vert frakta til sjøs. Rapporten er utforma etter *United Nations Conference on Trade And Development* (UNCTAD), som vert arrangert av FN kvart fjerde år. Denne rapporten belyser kor avhengige me er av den globale handelsflåten, og at det er lite som tyder på at dette kjem til å endre seg.

Med omsyn til sårbarheita til den maritime industrien, har International Maritime Organization (IMO) innført nye retningsliner for å betre cybersikkerheita om bord. I 2017 gav dei ut ein resolusjon som la vekt på cybersikkerheit, mellom anna ved å setje krav om at eit kvart fartøy skulle implementere cyberrisiko i sikkerheitsstyringssystemet innan fartøyets første verifisering av Document Of Compliance etter 1. januar 2021 (IMO, 2017). I juni 2020 vart det rapportert ein auke på 400% i tal forsøkte cyber-åtak i den maritime industrien (Ovcina, 2020, avsnitt 1). Krava i IMO-resolusjonen, kombinert med ein stadig auke i talet cyberåtak, gjer maritim cybersikkerheit til eit særs aktuelt og interessant tema.

1.1 PROBLEMSTILLING

På bakgrunn av valt tema, cybersikkerheit i maritim industri, har me utforma følgjande problemstilling:

«Korleis opplever ulike aktørar innan maritim industri handteringa av cyberrisiko om bord på skip?»

Ved å intervjue reiarlag, seglande dekksoffiserar og andre maritime aktørar ynskjer me å sjå korleis den maritime industrien handterer cyberrisiko om bord på skip, og om dei nye krava frå IMO om cyberrisiko har auka det generelle medvitet kring temaet. Me ynskjer også å sjå på dynamikken mellom reiarlag og seglande dekksoffiserar, og korleis informasjonsflyten er dei imellom. Dei menneskelege faktorane, og påverknaden dei har på cybersikkerheita i industrien, vil også vere sentralt for oppgåva.

1.2 AVGRENSING

Dalland (2012) skriv at ved å avgrense oppgåva vert det enklare å finne relevant litteratur. Sjølv om denne problemstillinga appellerer til den maritime industrien globalt, vert ei forsking av slikt omfang vurdert som lite hensiktsmessig. Det er valt å avgrense denne oppgåva til å handle om norske dekksoffiserar om bord på norskregistrerte fartøy, samt representantar frå norske reiarkontor og nordmenn i arbeid i klasseselskap med kontor i Noreg. Denne oppgåva tek dermed utgangspunkt i nordmenn som har vore tilsette i den norske maritime sektoren, både før og etter dei nye IMO-krava tredde i kraft. Eigen kapasitet har vore ein viktig faktor i denne slutninga. Ein ser at å foreta ei forsking som omfattar heile den globale maritime industrien ville krevje tilgang til eit stort nettverk av ressursar, samt eit vesentleg større tidsrom. Den norske industrien vil dessutan vere av meir relevans for oppgåva, då kompetansen som vart bygd i forkant av oppgåva har vore hjelp av ein norsk opplæringsmodell, kor norsk teknologi og utstyr, arbeidskultur og leiingsform er i fokus.

1.3 SPRÅK OG OMSETJING

Då denne oppgåva omhandlar cybersikkerheit i maritim industri, er det viktig å merke seg at det engelske språket står svært sentralt, både i data-universet og den maritime industrien.

Danesi (2008, som sitert i Bergami, Aulino og Zafar, 2012) skriv det følgjande om det engelske språket i datasamanheng:

> Det engelske språket er heilt klart standardspråket i globale kommunikasjonar. Trollbunde av den lokkande amerikanske pop-kulturen, har ei aukande mengd unge folk over heile verda teke i bruk Engelsk, ikkje fordi det er noko betre enn deira eigne språk, men fordi det er der … overalt (Bergami, Aulino og Zafar, 2012, s. 117).

Innan internett og verdsveven hadde byrja å ta av som eit massefenomen på midten av 90-talet, hadde engelsk vorte rekna som det globale fellesspråket i fleire tiår. Ifølgje lovgjevinga er engelsk i skipsfartsindustrien kjend som maritim engelsk, og undervisninga av dette som fag på alle maritime universitet, institutt og høgskular over heile verda er styrt av IMO model course 3.17 (Maritime English). Følgjeleg har dette verdsklasse-standarddokumentet for opplæring sett ein standard for det engelskspråket som skal undervisast og meistrast for å overhalde forskrifta i maritim sektor (Sia og Said, 2018).

Grunna dette, ser ein at fleire av omgrepa, dersom omsette til norsk, ville mista deler av si tyding, grunna mangel av faguttrykk på norsk. Ettersom fagspråket opphavleg er på engelsk, vil oppgåva i fleire tilfelle behalde somme faguttrykk, kor ei norsk forklaring på uttrykka følgjer, eller vert funne i omgrepslista. Sitat vert omsette til nynorsk for å halde best mogleg språkleg kontinuitet, då skriftspråket i oppgåva er nynorsk. Dette gjeld både om det opphavlege sitatet er på engelsk og om det er på bokmål.

1.4 OPPGÅVAS OPPBYGGING

Oppgåva består av 5 hovudkapittel. I innleiinga vert oppgåva si problemstilling og rammene kring den teke føre seg. Vidare vert relevant teori presentert, som skal nyttast til drøfting av resultata seinare. Metodekapittelet tek føre seg kva for metode som har vorte nytta til innsamling og omarbeiding av data. Deretter vil oppgåva sine resultat verte presentert, og desse vert drøfta opp mot problemstillinga og det teoretiske grunnlaget i påfølgande kapittel. I siste kapittel vert oppgåva avslutta med betraktningar kring cybersikkerheita i dag og i komande tid, og med anbefalingar til vidare arbeid.

2.0 TEORETISK GRUNNLAG

I dette kapittelet vil litteraturen om temaet verte gjennomgått. Dette vert seinare nytta til drøfting av resultata i kap. *5 Drøfting*. Teori om IMO-resolusjonen og om cybersikkerheit er sentralt for oppgåva, og vert difor presenterte først. Deretter tek kapittelet føre seg teori om IT- og OT-system. Deretter kjem teori om cyberrisikostyring, og ei tilnærming til dette. Kapittelet vert avslutta med teori og menneskelege faktorar, og om opplæring om bord.

2.1 IMO-RESOLUSJON MSC.428(98)

IMO-resolusjon MSC.428(98), kalla «Maritime Cyber Risk Management in Safety Management Systems», vart vedteke av International Maritime Organization (IMO) i 2017. Denne erkjenner det pressande behovet for å heve medvit om cybertruslar og sårbarheiter for å kunne støtte trygg og sikker skipsfart, som er motstandsdugeleg mot cyberrisiko. Resolusjonen består hovudsakleg av 4 delar. Maritime Safety Committee:

1. BEKREFTAR at eit godkjent sikkerheitsstyringssystem burde ta høgde for cyberrisikostyring i samsvar med måla og dei funksjonelle krava i ISM-koden;
2. OPPFORDRAR Administrasjonar til å sikre at cyberrisiko vert riktig behandla i sikkerheitsstyringssystem, seinast ved første årlege verifisering av selskapet sitt Document of Compliance etter 1. januar 2021;
3. ANERKJENNER dei naudsynte forholdsreglar som kan verte trengt for å bevare konfidensialitet for visse aspekt ved cyberrisikostyring; og
4. OPPMODAR medlemslanda om å gjere alle interessentar oppmerksam på resolusjonen (IMO, 2017).

Resolusjonen går hand i hand med MSC-FAL.1/Circ.3, kalla «Guidelines on Maritime Cyber Risk Management.» Retningslinene gjev anbefalingar om maritim cyberrisikostyring for å verne sjøfarten mot noverande og nye cybertruslar og sårbarheiter. Retningslinene inkluderer også funksjonelle element som støttar effektiv cyberrisikostyring (IMO, 2017).

2.2 CYBERSIKKERHEIT

Nätt og Heide (2015) skildrar cybersikkerheit som di eiga medvit om kva hackarar og svindlarar kan gjere, samt korleis du kan hindre at det skjer. Cybersikkerheit er også di eiga medvit om korleis ein oppdagar at noko gale har skjedd, og korleis ein kan minimere skadane.

Prosessen for å oppnå best mogleg cybersikkerheit kan vere kompleks, og krevjar ei heilskapleg forståing for systema sine oppbygningar og sårbarheiter. Dette vert understreka ved følgjande samanlikning:

> Å sikre eit bygg kan innebere mange ulike typar tiltak. I somme tilfelle er det nok med ein dørlås eller eit gjerde, medan det i andre tilfelle vil krevjast alarm, vakthund eller vektarar. På same måte vil cybersikkerheit ha mange ulike nivå for å kunne førebygge og for å kunne rydde opp (Nätt og Heide, 2015, s.13).

Maritim cybersikkerheit kan sjåast på som ein del av den maritime sikkerheita om bord relatert til beskyttelsen mot cybertruslar for alle aspekt av maritime datasystem, særleg vedrørande integritet og tilgjengelegheit. I tillegg handlar maritim cybersikkerheit om reduksjon av konsekvensane for cyberåtak retta mot maritime operasjonar. Dermed handlar ikkje maritim cybersikkerheit berre om det teknologiske, men også om informasjon og menneske (Hareide *et al.*, 2018).

Telenor (2020) skriv på si nettside at alt for mange ser på cybersikkerheit som eit område underlagt IT-avdelinga og med svak integrasjon til resten av bedrifta. Skal ein vurdere cybertruslar på lik line med andre truslar i ein organisasjon, er dette noko alle har ansvar for, og som alle må ta omsyn til.

Under tema cybersikkerheit er det fleire omgrep som må definerast:

- *Cybertrussel* kan definerast som ein trussel som utnyttar eit datanettverk eller brukarar.
- *Cyberrisiko* er risiko som er forårsaka av ein cybertrussel.
- *Cyberhending* er ei hending kor eit datasystem, tilsikta eller utilsikta, vert utsett for ein cybertrussel.
- *Cyberåtak* er cyberrelaterte handlingar som har som hensikt å skade eit datasystem.

2.2.1 TYPAR CYBERÅTAK

Bedrifter opplever vanlegast konsekvensane for cybertruslar som økonomiske hemningar, men dette er ikkje alltid tilfellet, då gjerningspersonar mellom anna kan vere:

- Terroristar

- Hacktivist-grupper
- Nasjonalstatar
- Insider-åtak
- Datakriminelle (Inmarsat, 2020).

BIMCO (Baltic and International Maritime Council) *et al.* (2018) definerer ei rekkje typar cyberåtak i utgjevinga «The Guidelines of Cyber Security Onboard Ships», og skildrar dei som følgjande:

Ikkje-målretta åtak:

Ikkje-målretta åtak nytter ofte verktøy og teknikkar tilgjengelege på internett for å lokalisere, oppdage og utnytte utbreidde sårbarheiter som også eksisterer i eit selskap og om bord i eit skip. Døme på slike verktøy og teknikkar er:

- **Malware (skadevare):** Skadeleg programvare designa til å få tilgang til eller skade ein datamaskin utanom eigar sin kunnskap om dette. Døme på malware-angrep er:
    - **Trojanar:** Dersom skadevare skjuler seg som ein del av andre applikasjonar, vert det kalla trojanar. Programmet fungerer som det skal og verker ikkje mistenkeleg, men i det skjulte gjer det operasjonar me ikkje er klare over.
    - **Ransomware:** Ein populær svindelmetode er at skadevaren låser maskinen for bruk eller krypterer data på disken, og ein må betale bakmennene lauspengar eller gjere andre handlingar for at dei skal frigjere maskinen eller dataa.
    - **Spyware (spionvare):** Spionvare er ei eiga gruppe skadevare som i det skjulte samlar inn informasjon frå maskinen din og sender den til bakmennene. Det kan være informasjon i form av dokument, tastetrykk (ofte avgrensa til teiknsekvensar som minner om brukarnamn og passord, betalingskortinformasjon osv.), skjermbilete, opptak frå webkamera eller mikrofon, historikken til nettlesaren eller kopi av e-post du mottek/sender.
    - **Virus:** Eit virus vert kjenneteikna ved at det spreier seg kvar gong dei infiserte filene vert opna av brukaren eller systemet. Viruset spreier seg til andre filer det finn som ikkje allereie er infiserte, på din maskin og tilkopla lagringsmedium (nettverksdiskar, minnepinnar/-brikkar osv.). Målet for eit virus er at somme av

dei infiserte filene skal verte køyrde på ein annan maskin, og dermed få infisert eit nytt mål.

    - **Worms (ormar):** Ein orm kan minne svært mykje om eit virus, men er ikkje avhengig av å infisere filer som offeret distribuerer, for å spreie seg. Ein orm spreier seg ved at den på eiga hand er i stand til å finne og kontakte nye offer, for eksempel via dine lagra e-postadresser i e-postklienten, vener på sosiale medium, systemet sine lister over maskinar du har kontakta, eller ved rein gjetting. Deretter nytter den internett (til dømes e-post og deling i sosiale tenestar) og lokale nettverk til å spreie seg (Nätt og Heide, 2015).

- **Water Holing:** Etablering av ei falsk nettside eller å kapre ei legitim nettside for å utnytte intetanande besøkande.
- **Scanning:** Søk av store delar av internettet etter utnyttbare sårbarheiter ved hjelp av stikkprøvar.
- **Typosquatting:** Også kalla phishing-nettside (Omgrepet "phishing" vert definert lenger nede) eller falsk URL. Typosquatting er avhengig av tabbar som skrivefeil (derav namnet, "typo" = skrivefeil på engelsk) gjort av brukaren ved skriving av nettadresser i ein nettlesar. Skulle ein brukar med uhell skrive inn ei ukorrekt nettadresse, kan dei verte ført til ei alternativ og ofte skadeleg nettside (BIMCO *et al*., 2018).

Målretta åtak:

Målretta åtak kan vere meir sofistikerte, og nytter verktøy og teknikkar laga spesifikt retta mot eit bestemt selskap eller skip. Døme på verktøy og teknikkar brukt under desse høva inkluderer:

- **Social Engineering:** Ein ikkje-teknisk metode brukt av potensielle datakriminelle til å manipulere innsideindivid til å bryte sikkerheitsprosedyrar, normalt, men ikkje utelukkande gjennom samhandling via sosiale medium.
- **Brute Force:** Eit åtak ved å prøve mange passordkombinasjonar med håp om å til slutt gjette korrekt. Åtakaren sjekkar systematisk alle moglege passord fram til det korrekte vert oppdaga.
- **Credential Stuffing:** Ved å nytte tidlegare stolne personopplysningar eller spesifikke ofte brukte passord, kan åtakaren få uautorisert tilgang til eit system eller ein applikasjon.
- **Denial of Service (DoS):** Denne typen åtak hindrar legitime og autoriserte brukarar i å få tilgang til informasjon, vanlegvis ved hjelp av å belaste eit nettverk med data. Eit

såkalla "Distributed Denial of Service"-åtak (DDoS) tek kontroll over fleire datamaskinar og/eller serverar for å implementere eit DoS-åtak.

- **Phishing:** "Phishing" er å sende e-post til eit stort nummer potensielle mål med førespurnad om enkelte delar av sensitiv eller konfidensiell informasjon. E-posten kan også innehalde skadelege vedlegg eller førespørje at offeret besøker ei falsk nettside ved bruk av ei hyperkopling inkludert i e-posten.
- **Spear-phishing:** "Spear-phishing" er som phishing, men ofte i form av personlege e-postar, som ofte inneheld skadeleg programvare eller hyperkoplingar som automatisk lastar ned skadeleg programvare.
- **Undergraving av forsyningskjeda:** Undergraving av forsyningskjeda kan vere å angripe eit selskap eller eit skip ved å infiltrere utstyr, programvare eller tenester som skal leverast til selskapet eller skipet (BIMCO *et al.*, 2018).

2.3 IT- OG OT-SYSTEM OM BORD PÅ SKIP

Om bord deler ein teknologiske system i to kategoriar: informasjonsteknologi (IT) og operasjonell teknologi (OT). OT-systema kontrollerer dei fysiske prosessane og teknologien om bord, som til dømes ballastsensorar, navigasjonssystem og kraner, medan IT-systema kontrollerer all annan teknologi om bord relatert til informasjonsbehandling, programvare, maskinvare og kommunikasjonsteknologiar. Tidlegare har dette vore to segregerte system, men sidan desse systema i større grad har vorte kopla til internett, har systema vorte knytt tettare saman. Utviklinga har ført til at det har oppstått nye sårbarheiter, som til dømes fare for mannskap om bord, last og det marine miljøet som følgje av forstyrringar på OT-systemet (BIMCO *et al.*, 2018).

2.4 CYBERRISIKOSTYRING

Risikostyring, også kalla risikoleiing eller sikkerheitsleiing, dreier seg om å førebygge og handtere uynskte hendingar. Dette kan sjåast som ein meir avgrensa del av sikkerheitsleiing, kor ein fokuserer på konkrete teknikkar for å eliminere risiko (Borch, 2016, s. 79).

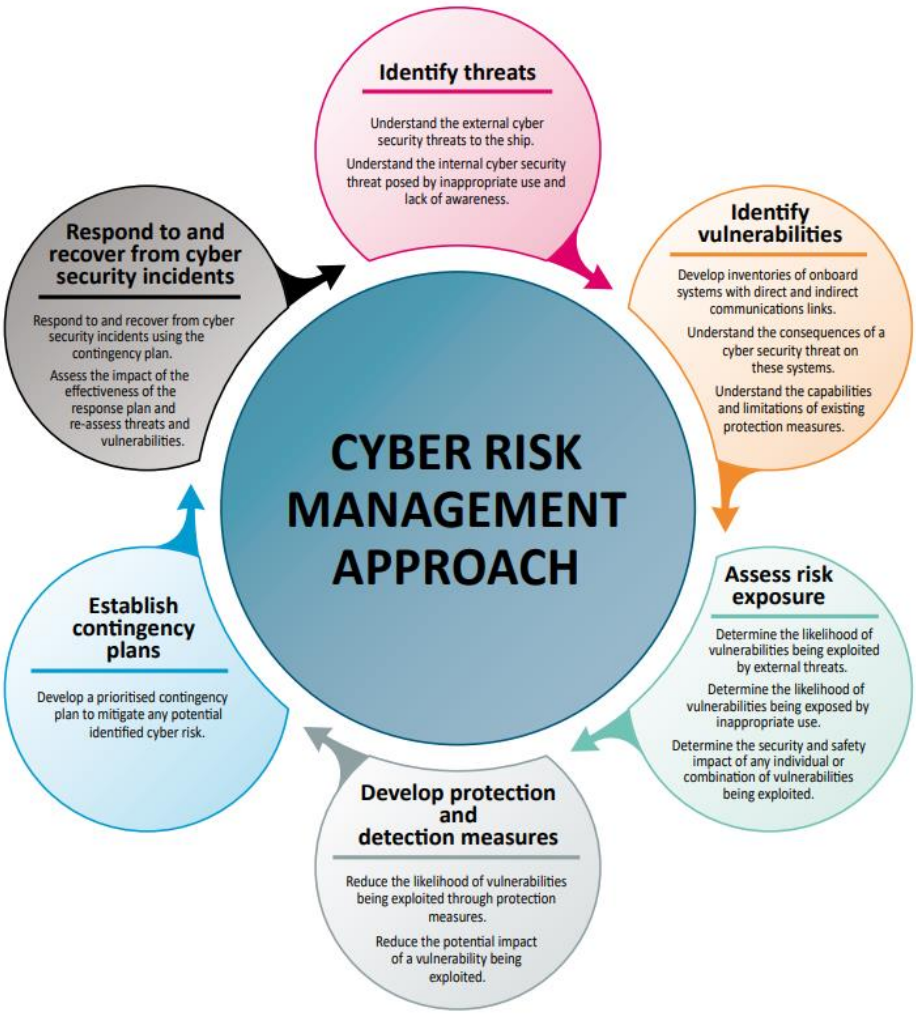
Cyberrisikostyring bør difor:

- Identifisere rollene og ansvaret til brukarar, nøkkelpersonell, og leiing både i land og om bord.

- Identifisere systema, eigedelar, data og evner, som om forstyrra kan utgjere ein risiko for skipets operasjon og sikkerheit.
- Implementere tekniske og prosedyremessige tiltak for å beskytte mot ei cyberhending og forsikre kontinuitet i operasjonar.
- Implementere aktivitetar for å førebu og respondere til cyberhendingar (BIMCO *et al.*, 2018).

2.4.1 TILNÆRMING TIL CYBERRISIKOSTYRING

I BIMCO *et al.* (2018) sin publikasjon «The Guidelines on Cyber Security Onboard Ships» kan ein finne ein modell som skildrar steg for steg korleis ein skal oppretthalde cybersikkerheita både om bord og på land. Modellen heiter «Cyber Risk Management Approach», og dei forskjellege stega innan denne tilnærminga er følgjande:



FIGUR 1: CYBER RISK MANAGEMENT APPROACH (BIMCO *ET AL.*, 2018, S. 4)

Identifisere truslar

Cyberrisikoen er spesifikk for selskapet, skipet, operasjon og/eller handel. Ved vurdering av risikoen, bør selskap ta i betraktning eit kvart spesifikt aspekt av operasjonen som kan auke sårbarheita for cyberhendingar. Ulikt andre områder for sikkerheit, der historisk bevis er tilgjengeleg, er cyberrisikostyring meir utfordrande grunna mangelen på informasjon om hendingar og deira påverknad. Innan slikt bevis er skaffa, vil skalaen og frekvensen av åtak fortsette å vere ukjend. I 2018 tok det gjennomsnittleg 140 dagar mellom infeksjonstidspunktet av eit offer sitt nettverk og oppdaginga av eit cyberåtak (BIMCO *et al.*, 2018). Det er difor viktig å vite kva risikoar som utgjer dei største truslane mot systema om bord, både med omsyn til kva type åtak som er vanlegast (ref. kap. *2.2.1 Typar Cyberåtak*) og kva type åtak som ville vore mest kritisk for selskapet, skipet, operasjonen og/eller handelen.

Identifisere sårbarheiter

Det er anbefalt at eit reiarlag på førehand gjennomfører ei evaluering av dei potensielle truslane som ein realistisk sett kan møte. Dette bør verte etterfølgt av evaluering av systema og prosedyrar om bord for å kartlegge robustheita deira i handteringa av trusselnivået. Den kan vere tilrettelagt av interne ekspertar eller støtta av eksterne ekspertar med kunnskap om den maritime industrien og nøkkelprosessane. Resultatet vert ein strategi forma kring dei største risikoane. Frittståande system vil vere mindre sårbare for cyberåtak samanlikna med dei som er kopla opp mot ukontrollerte nettverk eller direkte til internett. Aktsemd bør takast for å forstå kor kritiske system om bord kan vere når dei er tilkopla til ukontrollerte nettverk. Når ein gjer dette, bør ein ta det menneskelege elementet (ref. kap. *2.5 Menneskelege Faktorar*) i betraktning, då mange hendingar er som følgje av personale sine handlingar (BIMCO *et al.*, 2018).

Som nemnd i kap. *2.1 IMO-Resolusjon MSC.428(98)*, skal alle fartøy ha cyberrisiko implementert i sikkerheitsstyringssystema om bord. Eit sikkerheitsstyringssystem er ein dokumentert styringsreiskap som skal bidra til å gjere naudsynte avgjersler og handlingar, samt bidra til naudsynt dokumentasjon for å:

a) trygge liv og helse for passasjerar og mannskap,
b) ta vare på miljøet,
c) avverje valdelege handlingar som terror,

d) ivareta og heve kvalitetsnivået overfor kundar og andre med interesse i skipet og organisasjonen,
e) sikre og vidareutvikle materielle verdiar som eksisterer i fartøy, og
f) bidra til betring i måtar å drive på til beste for alle interessentar (Borch, 2016, s. 270).

Vurdere risikoeksponering

Cyberrisikovurdering bør starte på toppleiarnivået i eit selskap, i staden for å augeblikkeleg verte delegert til Ship Security Officer (SSO) eller leiaren for IT-avdelinga (BIMCO *et al*., 2018). Det er fleire grunnar til dette, og nokre av dei kan vere:

1. Initiativ for å betre cybersikkerheita og tryggleik kan på same tid påverke standard arbeidsprosedyrar og operasjonar, noko som gjer dei meir tidkrevjande og/eller kostbare. Det er difor ei toppleiar-avgjersle å evaluere og avgjere skadeavgrensinga.
2. Fleire initiativ for å betre cyberrisikostyringa er relaterte til arbeidsprosessar, øving, skipets tryggleik og miljøet, og ikkje til IT-system. Desse initiativa må difor forankrast organisatorisk utanfor IT-avdelinga.
3. Initiativ som aukar medvit for cybersikkerheita kan endre korleis selskapet samhandlar med kundar, leverandørar og myndigheiter, og pålegg difor nye krav til samarbeidet mellom partane. Det er ei toppleiar-avgjersle i kva grad og korleis ein gjer desse endringane i relasjonar (BIMCO *et al*., 2018).

Ved vurdering av risikoeksponering relatert til cybersikkerheit om bord i eit skip, kan følgjande spørsmål brukast som basis:

- Kva einingar er utsette?
- Kva er den potensielle verknaden til ei cyberhending?
- Kven har det endelege ansvaret for cyberrisikostyringa?
- Er OT-systema og deira arbeidsmiljø verna frå internettet?
- Er OT-systema fjernstyrte, og korleis er dei eventuelt overvakte og beskytta?
- Er IT-systema beskytta, og vert fjerntilgang overvakt og styrt?
- Kva er beste praksis for cyberrisikostyring om bord?
- Kva kompetansenivå har IT- og OT-operatørane (BIMCO *et al.*, 2018)?

Basert på svara, skal selskapet kunne delegere autoritet og avgjere det naudsynte budsjettet for å kunne halde ein full risikovurdering og utvikle dei beste løysingane for selskapet og operasjon av skipa deira. Ei risikovurdering vurderer systema om bord, for å kartleggje robustheita deira mot aktuelt cybertrusselnivå. Målet med ei slik vurdering er å identifisere alle sårbarheiter i systema. Risikovurderingar kan gjennomførast både internt i firma og av ein tredjepart (BIMCO *et al.*, 2018).

Utvikle tiltak for verning og oppdaging

Utfallet av selskapet si risikovurdering og påfølgjande cybersikkerheitsstrategi bør vere ein reduksjon i risiko, som gjer risikoen så lav som det er praktisk mogleg. På eit teknisk nivå vil dette innebere å implementere naudsynte handlingar for å etablere og ivareta cybersikkerheita. For å gjere data og utstyr motstandsdugeleg mot cyberåtak, kan det vere lurt å beskytte det med fleire lag av vernetiltak, som tek i betraktning rolla til personale, prosedyrar og teknologi for å:

- Auke sannsynet for at ei cyberhending vert oppdaga.
- Auke innsats og ressursar ein treng for å verne informasjon, data eller tilgjengelegheita til IT og OT-system (BIMCO *et al.*, 2018).

Difor er det anbefalt ein kombinasjon av følgjande tiltak:

- Fysisk sikkerheit om bord, etter skipets sikkerheitsplan.
- Vern av nettverk.
- Innbrotsdeteksjon.
- Regelmessig sårbarheitstesting.
- Godkjenning av systemvare.
- Tilgang og brukarkontroll.
- Passande prosedyrar vedrørande bruk av flyttbare medium og passordpolicyar.
- Personale sitt medvit for risikoen og kjennskap til relevante prosedyrar (BIMCO *et al.* 2018).

Identifisering av innbrot og infeksjonar er ein viktig del av kontrollprosedyrane. Ei grunnline for nettverksdrift og forventa dataflyt for brukarar og system bør vere etablert og styrt, slik at terskelen for alarm ved ei cyberhending kan etablerast. Ein ynskjer for det første å redusere

sannsynet for at sårbarheiter vert utnytta, og for det andre å redusere det potensielle tapet dersom ein sårbarheit skulle vorte utnytta (BIMCO *et al.*, 2018).

Etablere beredskapsplanar

Når ein utviklar ein beredskapsplan for eit skip, er det viktig å forstå betydninga av eit kvart cyberåtak og vurdere passande respons. I dei fleste tilfelle, med unntak av lasteplanlegging og styringssystem, vil eit tap av IT-system vere eit problem for forretningskontinuiteten, og ikkje ramme trygg operasjon av fartøyet. I slike tilfelle bør prioriteten vere å starte ei etterforsking og ein gjenopprettingsplan. Tap av OT-system kan derimot ha ein betydeleg og umiddelbar påverknad på trygg operasjon av fartøyet. Dersom ei cyberhending resulterer i tap av eller feil ved OT-system, vil det vere essensielt at effektive handlingar vert føretekne for å sikre den umiddelbare tryggleiken til mannskapet, skipet, lasta og beskyttelse av havmiljøet. Passande beredskapsplanar for cyberhendingar, inkludert tap av kritiske system og behovet for alternative operasjonsmodusar, bør vere adresserte i dei relevante operasjons- og nødprosedyrane i sikkerheitsstyringssystemet. Somme av dei eksisterande prosedyrane i eit skip sitt sikkerheitsstyringssystem dekker allereie enkle cyberhendingar. Derimot kan cyberhendingar resultere i fleire feil, som får meir enn eitt system til å stenge ned. Beredskapsplanen bør ta slike hendingar i betraktning (BIMCO *et al*., 2018).

Følgjande er ei liste over døme på cyberhendingar, som bør adresserast i beredskapsplanen om bord:

- Tap av tilgang til elektroniske navigasjonsverktøy eller tap av integritet på navigasjonsrelatert data.
- Tap av tilgjengelegheit eller integritet av eksterne datakjelder, inkludert (men ikkje avgrensa til) GNSS.
- Tap av essensiell tilkopling til land, inkludert (men ikkje avgrensa til) GMDSS system.
- Tap av tilgang til industrielle kontrollsystem, inkludert framdrift, styresystem og andre kritiske system.
- *Ransomware* eller *Denial of Service*-åtak (BIMCO *et al.*, 2018).

Respondere til og gjenopprette frå cyberhendingar

Det er viktig å forstå at cyberhendingar ikkje alltid forsvinn av seg sjølv. Vert til dømes ECDIS infisert med skadevare, kan oppstart av reserve-ECDIS-en forårsake ei anna cyberhending. Difor er det viktig å ha ein plan for korleis ein reinsar og tilbakestiller infiserte system. Kunnskap om tidlegare identifiserte cyberhendingar bør brukast til å betre responsplanane på alle fartøy underlagt reiarlaget, og ein informasjonsstrategi for slike hendingar bør vurderast. Eit team, som kan bestå av ein kombinasjon av personale på land og om bord og/eller eksterne ekspertar, bør vere etablert for å kunne gripe inn med passande handling for å tilbakestille IT- og OT-systema, slik at skipet kan fortsette med normal drift. Teamet bør kunne handtere alle aspekt av responsen (BIMCO *et al*., 2018).

Det er viktig at relevant personale gjennomfører regelmessige øvingar innan cybersikkerheit for at dei skal kunne opprettholde evna til å respondere effektivt. Cybersikkerheitsøvingar bør, om mogleg, vere inspirerte av ekte hendingar, og kan vere simuleringar av stor-skala hendingar som eskalerer til krisesituasjonar. Dette gjev dei moglegheita til å analysere teknisk avanserte cyberhendingar, men også å vektleggje moment som forretningskontinuitet og krisehandtering (BIMCO *et al.*, 2018).

Gjenopprettingsplanar bør vere tilgjengelege i papirform, både om bord og på land. Føremålet til planen er å støtte gjenopprettinga av system og data som er naudsynte for å kunne tilbakestille IT og OT til operativ tilstand. For å sikre tryggleiken til mannskapet om bord, bør drift og navigasjon av fartøyet vere prioritert i planen. Gjenopprettingsplanen bør forståast av personale med ansvar for cybersikkerheit. Kor detaljert og kompleks ein gjenopprettingsplan er, kjem an på type fartøy og kva type IT, OT og andre system som er installert om bord (BIMCO *et al*., 2018).

Etterforsking av ei cyberhending, kan gi verdifull informasjon om korleis ein sårbarheit vart utnytta. Bedrifter bør, om mogleg, etterforske cyberhendingar som rammer IT og OT om bord i samhøve med bedrifta sine eigne prosedyrar. Ei detaljert etterforsking kan krevje ekstern eksperthjelp (BIMCO *et al.*, 2018).

2.5 MENNESKELEGE FAKTORAR

Menneskelege faktorar er ein vitskapeleg, teoretisk, og anvendt disiplin som tek føre seg psykologiske, fysiske og organisatoriske aspekt ved interaksjon mellom menneske og system (til dømes teknologi), hovudsakleg i yrkesrelaterte samanhengar. Feltet utvikla seg i stor grad etter at ein innsåg at den systematiske vurderinga av det menneskelege elementet kan vere eit stort bidrag i sikkerheitskritiske område (Grech, Horberry og Koester, 2008). Innan cybersikkerheit forbind ein ofte den menneskelege faktoren med menneske sine roller i ein sikkerheitsprosess. Eit risikomoment er mennesket som eit potensielt mål for cyberåtak, eller, sjølv uvitande, som deltakar i eit cyberåtak (Von Solms og Van Niekerk, 2013).

Etter andre verdskrig, byrja forskarar å studere menneskelege faktorar, då dei såg at trass i fungerande teknologiske fly- og våpensystem, vart statistikkane for ulukker vesentlege. Eit resultat av dette var at forskarar frå begge sider av fronten byrja å forske på samanhengen mellom menneske og maskin. Det var denne typen forsking som la grunnlaget for teorien om menneskelege feil og *HMI*-relaterte feil (Human-Machine Interaction). I ein studie om menneskelege feil i den maritime industrien for US Coast Guard, fann Rothblum (u.å.) at kring 75-96% av alle tap på sjøen, i alle fall til dels, kan skuldast ein form for menneskeleg feil (Schager, 2008).

James Reason (1997, som nemnt i Grech, Horberry og Koester, 2008) utvikla ein solid og anerkjend teori om organisasjonssvikt, og peikar på følgande punkt ein bør observere i forbindelse med menneskeleg prestasjon:

- Menneskelege handlingar er nesten alltid avgrensa av faktorar utanfor individet sin umiddelbare kontroll;
- Innanfor ei dugeleg, erfaren og velmeinande arbeidsgruppe, er situasjonar meir opne for endringar enn menneska sjølve;
- Menneske kan ikkje på ein enkel måte unngå dei handlingar som dei ikkje hadde tenkt til å utføre i utgangspunktet; og
- Feil skuldast fleire årsaker: personlege, oppgåvemessige, situasjonsmessige og organisatoriske faktorar (Reason, 1997, s. 128, som som nemnt i Grech, Horberry og Koester, 2008).

Teorien kan sjåast i samanheng med ein skuld-kultur som råda i mange år, kor ulykkesetterforskingar i det maritime domenet vart etterfølgt av ei tilnærming til menneskelege feil. Eit døme på dette er etterforskinga av ulykka som råka passasjerferja *Herald of Free Enterprise*. I etterkant av ulykka var den første konklusjonen, frå reiarlagsadministrasjonen, at ulykka vart forårsaka av ein matros som hadde forsove seg, og at ulykka difor var eit resultat av ein menneskeleg feil. Det vart seinare konkludert med at det var gjennomgåande feil i heile organisasjonen, og konklusjonen spreidde synet om at sikkerheit strekk seg forbi den individuelle menneskelege feilen, og omfamnar organisatoriske faktorar, som igjen påverkar menneskeleg prestasjon. Forsking innan organisasjonssvikt har også understreka to viktige distinksjonar innan feil-typar. Forskinga syner at menneskelege feil ikkje berre er knytt til menneska på den operasjonelle sida av eit system (aktive feil), men at dei også er knytt til organisatoriske feil (latente feil) (Grech, Horberry og Koester, 2008).

Aktive feil kan difor ofte knytast til ein større og lettare identifiserbar enkeltfeil, gjort av eit menneske i samhandling med teknologi, som resulterer i ei uynskt hending eller større ulukke. Latente feil kan resultere i ei meir kompleks hendingsrekkje, kalla ei feilkjede. Ei feilkjede kan definerast som ulike mindre feil som til saman vil kunne utvikle seg til ei uynskt hending eller større ulukke (Borch, 2016, s. 115).

FIGUR 2: FEILKJEDER (BORCH, 2016, S. 115)

2.6 OPPLÆRING OM BORD

I samsvar med skipssikkerheitsloven § 19 og STCW A-1/6 kviler det på reiarlaget og skipsføraren ansvar for at skipsbesetninga får opplæring i dei oppgåvene dei skal setjast til å utføre. Slik opplæring skal gjentakast regelmessig og ved innføring av ny teknologi og/eller nye risikomoment. Denne opplæringa skal dokumenterast. For lærlingar og kadettar vil krava til lærlingen og dokumentasjonen av den vere nedfelt i opplæringsbok eller sjøfartsdirektoratet sin nettbaserte «Web-cadet». For øvingar og drillar i forbindelse med ivaretakinga av skipet sin sikkerheit er det eigne reglar for kor ofte og i kva form desse skal overhaldast (Borch, 2016).

Alle mønstrar på eit fartøy med forskjellege føresetnadar, og ein bør take omsyn til dette ved å på førehand kartlegge enkeltpersonen sin bakgrunn i forkant av opplæring. Ein bør forsikre seg om at personen har dei naudsynte kvalifikasjonane for arbeidet og opplæringa. Den enklaste måten å gjere dette på, er ved å ha ein samtale med vedkommande for å skaffe seg klarheit i personen sine kunnskapar og erfaringar, og tilpasse deretter (Borch, 2016).

Det finst fleire forskjellege måtar å lære på, og ein må prøve å finne ut kva læringsform som er mest effektiv for kandidaten. I denne samanhengen vert tre omgrep ofte brukt: *Auditiv, visuell* og *kognitiv* læring. Auditiv læring er opplæring ved å verte fortalt eller å lese, gjerne generell informasjon, og kan fungere bra for mannskap med god, relevant erfaring/teori. Visuell læring er opplæring ved å verte vist, og vert gjerne nytta til læring av metodar og prosedyrar. Denne typen læring fungerer ofte bra for mannskap med noko relevant erfaring. Kognitiv læring handlar om praktisk læring, og gjerne det ein kallar for *«learning by doing»*-prinsippet, altså å lære ved å utføre. Denne typen læring er anbefalt for mannskap som har lite eller ingen relevant kunnskap eller erfaring (Borch, 2016).

3.0 METODE

«Ein metode er ein framgangsmåte, eit middel til å løyse problem og kome fram til ny kunnskap. Eit kva som helst middel som tener føremålet, høyrer med i arsenalet av metodar» (Aubert, 1985, s. 196, som sitert i Dalland, 2012, s. 110). Dette kapittelet vil først ta føre seg valet av metode og avklaring av eigen forståing. Deretter vil det ta føre seg oppgåva si planlegging, utføring og analyse, og til slutt reliabilitet og validitet.

3.1 FORSKINGSMETODE

Malterud (2017a, s. 43) hevdar at før ein byrjar å velje metode og førebu framgangsmåte, må ein klargjere prosjektet sitt føremål, og kvifor og korleis det kan utgjere ein forskjell. Malterud hevdar også at ei gjennomarbeida problemstilling er ein viktig føresetnad for eit godt resultat. Føremålet til prosjektet og problemstillinga har difor vore i fokus ved val av forskingsmetode.

Føremålet til prosjektet er å undersøkje korleis ulike aktørar innan maritim industri opplever handteringa av cybersikkerheit om bord på skip. Dalland (2012, s.112) hevdar at dei *kvantitative metodane* har den fordelen at den gjev data i form av målbare einingar, medan dei *kvalitative metodane* tek sikte på å fange opp meiningar og opplevingar som ikkje lar seg talfeste eller måle. Med dette som bakgrunn har me vurdert kvalitativ metode som best eigna for prosjektet.

3.2 AVKLARING AV EIGEN FORSTÅING

Ifølge Dalland (2012, s. 121) er det viktig for lesaren å vite kva for posisjon forskaren har innan det feltet han/ho har undersøkt. «Målet er ikkje å eliminere betydninga av forskaren sin medverknad, men tvert imot å synleggjere denne og opne for drøfting av konsekvensane av dette» (Malterud, 2017a, s. 114). Dalland (2012) hevdar også at det forskaren ber med seg av forhistorie, kunnskap og haldningar, også verkar inn på korleis ein tolkar og tilarbeider sine data, og det vert difor viktig å avklare dette.

Forskargruppa vår består av 3 studentar i siste semester av ein bachelor i nautikk ved NTNU i Ålesund. Vår faglege bakgrunn om temaet er ikkje stor, då utdanninga har hatt lite fokus på cybersikkerheit.

Vidare har alle erfaring frå Forsvaret, derav to på seglande fartøy i Marinen og éin i Hæren. I Marinen er det veldig stort fokus på cybersikkerheit, og spesielt på TEMPEST, noko som også gjeld for Hæren. Dette har ført til at me har ei viss innsikt i og medvit om cybersikkerheit. Me har likevel ikkje arbeidserfaring frå tida då IMO-krava tredde i kraft, og dette har difor gjeve avstand til den konkrete problemstillinga. Me er alle interesserte i den operasjonelle delen innanfor det maritime, og det er difor interessant å sjå kva påverknad dei nye IMO-krava har hatt på dette.

3.3 KVALITATIVT INTERVJU

Ifølge Dalland (2012, s. 152) er føremålet med det kvalitative intervjuet å innhente skildringar av intervjupersonen sin livsverd, for vidare å kunne fortolke kva for betydning den har for den som vert intervjua. Kvale og Brinkmann (2009, som nemnt i Dalland, 2012) nyttar også omgrepet livsverdintervju når tema frå dagleglivet skal forståast ut frå intervjupersonens eigne perspektiv. Her er *livsverd* forstått som intervjupersonen si oppleving av eige liv og han eller henne sitt forhold til omgjevnadane. Vidare i studien vert livsverdintervju omtalt som djupneintervju.

Basert på dette har me funne det best å velje djupneintervju som intervjuform. Djupneintervjuet er ein planlagt og fleksibel samtale som har som føremål å innhente skildringar av intervjupersonen sin livsverd, med fokus på tolking av meininga med dei fenomena som vert skildra (Kvale og Brinkmann, 2017). Dette gjev oss tryggleik ved at intervjuet er planlagt gjennom intervjuguiden, og fleksibiliteten til å belyse nærare dei temaa som ikkje kjem opp naturleg under intervjuet.

3.4 PLANLEGGING

For å kunne sikre best mogleg svar på problemstillinga, er planleggingsfasen avgjerande (Kvale og Brinkmann, 2017). I forkant av intervjua vart det planlagt korleis me ynskte å gå fram med oppgåva. Undervegs vart avgjersler som hadde innverknad på seinare slutningar og val tekne. Korleis studien har vorte strukturert, vert presentert i dei neste delkapitla.

Dette er første gong me har rolla som forskarar som hentar inn eigne data. For å sikre at studien behandlar personvernopplysningar i tråd med personvernregelverket, søkte me til Norsk senter

for forskingsdata (NSD). Prosjektet vart godkjent av NSD (Vedlegg 1) før gjennomføring av intervjua starta. I forkant av kvart intervju vart det sendt ut ei samtykkeerklæring og nærare informasjon om oppgåva (Vedlegg 2).

3.4.1 SKILDRING AV UTVAL

Utvalet i oppgåva har vorte satt saman av intervjupersonar som er både relevante og varierte når det gjeld dei fenomena me vil undersøkje, og er difor eit strategisk utval (Malterud, 2017b). Utvalet er også basert på kven som kunne stille til intervju, og utvalet er såleis eit behagsutval. Omsyn til formålet og essensen i oppgåva har også vorte teke, og det har difor vore ynskjeleg med intervjupersonar som har sete i same stilling både før og etter dei nye IMO-krava trådde i kraft 1. januar 2021.

I kvalitative studiar er innhaldsrike data og kontekst viktigare enn representativitet og standardisering (Malterud, 2017b). Vidare har det difor vorte vurdert kva yrkesgrupper som skulle intervjuast for å tene oppgåva best, og utan å måtte intervjue for mange for å sikre tilstrekkeleg informasjonsstyrke. Ved å intervjue både dekksoffiserar, reiarlagstilsette og ein tilsett i eit klasseselskap, kan me få fleire verdifulle perspektiv på problemstillinga. I vurderinga om ein maritim aktør er av relevans for oppgåva, vil aktøren sitt arbeid med cybersikkerheit vere vektlagt.

Basert på desse faktorane, består utvalet av fem intervjupersonar. To av intervjupersonane er dekksoffiserar om bord på seglande fartøy, kor den eine er skipsførar og den andre er overstyrmann. Me intervjua også to reiarlagstilsette, med ansvar for mannskap og datasikkerheit, og éin person som er tilsett som ansvarleg for datasikkerheit i eit klasseselskap. To av personane, skipsføraren og den eine reiarlagstilsette, er tilsette i same reiarlag, og dei tre siste er tilsette i forskjellige bedrifter. Gruppa har funne dette til å vere eit føremålstenleg utval.

3.4.2 INTERVJUGUIDE

Utforminga av ein intervjuguide er ein sentral del av ei oppgåve, då den skal leie intervjuaren gjennom intervjua (Dalland, 2012). Dei overordna temaa og spesifikke spørsmåla i ein intervjuguide er til dels styrande for eit intervju, men treng ikkje å verte følgde slavisk.

Intervjuguiden er ei hjelp til å hugse dei temaa som skal takast opp, og spørsmål vert utvikla undervegs i samtalen og følgjer av dei svara som intervjupersonen gjev (Dalland, 2012).

Det vart utvikla tre forskjellige intervjuguidar (Vedlegg 3, 4 og 5); ein for seglande dekksoffiserar, ein for reiarlagstilsette og ein for tilsette i klasseselskap. Desse inneheld dei same overordna temaa, men har spørsmål med ulik vinkling for på best måte å kunne dekkje dei forskjellege ståstadane til intervjupersonane. Intervjupersonane vart ikkje tilsendt intervjuguiden på førehand, då det var ynskjeleg med mest mogleg spontane svar (Dalland, 2012). Intervjuguidane vart utforma med ein bestemt struktur; introduksjon og oppvarming, hovuddel med refleksjon, og oppsummering.

I introduksjonen av intervjua har det vorte fokusert på å «varme opp» mot hovuddelen, og å skape ein god tillit for å kunne få utfyllande, spontane og ekte svar. Det kan skiljast mellom fleire typar av intervjuspørsmål. Hovuddelen startar med *innleiande spørsmål*, og freistar å få intervjupersonen til å fortelje og reflektere opent over temaet. Der det har vore ynskjeleg med vidare belysning over eit spesielt tema, har det vorte stilt *oppfølgingsspørsmål* (Kvale og Brinkmann, 2017). Dette har vorte gjort for å få belyst dei same temaa frå forskjellege intervjupersonar, slik at det er enklare å peike ut samanhengar, likskapar og ulikskapar. Med omsyn til både eigen kompetanse og oppgåva si problemstilling, vart ikkje spørsmåla av teknisk art, men heller av ein generell og overordna art.

3.5 GJENNOMFØRING AV INTERVJU

Kontakta med intervjupersonane vart hovudsakleg oppretta via e-post. Det vart sendt e-post til aktuelle intervjupersonar, kor me i første e-post sendte eit informasjonsskriv om studien, slik at mottakar kunne gjere seg kjend med studien før dei bestemte seg for om dei ynskte å delta. Grunna smittesituasjonen og tilgjengelegheit vart alle intervjua gjennomførte over Microsoft Teams.

Datainnsamlinga vart gjennomført i ein periode på over tre veker, grunna eiga tilgjengelegheit og intervjupersonane sin arbeidskvardag. Dette gjorde at me hadde god tid til å transkribere intervjua, og eventuelt betre nokon av spørsmåla. Me fekk i tillegg god tid til førebuing mellom intervjua.

Før opptaka starta, vart formalitetar som introduksjonar, tema, samtykke til opptak, og anonymitet og teieplikt gjennomgått. Ved opptaksstart vart intervjuet innleia med spørsmål om personalia og tidlegare erfaring. Sjølv om dette er informasjon som ikkje skal nyttast i stor grad vidare, er desse spørsmåla tiltenkt å skape ein god og trygg atmosfære. Vidare vart det fokusert på å ha ein meir flytande dialog, med moglegheit for innspel som strida med den opphavlege strukturen i intervjuguidane. Ei slik tilnærming til intervju vil også gi større sjanse for spontane, levande og uventa svar (Dalland, 2012).

Alle tre studentane var til stades under alle intervjua, men arbeidsoppgåvene vart fordelte slik at éin hadde rolla som intervjuar, og dei to andre hadde rolla som observatørar. Om observatørane hadde kommentarar eller spørsmål, var det rom for innspel undervegs.

Intervjuet skal utførast på bakgrunn av ein intervjuguide, med ei gjennomtenkt tilnærming (Kvale og Brinkmann, 2017). Gjennom intervjua hadde me intervjuguiden føre oss, for å halde oversikt over spørsmåla. Intervjuguiden var ein tryggleik, då den sørgja for at temaa me ynskte svar på, vart belyste. Me valte å ikkje notere undervegs da dette kan ta fokuset vekk frå intervjupersonen. Mot slutten av intervjuet vart dei forskjellige temaa oppsummerte. Intervjupersonane vart spurde om me sat med korrekt forståing, og om han/ho ville leggje noko til.

3.6 TRANSKRIPSJON

For å klargjere materialet for analyse, vart lydfilene transkriberte til ein skriftleg tekst. Målet med transkriberinga er å på ein best mogleg måte fange opp det intervjupersonen hadde til hensikt å dele (Malterud, 2017b).

Me føretok transkriberinga av intervjua sjølve, for å kunne lære meir om eigen intervjustil. Me vil også ha ei viss forståing av dei sosiale og emosjonelle aspekta til stades ved intervjuet (Kvale og Brinkmann, 2017). Det er fleire forskjellege transkripsjonssystem å velje mellom. Me valde ein enkel transkripsjonsstrategi, då detaljar som endring i toneleie, smil, stemmevolum osv. ikkje er relevant vidare i analysen. Transkripsjonen valde me å skrive om til skriftspråket nynorsk, og me valde å behalde nokre ord og utrykk på dialekt og på maritim engelsk.

3.7 ANALYSE

Datamaterialet har vorte analysert ved hjelp av Malterud sin systematiske tekstkondensering (2017b). Systematisk tekstkondensering er ei tverrgåande samanfatning av data frå fleire intervju. Metoden er skildra steg for steg, noko som gjer at den er gjennomførleg for oss som er nye i rolla som forskarar. Den inneberer strategiar for systematisk innsamling, organisering og tolking av skriftleg materiale frå samtale eller observasjon. Analysemetoden består av fire trinn: danne seg eit heilskapsinntrykk, lage førebelse tema, samle meiningsberande einingar i kodar, og sortere kodane i subgrupper og samanfatte betydningane av disse i kategoriar (Malterud, 2017b). I dei neste delkapitla skal me gå nærare inn på korleis analysen vart utført gjennom dei fire trinna.

3.7.1 TEMA

I første trinn skal me verte kjente med datamaterialet og danne oss eit heilskapsinntrykk. Detaljane er ikkje viktige i første trinn, kor me hovudsakleg ynskjer å sjå ein heilskap. Dette vert gjort ved å lese gjennom transkripsjonane frå intervjua. Når alt er lest gjennom skal ein summere inntrykka frå datamaterialet. Det dannast eit inntrykk av førebelse temaa som vekka vår merksemd gjennom eit fugleperspektiv (Malterud, 2017b, s.99). Nokre av temaa me kom fram til var øvingar, erfaringar, policy, trusselbilete og informasjonsflyt.

3.7.2 KODING

Ifølgje Malterud (2017b) er føremålet med kodinga å identifisere meiningsberande einingar. Ein skal skilje relevant tekst frå irrelevant, og sortere den delen av teksten som kan tenkast å belyse vår problemstilling. I vurderinga av kva som var relevant og ikkje, vart utsegna i transkripsjonane vurdert opp mot temaa frå førre trinn. Dei ulike temaa freistar å spegle heilskapen i intervjua. Intervjua har ein tematisk struktur som stammar frå intervjuguidane, og temaa i kodinga liknar difor på temaa i intervjuguidane.

Kodinga vart gjort i eit nytt Word-dokument, separert frå transkripsjonane. Dette var for å sikre tilgang til ikkje-redigerte transkripsjonar. Det vart fokusert på å få ned så mykje som mogeleg for å ikkje gå glipp av meiningsberande einingar, medan me samtidig tenkte på at omfanget skulle vere overkomeleg. Det var også enkelte meiningsberande einingar som var dekkjande for fleire tema, og dei vart koda deretter.

Undervegs i kodinga vart nokre tema lagt til, då det kom fram meiningsberande einingar som ikkje nødvendigvis fall godt under nokre av dei eksisterande temaa. I desse tilfella gjekk me systematisk gjennom transkripsjonane på nytt, for å sjå om me kunne finne fleire meiningsberande einingar som fall under dei nye temaa. Ifølge Malterud (2017b, s. 100) er det ein stor fordel å gjennomføre analysen med ein annan forskar, og det var difor to i gruppa som utførte dette.

3.7.3 KONDENSERING

Ifølgje Malterud (2017b, s. 105) er målet i dette trinnet å systematisk hente ut meining ved å kondensere innhaldet i dei meiningsberande einingane som er koda saman til kondensat. Sitata frå kodinga vart beheldt i eg-form, men vart forkorta og omskrive på ein slik måte at meininga og essensen i det opphavelege sitatet vart bevart.

I byrjinga sat me opp fire kodegrupper, men enda opp med tre, då den siste kodegruppa hadde få meiningsberande einingar. Denne vart plassert som subgruppe under ei anna kodegruppe. Malterud (2017b, s. 105) hevder at det er passeleg med tre til fem kodegrupper, og fortset: «Med fleire kodegrupper enn dette er det vanskeleg å halde oversikta, og også utfordrande å nå fram til tilstrekkeleg robuste resultatpresentasjonar for kvar av dei».

I laupet av prosessen fann me ut at problemstillinga måtte omskrivast. Dette var fordi me gjennom intervjua var meir opptekne av handteringa mellom sjø og land. Difor såg me det meir føremålstenleg å endre problemstillinga til å sjå på korleis industrien har handtert dei nye IMO-krava på ein meir generell basis, i staden for å fokusere spesifikt på sikkerheitsstyringssystemet, som var den opphavelege planen.

3.7.4 SAMANFATNING

I det fjerde trinnet av analysen skal me setje saman bitane igjen, for å danne nye omgrep og framstillingar av materialet. Det skal samanfattast ein tekst kor ein som forskar tek ansvar for tolkinga av intervjupersonane, og er lojal ovanfor stemmene deira (Malterud, 2017b, s.108).

I dette trinnet skal ein nytte kondensata frå førre trinn til å lage ein samanfatta tekst for kvar subgruppe og kodegruppe. Gullsitata belyser hovudfunna i studien, og skal bestå av utdrag frå

kondensata som på best mogleg måte omtalar og oppsummerer innhaldet i temaa. Gjennom desse fire trinna er kodegruppene gjort om til kategoriar som viser til funna i studien. Avslutningsvis gjev ein kategoriane velvalte namn som presenterer innhaldet i det påfølgande avsnittet (Malterud, 2017b).

I tabellen under viser me kort korleis ein av studien sine kategoriar vart til ved å nytte Malterud (2017b) sin metode; systematisk tekstkondensering.

Trinn 1	Tema	Etter gjennomgang av datamaterialet fann me nokon førebelse tema: Tiltak og opplæring.
Trinn 2	Koding	Identifiserer meiningsberande einingar som kan passe under tiltak og opplæring. Temaa heng saman, og dannar ei ny kodegruppe: Opplæring i cybersikkerheit.
Trinn3	Kondensering	Kodegruppene vert sorterte, og innhaldet vert kondensert i tilhøyrande subgrupper.
Trinn 4	Samanfatning	Kondensata vert skrivne om til ein analytisk tekst.

TABELL 1: KORTVERSJON AV ANALYSEPROSESSEN

3.8 RELIABILITET OG VALIDITET

Reliabilitet viser til kor pålitelege resultata i studien er. Ein viktig faktor relatert til reliabiliteten, er om resultatet kan reproduserast på eit seinare tidspunkt av andre forskarar (Kvale og Brinkmann 2017). I spørsmålet om intervjupersonane ville ha endra svara sine dersom ein annan intervjuar hadde stilt same spørsmål, hevder Malterud (2017b) at forskarane sin veremåte på ein eller annan måte vil påverke forskingsprosessen eller resultatet. For oss var det difor viktig å skape tillit til intervjupersonane, slik at me hadde ein god tone gjennom heile intervjuet. Dette vart gjort ved at me lytta interesserte, og stilte oppfølgingsspørsmål.

Validiteten viser til studien sin relevans og gyldigheit (Dalland, 2012). Kvale og Brinkmann (2017) skriv om *validering i sju stadier*, som kan fungere som ein kvalitetskontroll gjennom

heile forskingsprosjektet. Funna som vert gjort undervegs i studien må sjekkast kontinuerleg, stillast spørsmål til og tolkast. Validiteten bør også kontrollerast ved å undersøkje feilkjeldene (Kvale og Brinkmann, 2017). Dette kan ein gjere ved å vere merksam på avgrensingar og svakheiter i eige arbeid (Malterud, 2013). Utforminga av intervjuguiden kan ha vore prega av eigen forståing, og tilnærming til temaet.

4.0 RESULTAT

I dette skal kapittelet skal me presentere resultata frå intervjua. Her vil dekksoffiserane, dei reiarlagstilsette og den tilsette i klasseselskapet vere representerte. I somme av subgruppene vert ikkje resultata frå den tilsette i klasseselskapet vurdert som relevant, då subgruppene berre er aktuelle for dekksoffiserar og reiarlagstilsette. Analysen av datamaterialet resulterte i tre kategoriar med tilhøyrande subgrupper.

KATEGORI	SUBGRUPPER
Opplæring i cybersikkerheit	I: Tilrettelegging for kompetanseheving II: Tiltak for auka medvit III: Cybersikkerheitsøvingar
Opplevd cyberrisiko	I: Erfaringar og trusselbilete II: Cybersikkerheitspolicy III: Svakheiter
Driftsendringar som følgje av IMO-krav	I: Dagleg handtering II: Informasjonsflyt

TABELL 2: TABELL OVER RESULTATKATEGORIANE

Vidare i dette kapittelet skal me presentere kategoriane og subgruppene i eigne delkapittel, med tilhøyrande analytiske tekstar og gullsitat.

4.1 OPPLÆRING I CYBERSIKKERHEIT

Denne kategorien handlar om opplæring, og korleis dette vert gjennomført i og utanfor reiarlaget, korleis dette vert tilrettelagt og kva for nokre tiltak som er sette i verk. Kategorien er teke med for å danne eit bilete av fokuset på mannskapet og reiarlaget sine kunnskapar kring temaa cybersikkerheit og cyberrisiko.

4.1.1 TILRETTELEGGING FOR KOMPETANSEHEVING

Dekksoffiserane svarte at dei hadde vorte pålagte å gjennomgå ein form for digitalt kurs, då dei vart spurde om dei hadde fått noko opplæring i cybersikkerheit. Dette var noko dei fekk tilsendt, anten via minnepennar, e-post eller andre medium for intern kommunikasjon i reiarlaget. Omfanget av innhald i dei ulike kursa varierte, men fellesnemnaren såg ut til å vere ein opplæringsmodul etterfølgd av oppfølgingsspørsmål. Desse vart tilrettelagte for å kunne

gjennomførast om bord, men det var også rom for å gjennomføre dei i friperiodar. Ettersom dei nye IMO-krava tilseier at ein skal ha cyberrisiko inkludert i sikkerheitsstyringssystemet, hadde dekksoffiserane også vore gjennom ei familiarisering med sjekklister relatert til datasikkerheitstiltak om bord.

Den eine reiarlagstilsette svarte at dei hadde sett i gong haldningskampanjar med ein såkalla haldningsvideo, og hadde ein strukturert og systematisk opplæringsmodul, med registrering og dokumentering av mannskap sine kunnskapar gjennom ein multiple choice-test. Den eine dekksoffiseren, som er skipsførar i same reiarlag, gav derimot uttrykk for usikkerheit kring i kva grad dei faktisk hadde vore gjennom eit nettkurs, men landa på at dei hadde vore gjennom eit e-læringskurs ei tid attende. Han hugsa då at dette var eit kurs på eit veldig overordna plan. Vedkommande meinte derimot at cyberrisikostyring var noko ein til stor grad måtte gjere seg kjent med på eiga hand, då «vegen vert til medan ein går».

Ein annan dekksoffiser gav uttrykk for at kurset dei vart tilsendt ikkje hadde vore av høg prioritet om bord, trass i merkinga «mandatory for all crew» (obligatorisk for alle i mannskapet). Kurset hadde ikkje vorte tilstrekkeleg tydeleggjort, og vart dermed av tilfeldigheit oppdaga i skipet sin eigen e-postinnboks.

Det har berre vore nemnd slike databaserte, digitale kurs, og det har ikkje vore antyding til eit tradisjonelt kursoppsett, med fysisk opplæring frå ekspertar og praktiske øvingar. Då me spurde den tilsette i klasseselskapet, som dessutan tilbyr kursing innan cybersikkerheit, svarte vedkommande at det dei tilbyr er e-læringskurs og videoar.

Gullsitat

Reiarlaget mitt kom på slutten av fjoråret med ei familiarisering, bestående av informasjon, ei sjekkliste, og nokre oppfølgingsspørsmål. Det kunne ha vore ei betre løysing på dette, då eit slikt kurs ligg på eit veldig overordna plan.

4.1.2 TILTAK FOR AUKA MEDVIT

Etter spørsmål om det har vorte innført tiltak mot cyberåtak, svarar dei reiarlagstilsette at dei mest sårbare systema ikkje er kopla opp mot internett. Ein av grunnane til dette er for å sikre

posisjonen til fartøyet om nokon uvedkomande skulle få tilgang til systema. For dei reiarlagstilsette har det vore viktig å sikre e-posten til dei tilsette både om bord og på land. Ein av dei reiarlagstilsette seier at dei har innført multifaktor-autentisering på alle e-post-brukarar, slik at ein i tillegg til eit passord treng ein sekundærkontroll, som til dømes kan vere ein telefon.

Dekksoffiserane svarte at dei både har sett og høyrt meir om cybersikkerheit i forbindelse med dei nye IMO-krava som tredde i kraft i januar 2021. Cybersikkerheit er ei vaksande problemstilling, og har vorte sett meir i fokus av reiarlaget og leiinga om bord. I forbindelse med dette har begge dekksoffiserane fått tilsendt informasjon via e-post og sikkerheitsstyringssystemet, samt vore gjennom eit e-læringsskurs. Ein av dekksoffiserane svarte at det ikkje har vore fokus på cybersikkerheit før det siste halve året og var ikkje kjend med cyberrisiko før reiarlaget sendte ut familiseringa hausten 2020.

Dei reiarlagstilsette var tydleg på at cyber-relaterte hendingar skal rapporterast på lik line med annan naud på skipet, medan dekksoffiserane ikkje såg på eit cyberåtak som like alvorleg og ville ikkje ha rapportert det som eit naudstilfelle. Likevel etterlyste ein av dekksoffiserane meir informasjon om kva som kan skje dersom ein tredjepart skulle få kontroll på skipet eller enkelte system om bord.

Gullsitat

Prosedyren vår seier at ei kvar cyberhending som ein oppfattar som ein trussel skal meldast inn på lik line med annan naud på skipet, som til dømes grunnstøyting. Det vert då iverksett eit team som set i gang med risikoreduserande tiltak. På lik line med personskade og teknisk feil, genererer me ein rapport. Denne rapporten er viktig for å iverksette umiddelbare tiltak, og hindre nye angrep.

Mannskapet om bord har til dømes ikkje dei same tilgangane som dei hadde før, og det er heller ikkje mogleg å kople seg opp med eigne einingar..

4.1.3 CYBERSIKKERHEITSØVINGAR

Ved spørsmål om det hadde vorte utført cybersikkerheitsøvingar, svarte den eine dekksoffiseren avkreftande, og stilte spørsmål til korleis dette skulle vorte gjort.

Vedkommande sa at det berre var det siste halve året dei hadde fått beskjed frå kontoret om å tenkje meir på cybersikkerheit, og la til at dette ikkje er noko som til dagleg er ein prioritet om bord. Den andre dekksoffiseren var nølande, men landa på at dei hadde vore gjennom ei tabletop-øving.

Den eine reiarlagstilsette var usikker på intervallet, men sa at dei hadde lagt inn anten årlege eller halvårlege øvingar der mannskap og reiarlagstilsette skal gjerast medvitne om truslane ein kan utsettast for, og at dei også gjennomførte tabletop-øvingar. Vedkommande la til at dei hadde hatt ei øving på byrjinga av året der dei testa dei kontortilsette for å sjå kven som ville trykkje på ein ukjend link, og at 76% hadde gjort det. Dette hadde auka medvitet til dei tilsette, som i etterkant spurde om hjelp då dei fekk e-postar dei var usikre på. Den andre reiarlagstilsette sa at dei ikkje hadde gjennomført nokon øvingar enda, men at dei har køyrt andre typar drillar med forsikringsselskap, der cybersikkerheit har vore ein liten del av drillen.

Gullsitat

Nei, det har eigentleg ikkje vore noko fokus på drillar eller øvingar. Korleis skulle ein ha gjennomført ei slik øving? Det er eigentleg berre no det siste halve året at me har fått mail frå hovudkontoret om å tenkje meir på cybersikkerheit, men det er ikkje noko som til dagleg er ein prioritet om bord.

4.2 OPPLEVD CYBERRISIKO

Denne kategorien er teke med for å syne intervjupersonane sine erfaringar med cyberåtak og deira tankar om trusselbiletet. Den vil også syne deira medvit kring cybersikkerheitspolicyen, og sjå på svakheiter dei meiner er vesentlege i forbindelse med cybersikkerheita om bord og elles i reiarlaget.

4.2.1 ERFARINGAR OG TRUSSELBILETE

Den eine reiarlagstilsette seier at reiarlaget har vorte utsett for cyberåtak. Her vart tre reiarlagstilsette offer for e-post-åtak via spam, i tillegg til éin skipsførar som vart lurt til å gje frå seg passordet sitt. Skipsføraren si e-postadresse vart vidare nytta til å sende spam, men dette vart stoppa. Trass i dette vart det likevel ikkje noko databrot, virusinfiserte datamaskiner eller noko slikt, legg vedkommande til. Han stiller seg tvilande til om dei er ein utsett aktør eller

ikkje, men legg til at sjølv om sannsynet kanskje er lite, så vil risikoen likevel vere høg då konsekvensen er høg. Den andre reiarlagstilsette seier at reiarlaget ikkje har opplevd cyberåtak, men at dei kvar veke mottek phishing-e-postar. Dette kjem til dømes i form av ein e-post frå «sjefen» med ein utbetalingsførespurnad.

Den eine dekksoffiseren har ikkje opplevd cyberåtak, og seier at han ikkje føler dei er direkte trua. Potensialet er stort, og det er mange måtar å kome seg inn på systema på, avsluttar han. Den andre dekksoffiseren har ikkje opplevd cyberåtak, men fortel om ei hending der ho og andrestyrmannen sto og følgde med på ein tollar som plugga ein minnepenn til bru-PC-en for å printe ut noko. Me vurderte om det kunne vere virus på minnepennen, men heldigvis gjekk det fint, seier ho. Ho trur ikkje reiarlaget er meir utsett enn andre reiarlag, men legg til at dei er like mottakelege for cyberåtak som alle andre, då dei har mykje utstyr om bord med internett-tilkopling.

Den tilsette i klasseselskapet seier at IMO-resolusjonen er bygd opp kring risiko, slik at kvart enkelt reiarlag må vurdere sin risiko. Vidare seier han at det på éin måte er positivt, sidan eit avansert krigsskip med eigen infrastruktur og IT-avdeling har heilt andre ting dei må implementere enn eit enkelt fiskefartøy med elektriske system utan software. På den andre sida er det negativt, då det kan vere veldig vanskeleg å vite heilt konkret kva ein må gjere. Vedkommande seier også at det er lite transparens og få arenaer for erfaringsdeling når det kjem til cyberåtak, og meiner at industrien har ein del å lære. Han nemner at det er stor transparens når det gjeld personskadar og slike ting, men at dette ikkje har kome på plass for cyberåtak. Han legg til at det er ein del initiativ frå Reiarlagsforbundet og andre aktørar, men at dette ikkje er tilstrekkeleg.

<u>Gullsitat</u>

IMO- og ISM-resolusjonen er bygd opp rund risiko, slik at kvart enkelt reiarlag må vurdere sin eigen risiko. Dette er positivt då alle reiarlag og fartøy er forskjellige, men det kan samtidig vere veldig vanskeleg for kvart enkelt reiarlag og fartøy å vite heilt konkret kva ein må gjere.

Sjølv om sannsynet for eit cyberåtak kanskje er lite, vil risikoen likevel vere høg då konsekvensen er høg.

4.2.2 CYBERSIKKERHEITSPOLICY

På spørsmålet om alle fartøya sitt på ein klar og tydeleg sikkerheitspolicy, svarar dei reiarlagstilsette at den er implementert til alle fartøy, og at alle om bord er kjend med den. Når det kjem til oppdateringar, vil dei kome i form av publikasjonar, som nye dokument, revisjonar og nytt regelverk. Vidare fortel ein av dei reiarlagstilsette at skipsførarane på dei ulike fartøya må signere på at dei har motteke og lest oppdateringane. Kor vidt skipsførarane kommuniserer dei nye endringane vidare til mannskapet, vert seinare sjekka på ein inspeksjon eller gjennom telefonsamtalar.

Dei reiarlagstilsette trekk også fram at det er vanskeleg å lage ein policy som er klar og tydleg. Difor spelar personleg tolking ei viktig rolle. Ein av grunnane til at det er vanskeleg å lage ein spesifikk plan er at ulike fartøysgrupper har ulike behov, samt at ingen cyberåtak er like. Gjennom inspeksjonar og interne kontrollar sjekkar dei mannskapet sin kjennskap til policyen om bord. Den eine reiarlagstilsette legg også vekt på at det er klare prosedyrar på somme områder, medan det på andre område er sunn fornuft som gjeld.

Dekksoffiserane fortel at policyen går ut på korleis ein skal oppføre seg i forhold til nettsurfing, nedlasting og tilkopling av eksternt utstyr til datamaskiner. Dei trekk spesielt fram at dei ikkje skal opne usikre lenkjer eller nettsider. Den eine dekksoffiseren svarar tydeleg på at det ikkje er rom for tolking når det kjem til sikkerheitspolicyen, og at den er klar og tydeleg.

Gullsitat

Det er det som er utfordringa med informasjonssikkerheit, det er no alltid tolking, bevisstgjering og haldning. Så der er det diverre personleg tolking som avgjer.

Med haldning og sunn fornuft kjem ein seg veldig langt innan cybersikkerheit. Ein skal ikkje hive seg rundt og klikke på kvar einaste lenkje. Det er ikkje ein god start, for å seie det slik.

4.2.3 SVAKHEITER

Begge reiarlagstilsette seier at den menneskelege faktoren er ein av dei største svakheitene deira. Den eine seier også at brukaren er vanskeleg å kontrollere, då det går på haldningar, kompetanse og slike ting som ikkje så lett lèt seg kontrollere. Du kan setje deg inn i alt av

regelverk, retningsliner og slikt, men det er fort brukaren og hans tilbøyelegheit som er risikoen. Han understrekar dette med følgjande kommentar: «Den største risikoen sit mellom dataskjermen og stolryggen, som me seier».

Den eine dekksoffiseren tenkjer først og fremst på bru-PC-en som står ulåst som ein svakheit. Ho fortel at når dei ligg til kai, er det tre stykk satt opp på vakt. Vedkommande har bruvakt, medan to matrosar gjer andre ting. Det hendar også at alle tre er nede i lasterommet. Om landgangen då er nede, kan nokon i teorien ta seg om bord, gå opp til brua og kome seg inn på PC-en. Ho meiner at det alltids er betringspotensiale, men ho trur det kjem til å verte vanskeleg å få til ei endring over natta med tanke på mannskapet, og kva slags vanar som er om bord i dag. Ho skyt inn at ho på ein måte er mest bekymra for alle russarane som er om bord, grunna varierande engelsk-kunnskapar og generell tankegong, og stiller spørsmål ved om dei tek temaet alvorleg nok. Den andre dekksoffiseren fortel at dei er godt førebudd når det gjeld DP-systemet, kor det ikkje er mogeleg å kople seg på utan å fysisk vri på ein brytar. Men har ein dei rette folka, så kan ein fint kome seg inn på andre system, meiner han, og trekk fram IAS-en som særs kritisk i dette høvet.

Den tilsette i klasseselskapet seier at det som kanskje er svakheita med IMO-resolusjonen er at den som skal handtere cybersikkerheit om bord, gjerne også skal handtere sikkerheit for heile skipet. Cybersikkerheita vil då forsvinne litt i mengda, meiner han. Han poengterer også at det kan vere varierande grad av kunnskap om temaet hjå desse, og at dette kan føre til feil framgangsmåte i handteringa av cybersikkerheita.

Gullsitat

Den største risikoen sit mellom dataskjermen og stolryggen, som me seier. Brukaren er vanskeleg å kontrollere, for ein er avhengig av gode haldningar og kompetanse, som ikkje alltid er like lett lèt seg kontrollere. Det er alltids betringspotensiale, men det er vanskeleg å få til ei endring over natta grunna mannskap og vanar om bord i dag.

4.3 DRIFTSENDRINGAR SOM FØLGJE AV IMO-KRAVA

I denne kategorien ynskjer me å sjå om dei nye IMO-krava har ført til auka medvit blant dei reiarlagstilsette og dekksoffiserane, samt å sjå på korleis informasjonsflyten er i reiarlaget, og korleis informasjonen vert formidla ut til fartøya og vidare til mannskapet om bord.

4.3.1 DAGLEG HANDTERING

På spørsmålet om dei nye IMO-krava har ført til auka medvit i reiarlaget, svarar dei reiarlagstilsette at temaet er ganske aktuelt på land, og vert teke opp på møter kvar veke. Dette har ført til at dei tilsette er medvitne kring eigne val på nettet, og tenkjer seg om to gongar når dei får ein mistenksam førespurnad på e-post. Som tidlegare nemnt i kap. *4.1.3 Cybersikkerheitsøvingar* har vedkommande fortalt om testar dei har utført på dei tilsette. Dette har også auka medvitet i den daglege drifta.

Når me spør korleis dette påverkar mannskapet om bord, svarar ein av dei reiarlagstilsette at dei ikkje har same forhold til trusselbiletet, då det kan vere vanskeleg for dei å omstille seg. Dei legger også til at det er gjort endringar om bord i form av tilgangar, til dømes at det ikkje lenger er mogleg å kople seg opp på systema utan at dei på land har gjeve godkjenning til det. Ei slik godkjenning må vere personleg og over telefon. Den andre reiarlagstilsette fortel at det varierer i kva grad dette er vektlagt, grunna ulik kompleksitet på fartøya.

Dekksoffiserane om bord i båtane har merka stor forskjell etter dei nye IMO-krava tredde i kraft januar 2021. Dei legg begge vekt på at det siste halve året har det vore mykje fokus på cybersikkerheit frå reiarlaget, både på e-post og gjennom andre kanalar. Ein av dekksoffiserane meiner dette har auka medvitet, men at det ikkje er noko som ho tenkjer på i det daglege. Den andre dekksoffiseren nemner at det tidlegare har vore varierande merksemd kring cybersikkerheit. Etter at cybersikkerheit det siste året har vorte meir aktuelt, har fokuset og medvitet auka. Det er ikkje noko han ofte tenkjer på, men det ligg i bakhovudet. Dekksoffiseren nemner også at tilgangane er endra, slik som dei reiarlagstilsette skildrar. Dette er for å auke mannskapet sitt medvit om at det er andre inne på systema dei nyttar.

Den tilsette i klasseselskapet fortel at IMO-resolusjonen har bidrege til merksemd kring temaet, og reiarlaga har byrja å vurdere risiko i mykje større grad. Dessutan meiner han at det framleis

er avgrensa bevisstgjering om temaa cybersikkerheit og programvare. Intervjupersonen fortel at dei nye IMO-krava har ført til auka merksemd ved at reiarlaga får nytt regelverk å stille seg til, i tillegg til charter-krav, og krav frå oljeselskap og operatørar. Ynskje om å digitalisere bedrifta er også ein stor pådrivar til å ta cybersikkerheit på alvor. Han trekk fram fire trendar som aukar medvitet: auke i IT-hendingar, nye lovar og reglar, kommersielle krav og digitalisering.

Gullsitat

Kanskje det siste halve året har det vorte meir fokus/press på cybersikkerheit, med tanke på at eg ikkje har høyrt ein drit om det før. Kontoret sa at me no måtte fokusere meir på dette, etter ei oppmoding frå Sjøfartsdirektoratet om å verte flinkare på dette med cybersikkerheit og «bla bla bla».

Det er basert på fartøystype. På nokon fartøy er det eit vekentleg tema, medan det på andre fartøy sjeldan er eit tema grunna kompleksitet, men me har alle eit betringspotensiale.

4.3.2 INFORMASJONSFLYT

På spørsmålet om korleis informasjonsflyten kring cybersikkerheit i reiarlaget er, svarar den eine dekksoffiseren at informasjonen dei får stort sett går gjennom e-post. Han føler at reiarlagsadministrasjonen ikkje «masar» for mykje om temaet og at informasjonen dei får er behovsbasert, og legg til at dei legg mykje meir vekt på andre ting. Den andre dekksoffiseren seier at det kjem mykje informasjon gjennom vedlikehaldssystemet og sikkerheitsstyringssystemet, og at det gjerne er ein del kommunikasjon kring dette. Dei kan til dømes få beskjed frå reiarlaget om å sjekke ein ny policy i systemet, følgje den opp, sjekke nye dokument i sikkerheitsstyringssystemet osv. Vedkommande har ikkje høyrt om cyberåtak mot andre fartøy i reiarlaget, men er usikker på om dette er fordi det ikkje har skjedd, eller om reiarlaget berre ikkje har kommunisert det.

Den tilsette i klasseselskapet trur at det kan variere mykje korleis eit reiarlag handterer informasjonsflyten. Han meiner at mange reiarlag sikkert har gode rutinar for kommunikasjon, godt samarbeid og dedikerte personar med ansvar for sikkerheita om bord, medan andre manglar det.

Den eine reiarlagstilsette fortel at dei har ulike system som skal kontrollere informasjonsflyten, som til dømes ulike styringssystem og støttesystemet UniSea. Det varierer kor ofte cybersikkerheit kjem opp i samtalar med dei ulike fartøya, grunna forskjelleg kompleksitet osv. Han seier at utfordringa med cybersikkerheit er at det ofte går på tolking, bevisstgjering og handlingar, sjølv om ein kanskje har klare retningsliner. Han avsluttar med at han synst informasjonsflyten er grei, og at det vert kommunisert når det kjem nye policyar. Den andre reiarlagstilsette seier at dei også nyttar styringssystem, i tillegg til rundskriv, til å informere om korleis reiarlaget skal drivast. Mannskapa må kvittere på kva dei har lese via eit elektronisk verktøy. Dei prøver også å jamleg ha samlingar med tilsette for å informere om større endringar i regelverk, og diskutere utfordringar kring dette. I reiarlagsadministrasjonen får dei stort sett informasjon frå Sjøfartsdirektoratet og andre abonnementtenestar, fortel han.

Gullsitat

Det varierer nok mykje korleis eit reiarlag handterer informasjonsflyten. Enkelte har nok gode opplegg for korleis dei snakkar saman, har eit godt samarbeid og definert ansvar for sikkerheit om bord, medan andre manglar det.

5.0 DRØFTING

I dette kapittelet skal resultata presentert i førre kapittel drøftast opp mot problemstillinga og relevant teori. Kapittelet tek føre seg dei forskjellige kategoriane og subgruppene frå førre kapittel. Somme subgrupper har mindre drøftingsgrunnlag enn andre, og vil difor verte slått saman. Kapittelet vert avslutta med ei oppsummering.

5.1 TILRETTELEGGING FOR KOMPETANSEHEVING

I intervjua med dekksoffiserane, gav dei uttrykk for at opplæring innan cybersikkerheit ikkje vart lagt mykje fokus på, og at få grep har vorte tekne for å implementere temaet som ein del av opplæringsplanen om bord. Skipsføraren som vart intervjua uttrykte dessutan usikkerheit kring om det vart innført ein modul for bevisstgjering. STCW-konvensjonen seier at ansvaret for at mannskapet får opplæring i dei oppgåvene dei skal utføre, ligg på både reiarlaget og skipsføraren (Borch, 2016). Kap. *4.1.1 Tilrettelegging for kompetanseheving* peiker på at somme grep har vorte tekne, men i kva grad det har vorte tilrettelagt for kompetanseheving innan temaet, og om det er nok, kan diskuterast.

BIMCO *et al.* (2018) skriv at cyberrisikostyring bør byrje på toppleiarnivå, og ein kan difor tenke seg at det er naturleg for dei reiarlagstilsette i administrasjonen å avgjere kva opplæring mannskapa om bord på fartøya skal måtte gjennomgå. Likevel er det viktig å understreke at det ikkje har vorte lagt eit stort press, med strenge krav, på reiarlaga. IMO-resolusjonen set nemleg berre krav om at fartøy skal ha cyberrisiko implementert i sikkerheitsstyringssystema sine, og nemner ingenting om kurs og opplæring av mannskap. Hadde maritim cybersikkerheit vorte styrka dersom alle sjøfolk vart pålagte ein standard kursmodul?

Alle mannskap, operasjonar og fartøy er ulike, og eit skreddarsydd, avansert kurs kan difor verke meir hensiktsmessig enn ein standard kursmodul. Det kan likevel vere vanskeleg for administrasjonen i eit reiarlag å kunne tilby mannskapa eit omfattande, heilskapleg kurs om cybersikkerheit, då alle cyberhendingar er ulike, og trusselbiletet konstant endrar seg. «Vegen vert til medan ein går» nemner skipsføraren i kap. *4.1.1 Tilrettelegging for kompetanseheving*, og dette er eit uttrykk som kan nyttast til å argumentere mot eit slikt kurs. Tek ein utgangspunkt i denne tankegangen, kan ei aktuell tilnærming være å etablere ein standard kursmodul, eit grunnkurs, og deretter oppdatere og fornye kunnskapar basert på fartøy- og

operasjonsspesifikke moment og endringar i trusselbilete. Denne meir spesifikke opplæringa kan til dømes vere leia av interne/eksterne ekspertar som kjenner trusselbiletet og operasjon- og fartøyspesifikke moment.

Borch (2016) deler ein læringsprosess i to delar: innlæring og modning. Han forklarer at dette har ein samanheng med at ny kunnskap eller ferdigheitar treng tid til å modnast for å «setje seg» hjå det enkelte individ. Modningsprosessen tek tid, avhengig av kva forkunnskapar ein har. Dersom ein har dårlege forkunnskapar, og får opplæring basert på mangelfullt grunnlag, vil ikkje læringa vere god, og dette fører til at kunnskapar og ferdigheiter ikkje sit godt nok. Vårt generelle intrykk er at sjøfolk i dag har avgrensa forkunnskapar innan cybersikkerheit. Dermed kan også type læringsform diskuterast. Då kognitiv læring vert anbefalt for mannskap med lite eller ingen relevant kunnskap eller erfaring, kan dette sjåast på som den mest effektive måten å danne eit grunnlag for kompetanse på. Kognitiv læring i denne konteksten, kan til dømes vere eit fysisk kurs med praktisk case-basert trening (Borch, 2016).

Det er viktig å merke seg at det, trass i dette, kjem fram i resultatdelen at det berre har vorte gjennomført e-læring om bord på fartøya. Sjølv om andre læringsmetodar gjerne ville vore meir effektive, har altså reiarlaga landa på slutninga om å nytte denne metoden. Dette kan skuldast dei generelle haldningane mot cybersikkerheit i maritim industri, men ei rekke andre aspekt bør også nemnast. Intervjupersonen som representerte klasseselskapet nemnde i kap. *4.1.1 Tilrettelegging for kompetanseheving* at dei ikkje hadde nokon annan kursmodul enn e-læringsmodulen. Kanskje dette er gjennomgåande, og at det ikkje er ein marknad for andre typar kurs? Reiarlag er ikkje naudsynlegvis interesserte i å sende mannskapet sitt til fysiske kurs dersom det ikkje er lovpålagt, då dette ofte er meir kostbart enn ein e-læringsmodul. Det har vore debattert om opplæring i den maritime industrien er meir retta mot samsvar med regelverk enn det er retta mot kompetanseheving (FN, 2020). Dessutan kan utforminga av ein fysisk kursmodul by på vanskar for kursleverandørane, då cybersikkerheit er eit omfattande emne, som heile tida endrar seg. Det er mykje teori om emnet, men det kan vere vanskeleg å legge til rette for relevante praktiske læremåtar.

5.2 TILTAK FOR AUKA MEDVIT OG CYBERSIKKERHEITSØVINGAR

Det kjem fleire gongar fram i denne oppgåva at det i det siste året har vorte eit auka fokus retta mot cybersikkerheit, og at fleire av reiarlaga har innført nye tiltak. Desse tiltaka var mellom anna kurs til mannskap, vern av nettverk, rapportering av cyberhendingar og multifaktor-autentisering. Desse tiltaka reflekterer BIMCO *et al.* (2018) sine anbefalingar om tiltak, men berre ein del av dei. Dei anbefalte tiltaka er mellom anna innbrotsdeteksjon, regelmessig sårbarheitstesting, godkjenning av systemvare, brukarkontroll og prosedyrar vedrørande bruk av flyttbare medium (BIMCO *et al.*, 2018).

Somme av dei anbefalte tiltaka kan allereie ha vore sett i verk før IMO-resolusjonen i det heile teke var eit tema, og uavhengig av krava den medførte. Her er det viktig at ein vurderer intervjupersonane sitt medvit om kva tiltak som faktisk har vorte iverksette. Prosessen i å oppnå best mogleg cybersikkerheit krev ei heilskapleg forståing for systema ein nytter sine oppbygningar og sårbarheiter (Nätt og Heide, 2015). Kanskje desse tiltaka har vore oppfatta som relevante berre på det administrative planet. Likevel ser ein i kap. *4.1.2 Tiltak for auka medvit* at dei reiarlagstilsette har påpeikt at cybertruslar skal vurderast på lik line med andre truslar i ein organisasjon, noko som inneberer at dette er noko som alle har ansvar for, og som alle må ta omsyn til (Telenor, 2020). Det kan altså sjå ut som om det her har vore dårleg informasjonsflyt mellom land og fartøy, og bevisstgjering av systema om bord ikkje har vore tilstrekkeleg. Dette kan skuldast korleis informasjon om cybersikkerheit har vore formidla, men også korleis den har vore motteke. Ein kan stille spørsmål til kva prioritet slik informasjon er av, og i kva grad den vert tydeleggjort. Det kjem også fram i intervjua med dekksoffiserane at denne typen informasjon forsvinn litt i mengda, og at det ikkje har vorte gjort merkverdige tiltak for å betre medvitet kring cybersikkerheit.

Eit tiltak som effektivt kunne både auka og ivareteke medvitet, ville vore gjennomføring av øvingar. Det kan vere ei utfordring å simulere eit cyberåtak, men eit godt døme på dette vart nemnd av ein tilsett i eit av reiarlaga, som skildra i kap. *4.1.3 Cybersikkerheitsøvingar*, kor han fortalte om eit simulert cyberåtak for å teste reiarkontoret sine kunnskapar kring cybersikkerheit. Han påstår at dei tilsette skjerpa fokuset mot cybersikkerheit etter at dei fekk sjå resultatet på øvinga, og at øvinga førte til auke i kunnskapar. BIMCO *et al.* (2018)

oppfordrar relevant personale, inkludert mannskapet om bord, til å gjennomføre øvingar innan cybersikkerheit, og anbefaler å gjennomføre øvingar inspirerte av ekte hendingar.

Som nemnd i kap. *4.1.3 Cybersikkerheitsøvingar*, stiller den eine dekksoffiseren spørsmål til korleis ei cybersikkerheitsøving skal kunne gjennomførast. Dette er eit legitimt spørsmål å stille, då det kan vere både utfordrande og ressurskrevjande å gjennomføre realistiske øvingar som speglar att reelle cybertruslar. Truslar som trojanar og spyware er designa for å jobbe i det skjulte, og kan vere vanskeleg å etterlikne (Nätt og Heide, 2015). Andre, meir tydelege truslar som ransomware, virus, worms og Denial of Service er designa for å hemme eit datasystem, og kan difor by på store ulemper dersom skipet er i ein operativ tilstand under øvinga. Dermed er det berre dei typane åtak som rettar seg mot menneskeleg åtferd ein realistisk kan gjennomføre i øvingssamanheng om bord. Døme på slike typar øvingar er social engineering, phishing og spear phishing (BIMCO *et al.,* 2018). Dessutan endrar trusselbiletet seg kvar dag, noko som gjer det vanskeleg å vere førebudd på kva type åtak ein kan vere utsett for, og korleis ein skal kunne handtere det. Difor er det vanskeleg å drille mannskap i spesifikke typar hendingar, og det er kanskje meir føremålstenleg å sørgje for kunnskapar om grunnprinsipp og generelt medvit kring åtferd bak skjermen, då mange cyberhendingar vert sette i gong som følgje av mannskap sine eigne handlingar (BIMCO *et al.*, 2018). Desse tidlegare omtalte, meir omfattande åtaka er dessutan noko ein i røynda vil løyse i samhald med eit kriseteam på land, som bør kunne handtere alle aspekt av responsen, og som med passande handling kan tilbakestille IT- og OT-systema (BIMCO *et al.*, 2018).

5.3 ERFARINGAR OG TRUSSELBILETE

I juni 2020 vart det rapportert ein auke i talet forsøkte cyberåtak på 400% sidan februar same året (Ovcina, 2020, avsnitt 1). Likevel var det berre éin av intervjupersonane som hadde erfart eit cyberåtak. I dette høvet vart reiarlaget utsett for eit spear-phishing-åtak som ramma fleire reiarlagstilsette og ein skipsførar. Fleire av intervjupersonane stiller seg også tvilande til om dei er ein utsett aktør. Kvifor er det slik?

Det kan vere ei rekkje årsaker til at ikkje fleire av intervjupersonane har opplevd cyberåtak. Éin grunn kan vere at mannskapet og dei reiarlagstilsette ikkje er klare over at dei har vorte utsette for angrep. Malware (skadevare) er døme på skadeleg programvare som er designa for

å opprette tilgang til, eller skade ein datamaskin utan at brukaren oppdagar det. Det kan også gå lang tid frå ei eining vert infisert til åtaket vert oppdaga, og i 2018 var denne tida i snitt 140 dagar (BIMCO *et al*., 2018).

Ein artikkel frå 2020 hevdar også at talet på cyberåtak retta mot maritime OT-system har auka med 900% dei tre føregåande åra, og fortset:

> I motsetning til infrastrukturen i eit IT-system, finst det ikkje eit «dashbord» i OT-systemet der operatøren kan følgje med på helsa til alle tilkopla system. Operatøren veit sjeldan at eit åtak har funne stad, og kan sjå på unormal drift som ein enkel systemfeil, og noko som kan fiksast med ein omstart. Operatøren klarar sjeldan å skilje normal drift frå unormal. Systema vert infisert, og viruset kan spreie seg vidare til IT-system. (SAFETY4SEA, 2020, avsnitt 8).

Artikkelen understrekar kor vanskeleg det kan vere for ein operatør å oppdage ein pågåande virusinfeksjon, især dei som er retta mot OT-system.

Ein annan årsak kan vere at eit slikt åtak har vorte oppdaga, men ikkje rapportert. Fleire av intervjupersonane seier at dei ikkje har høyrt om cyberåtak i reiarlaget sitt, og legg til at det kan vere grunna at det ikkje har vorte rapportert. Den eine intervjupersonen sa: «Me har ikkje motteke rapportar om cyberåtak. Om dette er fordi me har vore flinke, eller fordi fartøya ikkje rapporterer dette, veit me ikkje enno». Det kan også vere fleire grunnar til at eit oppdaga angrep ikkje vert rapportert, som til dømes manglande erfaring og kunnskap, dårlege haldningar, uklar rapporteringsmetode osv. Borch (2016) skriv følgande om ansvar for sikkerheita om bord:

> Ansvaret for sikkerheita om bord tillegger reiarlaget og alt mannskap om bord. Det er likevel skipsføraren og skipet sine offiserar som har det overordna ansvar for ein sikker drift i det laupande arbeidet. Om bord i fartøyet vil det øvste ansvaret ligge på skipsføraren og leiargruppa med overstyrmann, maskinsjef og andre avdelingsleiarar (Borch, 2016, s. 208).

Det er altså både reiarlaget og alt mannskap som har ansvar for sikkerheita om bord, men skipsføraren og skipets offiserar har det overordna ansvaret. Desse må altså fasilitere for læring,

gode haldningar, gode rapporteringsmetodar osv. Det skal vere ein lav terskel for å rapportere alle typar uhell, også dei som er cyber-relaterte (Borch, 2016).

Fleire av intervjupersonane stilte seg tvilande til om reiarlaget deira var ein utsett aktør. Den eine intervjupersonen sa: «Sjølv om sannsynet for eit cyberåtak kanskje er lite, vil likevel risikoen vere høg, då konsekvensen er høg.», og sitatet representerer godt inntrykket me fekk av dei andre intervjupersonane også. Ein er komen langt på veg ved å forstå at eit cyberåtak kan få alvorlege konsekvensar for eit reiarlag, men ein må også kunne forstå at ein sjølv er eit potensielt mål for åtaka. For å auke denne forståinga, kan det vere lurt å setje seg inn i risikostyringsarbeidet som vert gjort om bord, nemnd i kap. *2.4 Cyberrisikostyring*. Ved å kartleggje alle måtar eit fartøy kan verte utsett for åtak på, kan ein sitje igjen med eit klarare trusselbilete.

Den tilsette i klasseselskapet meiner at det finst få arenaer for erfaringsdeling, og generelt lite transparens når det kjem til cyberåtak. Det er til dømes stor transparens når det gjeld HSE-hendingar, altså personskadar osv., men dette har ikkje kome på plass for cyberhendingar. Ein grunn til dette kan vere manglande kunnskap og erfaring om temaet. Veit ein ikkje at ein har vorte utsett for eit cyberåtak, kan ein heller ikkje rapportere eit cyberåtak. Ein annan grunn kan vere at reiarlaga ikkje har lyst til å snakke om noko dei ikkje har kontroll på, meiner vedkommande. Eit reiarlag kan også vere tilbakehaldne grunna omdømmetap. Dei kan altså risikere å miste oppdrag, og følgeleg inntekter, om det kjem fram i offentlegheita at reiarlaget har vore råka av eit cyberåtak. I ein artikkel hevdar Bradley (2019) at fullstendig transparens og openheit har sine fordelar, men at det også kan få negative konsekvensar for enkelte industriar i somme situasjonar. Artikkelen fortset:

> Mange organisasjonar er tilbakehaldne når det gjeld å dele informasjon om deira cybersikkerheit eller om truslar dei står ovanfor. Dei fryktar at å avsløre detaljar om sikkerheitsinfrastrukturen deira opnar for større risiko, og dette kan faktisk vere sant… Eit cyberåtak er som eit puslespel. Informasjon som vert samla om cyberåtak, og identifiserte sårbarheiter i selskapa, er som individuelle puslebitar. Problemet er at ingen av dei utsette selskapa veit korleis heile biletet ser ut, og puslebitane dei har samla gjev ikkje meining i seg sjølv. Om selskapa er opne med kvarandre og deler

informasjon, kan industrien i sin heilskap kome fram til avgjerande detaljar om komande cyberåtak, og vere betre førebudd på åtaka (Bradley, 2019, avsnitt 8).

5.4 SVAKHEITER

Resultata syner at begge reiarlagstilsette peikar ut den menneskelege faktoren som ei stor svakheit i cybersikkerheita i reiarlaget. Den eine reiarlagstilsette sa: «Den største svakheita sit mellom dataskjermen og stolryggen», noko som illustrerer poenget godt. Rothblum (u.å.) fann at mellom 75-96% av alle tap på sjøen, i alle fall til dels, kan skuldast ein form for menneskeleg feil (Schager, 2008). Det vert desto meir interessant å sjå på kvifor menneskelege feil, eller feil generelt, oppstår.

Den eine dekksoffiseren peikar ut bru-PC-en, og rutinane kring bruvakt til kai som ei svakheit. Ho fortel at bru-PC-en står ulåst, og at uvedkommande kan få tilgang til den om dei ligg til kai med landgangen nede, og brua ikkje er bemanna. Ho fortel også at dette skjer frå tid til annan. Dette dømet kan sjåast som ei feilkjede, nærare skildra i kap. *2.5 Menneskelege faktorar*. Her er den ulåste bru-PC-en eit uheldig val, og går under «Latent feil». Det at brua er ubemanna medan landgangen er nede, er ei rutine som ikkje vert følgt, og går under «Feil i handlingar». Det at uvedkommande kan få tilgang til den ulåste bru-PC-en, vil følgeleg vere siste ledd i feilkjeda. Ved å eliminere eitt av dei føregåande ledda, altså «Latent feil» eller «Feil i handlingar», kan ein bryte feilkjeda i si heilheit (Borch, 2016).

Teorien syner at det vert for enkelt å peike på menneskelege feil som opphavet til ulykker og uhell, og at ein bør sjå nærare på organisasjonen i sin heilskap for å finne kva som ligg til grunn for feila. I dømet ovanfor vert brua av og til ståande ubemanna. Utan kontekst, kan dette fort sjå ut som menneskeleg feil, men ein bør hugse på at det kan ligge meir bak. Kva om fartøyet er underbemanna, og den som eigentleg sit bruvakt er nøydd å forlate brua for at fartøyet skal kunne oppretthalde normal drift? Kva om reiarlaget ikkje har gjeve føringar på at bru-PC-en skal ha passord? Ein feil har fleire årsaker: personlege, oppgåvemessige, situasjonsmessige og organisatoriske faktorar. Ein menneskeleg feil kan heller ikkje berre verte knytt til mennesket i den operasjonelle delen av eit system, men også til organisatoriske feil (Grech, Horberry og Koester, 2008).

Den tilsette i klasseselskapet peika på ei svakheit i arbeidet med sikkerheitsstyring i forbindelse med IMO-krava. Han sa at personen som skal handtere cybersikkerheit om bord, gjerne også skal handtere all anna sikkerheit, og at cybersikkerheita vert nedprioritert som følgje av dette. Han meinte også at kunnskapen til personen ville vere av vesentleg betydning. Ifølgje Borch (2016, s. 209) vil det på større fartøy, og særleg på passasjerfartøy, vere ein sikkerheitsoffiser som skal følgje opp sikkerheitsarbeidet om bord. Han peikar også ut faktorar som utdanning, erfaring og medvit som viktige i forbindelse med korleis menneska observerer og handlar. Om ein då samanliknar cybersikkerheitsstyringa på eit stort passasjerskip, som til dømes eit cruiseskip, med ein fiskebåt, kan ein sjå på to forskjellige tilnærmingar til arbeidet.

Vedkommande nemnde også ein ibuande svakheit i IMO-resolusjonen (kap. *2.1 IMO-Resolusjon MSC.428(98)*), i at den kan vere open for tolking. Ser ein nærare på resolusjonen, vil ein sjå at den ikkje stiller spesifikke krav til korleis eit reiarlag skal gå fram for å vere i samsvar med den. Dette er positivt for somme, då den gjev naudsynt fleksibilitet til at ein sjølv skal kunne vurdere kva tiltak ein bør implementere. For andre reiarlag vil det likevel vere uklart kva tiltak ein bør implementere for å samsvare med resolusjonen. Han legg til at ei sterk tolking av resolusjonen kan vere at reiarlaget bør utnemne ein person om bord med ansvar for cybersikkerheit, implementere gode tiltak, og drive opplæring av mannskap og tilsette på land, medan ei svak tolking kan vere at reiarlaget berre køyrer opplæring. Det vil også vere vanskeleg for IMO å lage ein resolusjon som skal vere spesifikk, men som samstundes er tilsikta alle typar fartøy og reiarlag. Ein av grunnane er at det er vanskeleg å stille krav til spesifikt utstyr, då det kjem nytt utstyr heile tida. Det som kanskje er eit større problem, er at det er mange fartøy som seglar med gamal teknologi. Nye fartøy vert gjerne utrusta med ny teknologi, medan eldre fartøy kanskje ikkje har ressursar til å oppgradere teknologien dei har om bord. I 2020 var 39,5% av norskeigde skip i handelsflåten, registrert i Norsk Ordinært Skipsregister (NOR), 30 år eller eldre (SSB, 2021).

5.5 MEDVIT

IMO-resolusjonen sitt føremål er at alle reiarlag, uansett omfang, skal auke medvitet kring cybersikkerheit, gjennom å bekrefte, oppfordre, anerkjenne og oppmode den maritime industrien (IMO, 2017). Intrykket ein sit igjen med etter intervjua er at cybersikkerheit har vorte diskutert blant dei reiarlagstilsette dei siste månadane, i forbindelse med IMO-

resolusjonen. Det ser ut til at dekksoffiserane har lagt merke til ein auke i fokus kring temaet, men at dette ikkje er noko dei tenker på i dagleg drift. Ein kan difor diskutere om reiarlaga har gjort nok for å betre medvitet kring temaet, og om tiltaka dei har iverksett har hatt ein innverknad på haldningane til mannskapa om bord.

Trass i at det i intervjuet med skipsføraren kjem fram at han ynskte å vite meir om kva som kunne skje om nokon fekk tilgang til systema, fekk me inntrykk av at han ikkje var bekymra for cyberrisiko i same grad som for andre risikoar om bord. Begge dekksoffiserane nemnde at cybersikkerheit ikkje er noko dei tenker på i dagleg drift, og dette kan skuldast usikkerheit kring ansvarsområde. Telenor (2020) skriv at mange ser på cybersikkerheit som eit område underlagt IT-avdelinga, og at om ein skal vurdere cybertruslar på lik line med andre truslar i ein organisasjon, er dette noko alle har ansvar for, og som alle må ta omsyn til.

Gjennom familiarisering, nettkurs og nokre tabletop-øvingar har mannskapet om bord fått ei enkel innføring i dei nye IMO-krava. Dette har vore noko som administrasjonen på land har sendt ut det siste halve året. Ingen av dekksoffiserane gav uttrykk for at innføringane dei hadde fått, var noko dei sjølv hadde etterspurt. På den eine sida kan dette tyde på at skipsførarane har gjort for lite for å tileigne seg naudsynte kunnskapar om temaet. Ansvaret for at skipsbesetninga får naudsynt og relevant opplæring, kviler nemleg på både reiarlaget og skipsføraren (Borch, 2016). BIMCO *et al.* (2018) anbefaler på den andre sida at initiativet for å betre cyberrisikovurdering bør kome frå leiinga i reiarlaga.

I intervjua med reiarlaga vart det uttrykt ei uro for mannskapet om bord, mellom anna med kommentaren: «Det kan vere vanskeleg for dei om bord å omstille seg når dei får nye krav som må implementerast relativt fort.». Dette kan vere fleire årsaker til, som til dømes manglande forståing, avgrensa IT-kunnskapar og få øvingar retta mot cyberrisiko. IMO-resolusjonen oppfordrar reiarlaga til å auke medvitet til mannskapa om bord på skip (IMO, 2017). Det er derimot ingen krav til korleis ein skal auke medvitet, eller korleis opplæringa skal gå føre seg, då dette kjem fram som ei anbefaling. Ein tilsett i eit av reiarlaga som vart intervjua sa følgjande om nye krav og reglement: «Me har god tid heilt til alt kjem inn.», noko som kan tyde på at reiarlaga handlar i siste sekund, og ikkje før faktiske krav vert innførte. Han drog fram multifaktor-autentisering som eit døme på tiltak dei iverksette som følgje av IMO-krava. Sjølv

om dei hadde kjent til krava i nesten eit år, handla dei ikkje før i slutten av 2020, då krava tredde i kraft 1. januar 2021.

Resultata tyder på at IMO-resolusjonen har bidrege til auka merksemd kring cyberrisiko, men varierande medvit kring temaet. Dette understrekar også den tilsette i klasseselskapet under intervjua. Nytt regelverk, krav frå operatørar og charter-krav har ført til ein prosess hjå reiarlaga, kor dei i mykje større grad har måtte vurdere cyberrisiko som ein del av trusselbiletet. Dette er ein prosess som må forankrast utanfor IT-avdelinga, altså organisatorisk (BIMCO *et al.*, 2018). Det er her SSO kjem inn og kan bidra med å gje råd til administrasjonen om korleis ein kan forbetre arbeidsprosessar, øvingar og generell tryggleik om bord (Borch, 2016). Likevel krev dette at skipsleiinga har god kunnskap til dei nye krava og medvit kring cyberrisiko om bord. Intervjua kan indikere at dei har avgrensa kunnskap om tema, og ikkje har noko forhold til korkje leverandørar eller kundar som stiller desse krava.

5.6 OPPSUMMERING

I dette delkapittelet følger ei oppsummering av dei føregåande drøftekapitla, der hovudpunkt vil verte trekt fram.

STCW-konvensjonen seier at ansvaret for at mannskapet får opplæring i dei oppgåvene dei skal utføre, ligg på både reiarlaget og skipsføraren (Borch, 2016). Likevel kan det sjå ut til at cybersikkerheit ikkje er eit område kor skipsførarane har teke grep. Opplæringa om bord er dessutan prega av erfaringar, og slik det kjem fram i denne studien, har dekksoffiserane avgrensa erfaring å vise til. BIMCO *et al.* (2018) skriv at cyberrisikostyring bør byrje på toppleiarnivå, og dette tyder på at det kan vere reiarkontoret si oppgåve å sørgje for opplæringa. Dette har dei gjort ved å setje i verk nettbaserte kurs.

Det generelle intrykket som har vorte gitt, er at desse kursa har forsvunne litt i mengda, og gjerne ikkje vore av ein klar viktigheitsgrad. Borch (2016) skriv at den beste læringsforma for mannskap med lite eller ingen relevant kunnskap eller erfaring, er den kognitive læringsforma. Det ser diverre ikkje ut til å vere ein marknad for slike typar kurs, då kurs om cybersikkerheit ikkje kjem fram som eit krav i IMO-resolusjonen.

Ein viktig faktor til at cyberåtak førekjem, er den menneskelege faktoren, og at menneske opptrer uforsiktig bak skjermen. Difor kan eit viktig preventivt tiltak vere å sørgje for at mannskap har kunnskap om grunnprinsipp og medvit kring åtferd bak skjermen, og kjenner til dei aktuelle sårbarheitene, samt tiltak for å redusere risiko. Dette kan gjerast både ved kursing og øvingar. Skulle eit cyberåtak likevel førekome, vil det vere føremålstenleg å få støtte frå eit kriseteam på land. Det er då ein fordel at mannskapa allereie har oppretta eit forhold til teamet, for å oppnå ein effektiv dialog med dei.

I juni 2020 vart det rapportert ein auke i tal forsøkte cyberåtak med 400% sidan januar same året (Ovcina, 2020, avsnitt 1). Trass i denne statistikken, svarte berre éin av intervjupersonane at dei hadde opplevd cyberåtak i reiarlaget. I 2018 tok det gjennomsnittleg 140 dagar mellom infeksjonstidspunktet av eit offer sitt netverk og oppdaginga av eit cyberåtak (BIMCO *et al.*, 2018). Denne statistikken kan tyde på at det kan vere vanskeleg å oppdage eit cyberåtak, og at reiarlag ikkje naudsynlegvis er medvitne om pågåande truslar.

Den menneskelege faktoren har vore sentral i denne oppgåva. Dette vert mellom anna illustrert ved kommentaren «Den største svakheita sit mellom dataskjermen og stolryggen» i intervju med ein tilsett i ein av reiarlaga. Rothblum (u.å.) fann i ein studie at mellom 75-96% av alle tap på sjøen, i alle fall til dels, kan skuldast ein form for menneskeleg feil (Schager, 2008). Alle intervjupersonane gav inntrykk for at dei var kjende med det menneskelege elementet som ein svakheit. Den eine dekksoffiseren peikar på tekniske feil, medan den andre peikar på rutinar som ikkje vert følgt, som svakheiter. Begge desse kan sjåast i samanheng med feilkjeder, nærare skildra i kap. *2.5 Menneskelege faktorar*.

I kva grad IMO-resolusjonen direkte har auka medvitet kring temaet, er også viktig å ta føre seg. Det ser ut til at den generelle merksemda rundt emnet har auka, men medvitet kring bruk av datasystem ser framleis ut til å vere varierande. Brukarar oppfattar gjerne cybersikkeheit som noko som berre er underlagt IT-avdelinga. Ein svakheit med IMO-resolusjonen er dessutan at den er open for tolking, noko som har gjort at tiltak som har vore iverksette, har vore avhengig av dei enkelte reiarlaga sine tilnærmingar.

6.0 AVSLUTNING

Hensikta med denne studien har vore å gi eit inntrykk av korleis ulike aktørar innan den maritime industrien opplever handteringa av cyberrisiko om bord på skip, og korleis synet på cybersikkerheit om bord har vorte endra det siste året, som følgje av at IMO Resolution MSC.428(98) tredde i kraft 1. januar 2021.

Studien har gjeve eit innblikk i korleis den maritime industrien har handtert IMO-krava. Studien sine funn, presentert i resultatkapittelet og drøfta i påfølgande kapittel, tyder på at medvitet kring temaet er varierande, men at merksemda har auka som følgje av krava. Ein ytterlegare auke i medvit vil vere naudsynt i dei komande åra, då talet på cyberhendingar heile tida aukar, og lite tyder på at denne trenden vil snu.

Funna i denne studien gjev rom for betring, og ein har sett at det i stor grad handlar om opplæring, medvit og kommunikasjon. Enkelte tiltak kan implementerast, både overordna i den maritime industrien, og internt i reiarlag, for å endre desse haldningane og auke medvitet. Anbefalingane er baserte på ulike moment som vert drøfta i dette kapittelet, og er som følgjande:

- IMO bør legge til rette for eit grunnkurs i cybersikkerheit etter ein STCW-standard, anten som ein del av utdanningsløpet, eit sjølvstendig kurs eller som ein del av det grunnleggande sikkerheitskurset deira.
- Øvingar retta mot cyberrisiko bør verte meir vektlagt både om bord og i reiarlaget. Desse kan gjennomførast i samhald med eit kriseteam, som kan vere IT-avdelinga og/eller interne/eksterne spesialistar. På denne måten kan øvingane verte meir relevante og realistiske.
- Reiarlaget bør sørgje for at fartøya er i regelmessig dialog med kriseteamet, for å kunne oppnå ein betre kommunikasjonsflyt mellom begge partar ved ei cyberhending, samt ein lågare terskel for å opprette kontakt.
- Det bør opprettast eit register kor alle reiarlag kan rapportere inn cyberåtak dei vert utsett for. Registeret børe vere ope, slik at det vert meir openheit kring temaet, og ein kan lære av kvarandre sine feil eller manglar.

REFERANSAR

Bergami, R., Aulino B. og Zafar, A. (2013) *The Influence of Cyber Language on Adolescents Learning English as a Second Language: Voices from Italy and Pakitan.* Champaign: Common Ground Publishing LLC.

BIMCO, CLIA, ICS, Intercargo, Intermanager, Intertanko, (…) World Shipping council. (2018). *The Guidelines on Cyber Security Onboard Ships.* 3. utg. In: Bagsvaerd.

Borch, O. J. (2016) *Fartøysledelse og kontroll av skipets drift: For maritime studier.* Bergen: Fagbokforlaget.

Braathe Gruppen (2020) *Multifaktorautentisering: Hvorfor skal du aktivere det også på dine private kontoer?* Tilgjengeleg frå: https://braathe.no/to-faktor-autentisering-hvorfor-skal-du-aktivere-det-ogsa-pa-dine-private-kontoer/ (Henta: 26. mai 2021)

Bradley, T. (2019) *Greater Transparency Leads to Better Cybersecurity*. Tilgjengeleg frå: https://securityboulevard.com/2019/04/greater-transparency-leads-to-better-cybersecurity (Henta: 27. mai 2021)

Dalland, O. (2012) *Metode og oppgaveskriving*. 5. utg. Oslo: Gyldendal Norsk Forlag AS.

ESC (2017) *Beredskapsøvelser og læring*. Tilgjengeleg frå: https://www.einangsafety.no/blog/beredskapsovelser-og-laering (Henta: 15. mai 2021).

FN (2020) *United Nations Conference on Trade and Development: Review of Maritime Transport 2020*. New York: United Nations Publications.

Forsvarsdepartementet (2012) *Forskrift om endring i forskrift om informasjonssikkerhet*. Tilgjengeleg frå: https://lovdata.no/dokument/LTI/forskrift/2012-06-22-653 (Henta: 15. mai 2021).

Grech, M. R., Horberry, T. J. og Koester T. (2008) *Human factors in the maritime domain*. Boca Raton: Taylor & Francis Group.

Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R. Og Helkala, K. (2018) *Enhancing Navigator Competence by Demonstrating Maritime Cyber Security.* Tilgjengeleg frå: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2598842 (Henta: 20. mai 2021).

IMO (2017) *Guidelines on Maritime Cyber Risk Managment*. Tilgjengeleg frå: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf (Henta: 15. mai 2021).

IMO (2019) *International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978*. Tilgjengeleg frå: https://www.imo.org/en/OurWork/HumanElement/Pages/STCW-Convention.aspx (Henta: 15. mai 2021).

Inmarsat (2020) *Cyber security recuirements for IMO 2021, white paper.* Inmarsat Research Programme. Tilgjengeleg frå: https://fullavantenews.com/inmarsat-cyber-security-requirements-for-imo-2021-white-paper/ (Henta: 20. mai 2021).

Kjerstad, N. (2019) *Elektroniske og akustiske navigasjonssystemer: for maritime studier*. 6. utg. Bergen: Fagbokforlaget.

Kvale, S. og Brinkmann, S. (2017) *Det kvalitative forsknings intervju.* 3. utg. Oslo: Gyldendal Norsk Forlag AS.

Malterud, K. (2017a) *Kvalitativ metasyntese som forskningsmetode i medisin og helsefag*. Oslo: Universitetsforlaget.

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

Nätt, T. H. og Heide, C. F. (2015) *Datasikkerhet: Ikke bli svindlerens neste offer*. Oslo: Gyldendal Norsk Forlag AS.

Ovcina, J. (2020) Naval Dome: 400% increase in attempted hacks since Febuary 2020. Tilgjengeleg frå: https://www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/ (Henta: 13. mai 2021).

Refsdal, A., Solhaug, B. og Stølen, K. (2015) *Cyber-Risk Management*. Oslo: Springer.

Schager, B. (2018) *Human error in the maritime industry: how to understand, detect and cope.* Sweden: Vinnova and Bengt Schager.

Sia, T. C. og Said, M. H. (2018) *The Importance of Maritime English Proficiency in Other Marine Related Undergraduate Programs.* Kuala Terengganu: School of Ocean Engineering, University Malaysia Terengganu. Tilgjengeleg frå: https://www.clausiuspress.com/conferences/AEASR/MSMI%202018/103.pdf.pdf (Henta: 20. mai 2021).

Telenor (2020) *Lær mer om datasikkerhet.* Tilgjengeleg frå: https://www.telenor.no/bedrift/sikkerhet/cybersikkerhet/ (Henta: 20. mai 2021).

The Editorial team (2020) Cyber attacks on maritime OT-systems increased 900% in the last three years. Tilgjengeleg frå: https://safety4sea.com/cyber-attacks-on-maritime-ot-systems-increased-900-in-last-three-years/?__cf_chl_jschl_tk__=d3c1437c5a6775892038b154bfd433fcf440b677-1620898685-0-Aeuz5MDMXSPXsdH6wJlBsdPsebKExnn9lcd_bk0meQJoRaO4t8-rPMrnBeDDLVThtyMXcnC7tgZsksxFcnrh7q-EGB1O2mOF5l0zVPvhlmmA5gGGFnnOwmrOBYVtYO2Td6mw2Uz5u0h71j1ujT1MJxWsD4Ui-J56Dhg92Uk-TB-Q99OTMEZUyIDEe18PI3SKx53zmHz27nCeNRTZOGBfY-U1-

iU79XQ3QA8NMBHkyWc2UJYy8B2ibDzM1QRxfRT_5WZW3iIHwEVQrOiWCtSPv-TDYP7IblTvweRpJetCaanWfMMtWmBakplJoMMwsih4XSXeLmnC27rQyT_hIs5kYQMYHtcBVCBdJlzp-Z7Z2YaHXir3wLOZg_l5TieeZUKIOpOdDL-sGWbNJWB_QoR6a55jnj51nL30vifcNyT2vcVXHRbv7lH3Pm4jWgHwPqyL_jgb79c0xnxzs5JtRxD28QG8YkND43nqtkdsV2XTyxSY (Henta: 13. mai 2021).

von Solms, R. og van Niekerk, J. (2013) *From information scurity to cyber security.* Port Elizabeth: Nelson Mandela Metropolitan University.

SSB (2021) *Handelsflåten, norskregistrerte skip* Tilgjengeleg frå: https://www.ssb.no/handelsfl/ (Henta: 27. mai 2021)

VEDLEGG 1: NSD SIN VURDERING

Prosjekttittel

Cybersikkerheit i maritim industri

Referansenummer

175907

Registrert

28.01.2021 av Pål Utslottøy - paalut@stud.ntnu.no

Behandlingsansvarlig institusjon

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

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Marie Haugli Larsen, marie.h.larsen@ntnu.no, tlf: 45061300

Type prosjekt

Studentprosjekt, bachelorstudium

Kontaktinformasjon, student

Pål Utslottøy, paalutslottoy@yahoo.com, tlf: 95211954

Prosjektperiode

01.03.2021 - 31.05.2021

Status

05.02.2021 - Vurdert

Vurdering (1)

05.02.2021 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar

med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg 05.02.2021. Behandlingen kan starte.

DEL PROSJEKTET MED PROSJEKTANSVARLIG

Det er obligatorisk for studenter å dele meldeskjemaet med prosjektansvarlig (veileder). Det gjøres ved å trykke på "Del prosjekt" i meldeskjemaet.

MELD VESENTLIGE ENDRINGER

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD 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 NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET

Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 31.05.2021.

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 attende. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER

NSD 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

NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

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).

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

NSD 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).

Dersom du benytter en databehandler i prosjektet må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET

NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Tlf. Personverntjenester: 55 58 21 17 (tast 1)

VEDLEGG 2: INFORMASJONSSKRIV OG SAMTYKKEERKLÆRING

Vil du delta i forskningsprosjektet
Cybersikkerhet i maritim industri?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å avdekke hvordan den maritime industrien håndterer de nye IMO-kravene om implementering av cyberrisiko i sikkerhetsstyringssystem om bord på skip. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Formålet med studien er å avdekke det potensielle nedslaget av de nye IMO-kravene, hvordan de eventuelt har hjulpet med økt bevisstgjøring i den maritime industrien, og hvilke tiltak industrien har gjennomført for å imøtekomme kravene.
Dette prosjektet er en bachelor ved NTNU i Ålesund.

Hvem er ansvarlig for forskningsprosjektet?

NTNU er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Vi trenger informasjon fra fagfolk og anser deg som en ekspert på området.

Hva innebærer det for deg å delta?

Hvis du velger å delta innebærer det å være med på et intervju hvor lydopptaket blir tatt opp og analysert for å brukes i vår oppgave. Intervjuet vil vare i 30-60 minutter. Opptaket blir slettet etter sensurfrist av oppgaven vår. (Utgangen av juni).

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket attende uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet.

Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- De som vil ha tilgang til informasjon vi innhenter er vi tre studentene (Emilie B. Stang, Pål Utslottøy og Henrik N. Vatle) og veileder (Marie Haugli Larsen).
- Personvernopplysninger om deg vil bli erstattet med en kode som lagres på egen navneliste adskilt fra øvrige data.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Prosjektet skal etter planen avsluttes 31.05.21. Personopplysningene og opptaket vil da bli slettet etter sensurfrist 21.06.21.

Dine rettigheter

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

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

Hva gir oss 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 personvernopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg 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 Larsen

  - Marie.h.larsen@ntnu.no
  - Tlf +47 450 61 300
- Vårt personvernombud:

  Thomas Helgesen
  - Thomas.helgesen@ntnu.no
  - Tlf +47 930 79 038
- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Marie Haugli Larsen — Pål Utslottøy

Rettleiar — Student

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Cybersikkerhet i maritim industri*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

☐ å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

VEDLEGG 3: INTERVJUGUIDE DEKKSOFFISER

Intervjuguide - Offiser

Kva me ynskjer å vite noko om	Forslag til spørsmål (intervjuguide)
Informasjon før opptak	Seie litt om temaet for samtalen (bakgrunn og formål) Forklar kva intervjuet skal nyttast til, og forklar teieplikt og anonymitet Spør om noko er uklart og om intervjuobjektet har nokre spørsmål Informer, få samtykke til og start opptak
Personalia	Utdanning Års erfaring på sjøen Noverande stilling
Generelt	Kva forbinder du med cybersikkerheit? • Har du opplevd eit cyberangrep? • Kva skjedde? • Korleis vart det handtert? Korleis er synet på cyberrisiko om bord og elles i reiarlaget? Tenker du ofte på cyberrisiko i dagleg operasjon?
Opplæring og kunnskap	Har du fått noko opplæring i cybersikkerheit? • Opplæring om bord? • Frå reiarlaget? • Under utdanninga? Korleis bør ein vektlegge cyber-relaterte truslar mot fysiske truslar i sikkerheitsbiletet om bord?
Rutinar og tiltak mot cyberangrep	Korleis er ein førebudd på cyberangrep om bord?

	Finst det ein policy om bord mot: • Nettsurfing? • Tilkopling av private einingar? • Spreiing av konfidensiell informasjon? Er reiarlaget sine krav til cybersikkerheit opne for tolking, eller er føringane klare? Har det vore gjennomført øvingar med cybersikkerheit i fokus? Korleis er informasjonsflyten mellom administrasjonen på land og fartøyet når det gjeld cybersikkerheit? Kva system om bord er mest sårbare for cyberangrep? (Kor mange einingar er tilkopla internett?) Kven har tilgang til dei sårbare systema?(Brukarar, passord)
IMO-krav	Korleis har reiarlaget informert om dei nye IMO-krava? • Kursing • Briefing • Informasjonsskriv/e-postar Har reiarlaget følgt opp IMO-krava ved å implementere cyberrisiko i sikkerheitsstyringssystem? • Om så, har dette ført til auka medvit? • Har andre endringar vore iverksette?
Oppsummering	Kva syns du om cybersikkerheita om bord? • Korleis kan den bli betre? Har me forstått deg riktig? Er det noko du ynskjer å leggje til?

VEDLEGG 4: INTERVJUGUIDE REIARLAGSTILSETT
Intervjuguide – Reiarlag

Kva me ynskjer å vite noko om	Forslag til spørsmål (intervjuguide)
Informasjon før opptak	Seie litt om temaet for samtalen (bakgrunn og formål) Forklar kva intervjuet skal nyttast til, og forklar teieplikt og anonymitet Spør om noko er uklart og om intervjuobjektet har nokre spørsmål Informer, få samtykke til og start opptak
Personalia	Utdanning Års erfaring på sjøen Noverande stilling
Generelt	Kva forbinder du med cybersikkerheit? • Har du opplevd eit cyberangrep? • Kva skjedde? • Korleis vart det handtert? Korleis er synet på cyberrisiko i reiarlaget? Vert cyberrisiko vurdert likt hjå mannskapet som i administrasjonen? Tenker du ofte på cyberrisiko i det daglege?
Informasjonsflyt	Korleis får dykk informasjon om viktige krav (IMO, ISM osv.)? Korleis vart dykk medvitne på dei nye IMO-krava? Korleis er informasjonsflyten frå reiarlaget og ut til fartøya? • Korleis blir mannskapet informert? Kurs/munnleg/e-post? Korleis er den laupande informasjonsflyten/dialogen mellom reiarlag og fartøy?

Rutinar og tiltak mot cyberangrep	Har reiarlaget ein klar og tydeleg cybersikkerheit-policy som alle fartøya sit på? • Vert det gitt strenge føringar om korleis dei forskjellege fartøya skal forhalda seg til denne policyen, eller vert det gitt ein viss tolkingsfriheit til dei enkelte fartøya? Er det utarbeida ein plan om eit cyberangrep skulle inntreffe? Blir det gjennomført øvingar på cyberangrep? • Er det da eit samarbeid mellom administrasjonen på land og dei om bord? Kven har tilgang til dei sårbare systema både om bord og på land?(Brukarar, passord)
IMO-krava	Korleis har dykk informert om dei nye IMO-krava? • Kursing • Briefing • Informasjonsskriv/e-postar Korleis handterar dykk IT-sikkerheita på line med andre risikoar om bord? Har dykk følgt opp IMO-krava ved å implementere cyberrisiko i sikkerheitsstyringssystem? • Om så, har dette ført til auka medvit? • Har andre endringar vore iverksette?

Oppsummering	Kva tenker du om cybersikkerheita i reiarlaget i dag? Er den god nok?| Meiner dykk at cybersikkerheita er god nok i reiarlaget? Har me forstått deg riktig? Er det noko du ynskjer å leggje til?

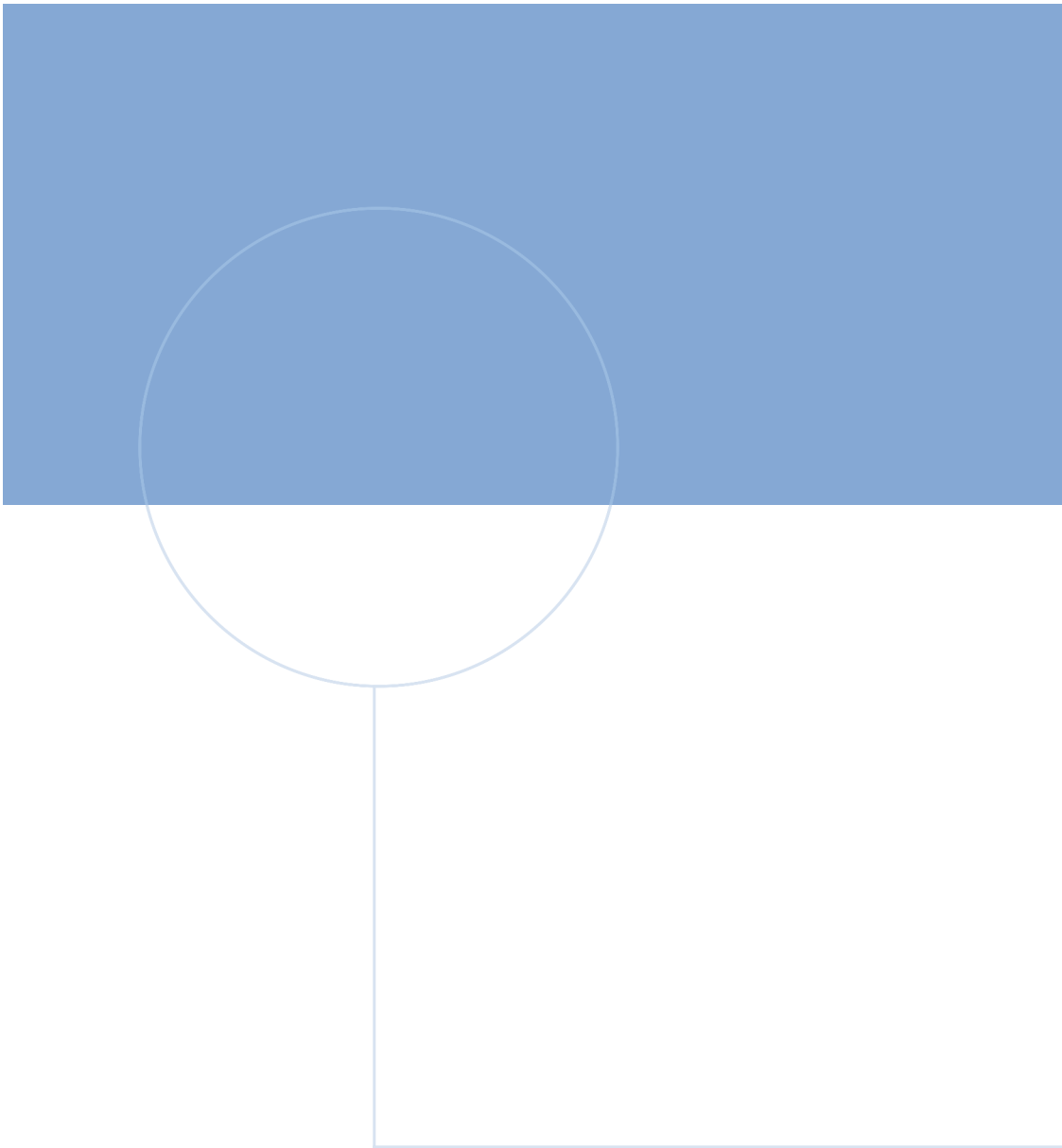
VEDLEGG 5: INTERVJUGUIDE KLASSESELSKAP

Intervjuguide - Bedrift

Kva me ynskjer å vite noko om	Spørsmål
Informasjon før opptak	Seie litt om temaet for samtalen (bakgrunn og formål) Forklar kva intervjuet skal nyttast til, og forklar teieplikt og anonymitet Spør om noko er uklart og om intervjuobjektet har nokre spørsmål Informer, få samtykke til og start opptak
Personalia	Utdanning Års erfaring med cybersikkerheit (IT på sjøen?) Noverande stilling
Generelt	Korleis ser trendane for cybersikkerheit i den maritime industrien i dag ut? Opplever dykk at reiarlag tek cybersikkerheit på alvor? Kva meiner dykk er grunnen til at IMO no har lagt større fokus på cybersikkerheit?
Bedrifta sin praksis	Kva er dei viktigaste faktorane dykk ser etter under ein revisjon av Document of Compliance om bord i fartøy? Kva kan reiarlag gjere for å beskytte seg mot angrep? • Har nye faktorar vorte sett i fokus no, kontra tidlegare? Har ein registrert store sprik i fokus på cybersikkerheit under revisjonar i fortida? Kva kan dykk tilby reiarlaga for å hjelpe dei imøtekome IMO-krava?

	Korleis "fungerer" cybersikkerheit-notasjonen i ei klassing? • Kven ser etter denne (Equinor osv.)? • Fordelaktig i tender? • Evt. konsekvensar om fartøyet ikkje har denne? Dyrare forsikring?
Opplæring	Korleis foregår opplæringa? • Administrasjonen • Offiserane Kva kompetanse er dykk mest opptekne med å lære vekk under opplæringa?
Informasjonsflyt	Korleis oppfattar dykk at kommunikasjonen mellom reiar og fartøy er, særleg vedrørande cybersikkerheita? Korleis vert informasjon spreidd til klientellet dykkar, og korleis vert den motteken? • Vert dykk tekne på alvor? • Har klientane nok kjennskap til emnet? • Er responsen prega av meiningar? Samlar dykk inn verdifulle data frå klientane dykkar for å oppnå eit heilskapleg overblikk over risikobiletet?
IMO-krava	Korleis syns dykk reiarlaga og industrien handterer datasikkerheit i forhald til den teknologiske utviklinga? Kva for nokon erfaringar har dykk med maritim datasikkerheit, og kva tankar vil vere viktig framover for å ivareta dei nye IMO-krava og sikkerheita om bord?

Oppsummering	Kva retning trur dykk industrien vil ta i framtida? • Vil det noverande fokuset på cybersikkerheit halde seg? • Vil cybersikkerheit bli ein del av utdanninga til framtidige styrmenn i større grad enn det er no? Har me forstått deg riktig? Er det noko du ynskjer å leggje til?



NTNU

Norwegian University of
Science and Technology