Masteroppgave

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

Idun Bakken

Cybersikkerhet og situasjonsbevissthet i maritim næring

En kvalitativ studie av skipsoperatørers erfaringer

Masteroppgave i Operativ Maritim Ledelse
Veileder: Marie Haugli-Sandvik
Mai 2024

NTNU
Kunnskap for en bedre verden

Idun Bakken

Cybersikkerhet og situasjonsbevissthet i maritim næring

En kvalitativ studie av skipsoperatørers erfaringer

Masteroppgave i Operativ Maritim Ledelse
Veileder: Marie Haugli-Sandvik
Mai 2024

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

NTNU
Kunnskap for en bedre verden

Forord

Denne oppgaven er skrevet våren 2024 som en avslutning på min mastergrad innen Maritim Operativ Ledelse. Den markerer også slutten på fem år med høyere utdanning ved NTNU Ålesund, som alt i alt har gitt meg en faglig tyngde og enormt med hodebry.

Skriveprosessen og arbeidet med studiet har vært lang og krevende, men også svært lærerik og spennende. Jeg vil takke alle som stilte til intervju og delte sine erfaringer – dere ga meg dyrebar innsikt i deres opplevelser. En stor takk må rettes til min veileder, Marie Haugli-Sandvik, for gode råd, rettledning og konstruktive tilbakemeldinger underveis i prosessen. Din kompetanse har hjulpet meg mye og har hatt stor betydning for oppgaven. Til slutt vil jeg også takke familie og gode venner for gode ord, støtte og oppmuntring fra start til slutt.

God lesing!
Idun Bakken

Sammendrag

Bakgrunn: Cybersikkerhet er et tema som stadig blir viktigere for maritime og offshore-industrier grunnet rask digital transformasjon, og situasjonsbevissthet er en viktig teori for å kunne forklare og forstå menneskelig oppførsel og for å unngå menneskelige feil. Det er derfor et behov for mer forskning på dette menneskelige aspektet ved cybersikkerhet.

Formål: Formålet ved denne studien handler om å skape en større forståelse for hvordan cybersikkerhet oppleves av skipsoperatører i norske rederier.

Problemstilling: «*Hvordan opplever skipsoperatører cybersikkerhet i sin arbeidshverdag*?».

Teori: Innholdet i teorigrunnlaget betrakter oppgavens tema som er sentrert rundt cybersikkerhet. Teorigrunnlaget vil starte med en generell redegjørelse av cybersikkerhet og cyber risikostyring på organisasjons- og teamnivå, før det snevres inn på individuell situasjonsbevissthet og kognitiv beslutningsteori, samt heuristikker og bias.

Metode: Kvalitativ metode med semistrukturert oppbygning. Utvalget består av skipsoperatører, som er en samlebetegnelse for stillingen vessel manager og operations manager m.m. Intervjupersonene har enten denne stillingstittelen nå eller fra tidligere, eller en stilling som er tilsvarende. Systematisk tekstkondensering er brukt for å analysere de transkriberte intervjuene.

Resultater: Funnene tyder på at skipsoperatørene har en grunnleggende forståelse av cybersikkerhet, men at variasjon i stillingsrelevans og egen interesse skaper et skille i kunnskapsnivået. Dette gjelder også opplevelsen av opplæring, tolkning av cyberrisikostyringssystem, og organisatorisk rammeverk. Styringssystemet og tilrettelegger for rask håndtering og bistand, men amputerer dermed en dypere forståelse av cybersikkerhet.

Konklusjon: Organisasjoner med styringssystem og opplæringsprogram som ikke er tilstrekkelige i møte med cyberrisikoer, kan i verste fall gjør menneskene til en større risiko enn ressurs. Studiet gir en implikasjon på hvilke individuelle faktorer og systemfaktorer som i større eller mindre grad påvirker skipsoperatørers situasjonsbevissthet rundt cybersikkerhet. Det kan dermed argumenteres for at mer dybdegående opplæring av ansatte og tilrettelegging i styringssystemene kan gi en større atferdsendring på et organisatorisk nivå, som igjen kan styrke cybersikkerheten hos rederiene.

Nøkkelord: Cybersikkerhet, cyber risiko, cyber risikostyring, situasjonsbevissthet, heuristikker, individuelle faktorer, skipsoperatører, norske rederier og bevisstgjøring

Summary

Background: Cybersecurity is an increasingly important issue for maritime and offshore industries due to the rapid digital transformation. Situation awareness is a key theory for explaining and understanding human behaviour and preventing human errors. Thus, there is a need for more research on the human aspect of cyber security.

Purpose: The purpose of this study is to create a greater understanding of how cybersecurity is experienced by ship operator in Norwegian shipping companies.

Research question: "How to ship operators experience cybersecurity in their daily work?"

Theory: The theoretical framework of the thesis focuses on cybersecurity. It begins with a general overview of cybersecurity and cyber risk management at an organizational and team level, then narrows down to individual situation awareness and cognitive decision theory, primarily heuristics and biases.

Method: The study employs a qualitative method with a semi-structured design. The selection consists of five ship operators, a collective term for the position of vessel manager and operations manager. The interviewees either currently hold or have previously held these positions or equivalent ones. Systematic text condensation is used to analyze the transcribes interviews.

Results: The findings suggest that ship operators have a basic understanding of cybersecurity, but variations in job relevance and personal interest create a disparity in knowledge levels. This also applies to the experience of training, interpretation of cyber risk management systems, and the organizational framework. The management system facilitates quick handling and assistance but hinders a deeper understanding of cybersecurity.

Conclusion: Organizations with management systems and training programs that do not educate and make employees more resilient to cyber risks, might turn people into a greater risk than a resource. The study highlights which individual and system factors influence ship operators' situation awareness regarding cyber security. It can therefore be argued that more in-depth training of employees and facilitation in the management systems can lead to greater behavioral change at an organizational level, which in turn can strengthen the cyber security of shipping companies.

Keywords: Cybersecurity, cyber risk, cyber risk management, situational awareness, heuristics, individual factors, ship operators, Norwegian shipping companies, awareness.

Begrepsavklaring

Autentisering	Handling for å bekrefte identitet (Datatilsynet, 2024)
BIMCO	Baltic and International Maritime Council (BIMCO, 2021)
Cybersikkerhet	En tverrfaglig, gjennomgående og kontinuerlig prosess som eies av virksomhetens øverste leder (NSM, 2020)
Cyberrisiko	En risiko som oppstår fra trusler som utnytter cyberspace, eksempelvis tjenester eller datasystemer, samt den informasjonen som er lagret og distribuert gjennom disse systemene (Lund & Larsen, 2021)
Cyberrsikostyring	Prosessen med å identifisere, analysere, vurdere og kommunisere en cyberrelatert risiko, og videre akseptere, unngå, overføre eller redusere den til et akseptabelt nivå ved å hensynta de kostnadene og fordelene ved handlinger utført av interessenter (BIMCO, 2021).
DNV	Det Norske Veritas, klasseselskap
Digitale verdier	Dokumenter, filer, digitale plattformer og systemer som virksomheten er avhengig av for å opprettholde sine funksjoner i form av oppgaver og leveranser innenfor virksomhetenes fysiske infrastruktur, administrative og organisatoriske forhold, samt regelverk (BIMCO, 2021)
Digitalisering	Tilrettelegge for generering av digital informasjon, samt håndtering og utnyttelse av informasjonen ved hjelp av informasjonsteknologi (Dvergsdal, 2021)
Heuristikker	Kognitive snarveier (Tversky & Kahneman, 1974)
IMO	Den Internasjonale Maritime Organisasjonen
Informasjonssikkerhet	Sikring av opplysninger ved å bruke prinsippene konfidensialitet, integritet og tilgjengelighet (Datatilsynet, 2024)
IT	Informasjonsteknologi, administrerer data som adgangskontrollsystemer, passasjerinformasjon, offentlige

	nettverk, administrative velferdssystemer, samt kommunikasjonssystemer fra skip til skip, og skip til land (Lund & Larsen, 2021)
OT	Operasjonell teknologi, styrer de fysiske enhetene og prosessene ombord, sånn som styringssystemer for last, brosystem, maskin- og fremdriftsstyring, og lignende (Lund & Larsen, 2021)
Phishing	Referer til prosessen med å lure mottakere til å dele sensitiv informasjon med en tredjepart (BIMCO, 2021)
Situasjonsbevissthet	Teori for å kunne forklare og forstå menneskelig oppførsel og for å unngå menneskelige feil (Endsley, 2000)
Skipsoperatør	I denne oppgaven: en samlebetegnelse for rederiansatte som koordinerer og kommuniserer med fartøy, kunder, og relevante interessenter.
Trussel	Kan være hva som helst, enten fysisk eller abstrakt, dersom det har potensiale til å negativt påvirke et objekt eller et system (Bergsjø & Windvik, 2020)
Trusselaktør	En entitet som er involvert i utførelsen av et inntrengingsforsøk (Bergsjø & Windvik, 2020)

Innholdsfortegnelse

Liste over figurer

Liste over tabeller

1 Innledning og bakgrunn for valg av tema

Da Maersk ble angrepet i 2017, markerte det et betydelig skifte i hvordan man oppfatter alvoret i den cybertrusselen som maritim næring står ovenfor i dag. Angrepet førte til et samlet tap på omtrent 300 millioner dollar, og i årene etter har flere maritime selskaper blitt utsatt for lignende cyberangrep i både større og mindre skala (DNV, 2023). Sånne hendelser medfører betydelige økonomiske og omdømmemessige skader. I en undersøkelse utført av DNV mellom mars og april 2023, blir det antydet blant 801 maritime fagpersoner at cyberangrep kan forstyrre global skipsfart ytterligere, og til og med true fysisk helse og sikkerhet (DNV, 2023). Cybersikkerhet blir et stadig viktigere tema for maritim næring, da rask digital transformasjon medfører nye og økende cybertrusler. Det er en kontinuerlig prosess hvor menneskelige faktorer spiller en avgjørende rolle i håndteringen av nåværende og fremtidige cyberrisikoer.

Situasjonsbevissthet handler om å gi mening til komplekse og dynamiske situasjoner, og er viktig for å forbedre ytelse, effektivitet og sikkerhet på ulike områder (Endsley, 2000). Det er en kritisk komponent i hvordan man kan forstå menneskelige faktorer og beslutningstaking, og påvirkes av kognitive evner, erfaring, trening og miljøfaktorer (Endsley, 2015). Situasjonsbevissthet er viktig for å kunne forklare og forstå menneskelig atferd, og sett i sammenheng med cybersikkerhet er det viktig at ansatte er klar over og forstår cybertrusler i den operasjonelle konteksten for å ta riktige beslutninger når de skal håndteres.

Situasjonsbevissthet er et konsept som hadde sin opprinnelse innen militær luftfart, og hadde som hensikt å øke sikkerheten og effektivisere militære operasjoner ved å ta utgangspunkt i tidligere forskning rundt kognitive konstruksjoner. Endsley (2015) sin definisjon har vært svært omdiskutert og det kommer stadig vekk uenigheter som fører til at den fortsatt blir forsket på. Poenget med modellen var likevel å tydeliggjøre sammenhengene mellom kognitive mekanismer, erfaringer, forståelse og målene til menneskene, noe som også vil gjøre den relevant i sammenheng med menneskers oppfattelse og erfaringer rundt cybersikkerhet.

Valg av tema i denne oppgaven ble gjort på grunnlag av et stadig økende behov for forskning på menneskelige faktorer innenfor cybersikkerhet i maritim næring. Studiets formål har som hensikt å undersøke hvordan skipsoperatører opplever cybersikkerhet i sin arbeidshverdag, og hvordan læring kan påvirke deres situasjonsbevissthet rundt dette. I tillegg vil det bli undersøkt

hvordan skipsoperatørene erfarer at retningslinjer og styringssystemer har en innvirkning på deres arbeid, og hvordan de opplever nødvendigheten for informasjonssikkerhet i eget rederi.

1.1 Problemstilling

Problemstillingen som er forsøkt belyst i denne oppgaven er:

> «*Hvordan opplever skipsoperatører cybersikkerhet i sin arbeidshverdag?*»

Problemstillingen er relativt bred, noe som gjør det mer krevende å belyse tematikken uten ytterligere presisering. Jeg har derfor valgt å inkludere tre forskningsspørsmål som skal bidra til å underbygge problemstillingen. Disse vil også legge rammeverket for valg gjort i teoretisk grunnlag, metodekapittel, datainnhenting og senere drøfting. Forskningsspørsmålene er som følger:

- *Hvordan erfarer skipsoperatører at rammeverk rundt cybersikkerhet virker inn på deres arbeid?*
- *Hvordan kan læring påvirke skipsoperatørers situasjonsbevissthetet rundt cybersikkerhet?*
- *Hvordan opplever skipsoperatører nødvendigheten for informasjonssikkerhet i eget rederi?*

1.2 Avgrensing

For å lettere finne frem til relevant litteratur for å kunne danne et teoretisk grunnlag for studiet, er det nødvendig å avgrense problemstillingen, samt ta stilling til egen faglige posisjon og utgangspunkt. Eksempelvis ville det vært interessant å undersøke rederienes konkrete arbeid med cyberrisikostyring. Det kunne også vært et alternativ å se nærmere på konnektiviteten mellom sjø- og landsystemer, for å også belyse sjøfolkenes perspektiver på temaet. I tillegg er operasjonell teknologi (OT) et aspekt som ofte blir nevnt i forbindelse med cybersikkerhet, og noe som ville vært interessant å inkludere. Dette vil dog åpne en dør inn til et større tema, og oppgaven vil derfor avgrenses til å legge hovedfokus på informasjonsteknologi (IT), og OT vil derfor bare bli nevnt med hensyn til kontekst.

Oppgavens omfang vil videre avgrenses til landsiden, og da spesifikt mot rederiansatte som ikke har en direkte tilknytning til arbeid med cybersikkerhet eller risikostyring. Studiet tar derfor utgangspunkt i rederiansatte som enten har eller har hatt stillingstittel som vessel manager, eller som arbeider med relativt tilsvarende oppgaver, som hovedsakelig innebærer hyppig kontakt med eller koordinering av skip. Dette er for å belyse deres perspektiver og opplevelser uten at de gjennom sin stilling har en direkte tilknytning til arbeid med cyberrisikostyring. De vil heretter bli omtalt som skipsoperatører, med mindre noe annet tilsier det. I denne oppgaven vil det innebære rederiansatte som koordinerer og kommuniserer med fartøy, kunder, og relevante interessenter.

Problemstillingens tema aktualiserer flere teorier og modeller, men grunnet studiens omfang og varighet er det valgt å avgrense teorien til det som presenteres i neste kapittel. Innholdet i teorigrunnlaget betrakter oppgavens tema som er sentrert rundt cybersikkerhet. Teorigrunnlaget vil starte med en generell redegjørelse av cybersikkerhet og cyber risikostyring på organisasjons- og teamnivå, før det snevres inn på individuell situasjonsbevissthet og kognitiv beslutningsteori, hovedsakelig heuristikker og bias. Dette vil være hovedfokuset i oppgavens teorigrunnlag og som vil tas videre i senere drøfting av teori og empiri.

1.3 Språk og oversettelser

Maritim industri er en internasjonal bransje, og derfor er mye av arbeidsspråket basert på det engelske språket. Dette medfører at noen engelske begreper innen maritim næring ikke kan oversettes til norsk på en tilstrekkelig måte. Det er derfor valgt å beholde noen av de engelske ordene i de tilfellene hvor den norske oversettelsen kommer til kort. Både engelske og norske begreper vil bli forklart i begrepsavklaringen som er å finne under sammendraget i denne oppgaven.

I tillegg er det brukt noen modeller som opprinnelig er på engelsk. Disse vil ikke bli oversatt til norsk, da det føltes unaturlig å ikke ivareta den originale formen. Det kan også medføre at meningen og hensikten med modellene ikke blir like forklarende som det de er på det opprinnelige språket.

1.4 Oppgavens oppbygning

Oppgaves hoveddel består av fem kapitler. Første del presenterer de teoretiske perspektivene som senere skal bli brukt som drøftingsgrunnlag av studiets resultater. Videre vil det være et metodekapittel som redegjør for valg av metode og vurderinger gjort underveis i arbeidet. Studiets empiriske funn vil bli presentert i kapittel fire, og deretter drøftet i påfølgende kapittel. Avslutningsvis vil oppgaven rundes av med betraktninger rundt implikasjoner for praksis, samt forslag til videre forskning.

2 Teoretisk grunnlag

Dette kapittelet vil inneholde relevant litteratur om temaet som blir gjennomgått i denne studien. Teorien vil bidra til å skape drøftingsgrunnlag for funnene gjort i den kvalitative datainnsamlingen.

Første del vil gi en generell redegjørelse av cybersikkerhet, herunder cyberrisiko og risikostyring, relevant rammeverk og forvaltning av digitale verdier. Neste delkapittel vil omhandle den organisatoriske tilnærmingen til cybersikkerhet, og det vil bli sett nærmere på cybersikkerhetslæring i organisasjoner. Deretter vil det teoretiske rammeverket gå mer inn på individnivå, hvor det først vil bli redegjort for situasjonsbevissthet og hvordan individuelle faktorer virker inn på situasjonsbevissthet. Det avsluttende delkapittelet vil ta for seg en del innenfor kognitiv beslutningsteori hvor fokuset blir lagt på heuristikker og bias.

2.1 Cybersikkerhet

Cybersikkerhet er en tverrfaglig, gjennomgående og kontinuerlig prosess som eies av virksomhetens øverste leder. Maritime bedrifter besitter verdier som vil være attraktive for trusselaktører. Bedriftene har også sårbarheter som eksponerer verdier og som trusselaktørene utnytter (DNV, 2024). Verdienes verdi er satt, og trusselaktørene vil forbli et faktum, dog kan sårbarhetene forsøkes å reduseres (NSM, 2020).

Cybersikkerhet er et tema som stadig blir viktigere for maritime og offshore-industrier grunnet rask digital transformasjon, noe som derfor medfølger nye trusler og regulatoriske krav (DNV, 2024). Cybersikkerhet fokuserer på trusler som kan gjøre skade gjennom cyberspace, og kan defineres som beskyttelsen av cyberspace, digital informasjon, IKT-systemer som støtter cyberspace, og brukerne av dette som er sårbare for angrep via cyberspace (Lund & Larsen, 2021).

2.1.1 Cyberrisiko

Mange har et lite bevisst forhold til risiko. Dette kan være fordi man som oftest forbinder risiko med de store katastrofene, mens det i virkeligheten er de mange små hendelsene som til slutt har størst påvirkning. Enhver person som er ansatt i en virksomhet, bør ha et bevisst forhold både ovenfor de direkte risikoene, samt de risikoene virksomheten skaper ovenfor seg selv og

omgivelsene (Aarset, 2010). Det er altså ikke nødvendigvis slik at risikoer kun omhandler store, spektakulære hendelser, sånn som digitalt innbrudd eller løsepengevirus, men at det også finnes mange «hverdagslige» risikoer. Dette kan eksempelvis være å sende personnummer og passord på mail, ikke låse datamaskinen før man forlater pulten, eller koble seg til åpent WiFi på den lokale kaffebaren.

Det finnes mange definisjoner på risiko, men i all hovedsak er det et begrep knyttet til en uønsket hendelse. Risikoen øker i hovedsak parallelt med hyppigheten av den uønskede hendelsen og omfanget av konsekvensen dersom den skulle inntreffe (Aarset, 2010). Innen datasikkerhet, blir risiko vanligvis uttrykt som forholdet mellom trussel, verdi og sårbarhet, og dersom disse reduseres, vil de totalt gi en lavere risiko (Bergsjø & Windvik, 2020).

Cyberrisiko kan defineres som en risiko som oppstår fra trusler som utnytter cyberspace, eksempelvis tjenester eller datasystemer, samt den informasjonen som er lagret og distribuert gjennom disse systemene (Lund & Larsen, 2021). I forbindelse med cyberrisiko, nevner Lund og Larsen (2021) at det er vanlig å dele systemene inn i to kategorier: Operativ teknologi (OT) og Informasjonsteknologi (IT). OT-systemene ombord fartøy er cyberfysiske systemer som samhandler med omgivelsene. Disse styrer de fysiske enhetene og prosessene ombord, sånn som styringssystemer for last, brosystem, maskin- og fremdriftsstyring, og lignende. IT-systemer administrerer data som adgangskontrollsystemer, passasjerinformasjon, offentlige nettverk, administrative velferdssystemer, samt kommunikasjonssystemer fra skip til skip, og skip til land (Lund & Larsen, 2021).

Tidligere har IT-systemer vært mer moden når det kommer til cybersikkerhet, da prosedyrene, teknologiene og opplæringen allerede har vært godt etablert over flere år ved hjelp av et informasjonssikkerhetssytringssystem (ISMS), og da spesielt på landsiden (DNV, 2024). Brudd på IT-systemer kan ha betydelig innvirkning på omdømme og økonomiske faktorer, men imidlertid påvirker det vanligvis ikke sikker drift av skip. OT er derimot ikke like moden når det gjelder cybersikkerhet. Et angrep på et skips OT-systemer kan ha stor innvirkning på skipets og mannskapets sikkerhet, samt marine miljø (DNV, 2024). OT og IT har tidligere ofte blitt håndtert som to separate systemer, som på et vis ikke har hatt en direkte sammenheng. Dog har den teknologiske utviklingen medført at disse to systemene har blitt mer integrert og samhandler i mye større grad enn før, blant annet gjennom fjernstyring og autonomi fra land. Dette vil derfor skape nye sårbarheter som kan utgjøre en stor risiko for manskapssikkerhet,

marine miljøet, infrastruktur og fartøyet i seg selv (Lund & Larsen, 2021). Det vil ikke bli gitt en bredere redegjørelse rundt OT-systemer og sammenhengen med IT-systemer, men det blir inkludert for å illustrere omfanget av IT-systemer og maritim cybersikkerhet.

2.1.2 Cyber risikostyring

BIMCO (2021) definerer cyber risikostyring som en helhetlig prosess. Prosessen innebærer å identifisere, analysere, vurdere og kommunisere en cyberrelatert risiko, og videre akseptere, unngå, overføre eller redusere den til et akseptabelt nivå ved å hensynta de kostnadene og fordelene ved handlinger utført av interessenter (BIMCO, 2021).

Figur 1: Tilnærming til håndtering av cyberrisiko som beskrevet i BIMCOs retningslinjer (BIMCO, 2021).

Det vil være krevende å utvikle, implementere og vedlikeholde en styringsprosess som samsvarer med tilnærmingen i figuren ovenfor. Det krever at flere ledd i virksomheten engasjerer seg i prosessen for å sørge for at det faktisk er gjennomførbart. For å håndtere risiko innenfor en akseptabel grense, er det derfor viktig å sikre at balansert forhold mellom beredskapsplanlegging og beskyttelse. Risikostyring er ikke et engangstiltak, men noe som bør

jobbes med kontinuerlig gjennom å vurdere trusler, sårbarheter, sannsynligheter, påvirkninger og risikoer, og om de tidligere iverksatte tiltakene fortsatt er hensiktsmessige (BIMCO, 2021).

Ifølge Kessler og Shepard (2022) kan risikovurdering foregå i to former: kvantitativ og kvalitativ. Den kvantitative tilnærmingen er målbar og objektiv, noe som videre vil kunne identifisere utsatte cybersårbarheter, og dermed bestemme den potensielle konsekvensen og hyppigheten av disse. Dette vil være mer problematisk dersom mindre håndfaste ting, sånn som omdømme og tillitt hos interessenter, skal måles. Den kvalitative metoden er basert på scenarioer av hendelser som kan gå galt. For hvert enkelt scenario blir det bestemt hvordan risikoen skal håndteres for å kunne redusere hyppigheten og påvirkningen til et mer akseptabelt nivå (Kessler & Shepard, 2022).

Ifølge IMO (2022) sine retningslinjer for cybersikkerhet i maritim næring, er målet med cyber risikostyring å bygge opp under en sikker skipsfart som er driftsmessig robust imot cyberrisikoer. De poengterer også at denne risikostyringen bør ha forankring på toppledernivå, for å sørge for en kultur der alle nivåer i virksomheten er bevisst cybersikkerhet i arbeidshverdagen. Dette er for å sikre en helhetlig ordning for cyberrisikostyring som pågår og evalueres kontinuerlig. En måte å gjøre dette på, er blant annet å gjennomføre en dybdegående vurdering av nåværende situasjon rundt cyberrisiko, og videre sammenligne dette med den ønskelige situasjonen for å lettere avdekke mangler eller hull som kan utbedres og utvikles (IMO, 2022).

Den internasjonale sjøfartsorganisasjonen (IMO) utvikler regelverk for skipsfart og arbeider for å skape og bevare trygghet, sikkerhet og mer effektiv skipsfart på rene hav (IMO, 2024). IMOs regelverk gjelder alle aspekter av internasjonal skipsfart, blant annet konstruksjon, utstyr, bemanning og drift, for å kunne sikre at sektoren holdes trygg, miljøvennlig, sikker og energieffektiv. Retningslinjene som omhandler cyber risikostyring er utformet for å hjelpe maritime virksomheter med å bygge en solid grunnmur for cybersikkerhet og håndtering av cyberrisikoer. Noen av de viktigste punktene i disse retningslinjene omhandler risikovurdering, beskyttelsestiltak, policy og ansvar, opplæring og bevissthet, og overvåking og evaluering (IMO, 2022).

Ifølge IMO (2022) er målet med cyber risikostyring å bygge opp under en sikker skipsfart som er driftsmessig robust mot cyberrisikoer. De poengterer også at denne risikostyringen bør ha

forankring på topplednivå, for å sørge for en kultur der alle nivåer i virksomheten er bevisst cybersikkerhet i arbeidshverdagen. Dette er for å sikre en helhetlig ordning for cyberrisikostyring som pågår og evalueres kontinuerlig. En måte å gjøre dette på, er blant annet å gjennomføre en dybdegående vurdering av nåværende situasjon rundt cyberrisiko, og videre sammenligne dette med den ønskelige situasjonen for å lettere avdekke mangler eller hull som kan utbedres og utvikles (IMO, 2022).

Det er anbefalt at disse retningslinjene inkorporeres i rederienes eksisterende sikkerhetsstyringssystem. IMO sine retningslinjer bør også suppleres med blant annet retningslinjene fra BIMCO. BIMCO's retningslinjer på cyberrisikostyring gir en detaljert oversikt over hvordan maritime virksomheter kan håndtere cyberrisiko best mulig. Disse innebærer anbefalinger for risikovurdering, implementering av cybersikkerhetsrutiner og policyer, opplæring av ansatte og håndtering av hendelser. Hensikten er å spre kunnskap, skape forståelse og adressere den stadige økningen av digitale trusler, samtidig som de sikrer at operasjoner forblir sikre, pålitelige og robuste i en mer digitalisert verden (BIMCO, 2021).

2.1.3 Forvaltning av digitale verdier

Bergsjø og Windvik (2020) definerer verdi som en ressurs, som dersom utsettes for uønsket påvirkning, kan føre til negative konsekvenser for eieren, forvalteren eller noen andre som drar fordel av denne ressursen (Bergsjø & Windvik, 2020). Begrepet «digitale verdier» er veldig bredt, og kan innebære digitale dokumenter, lydopptak, bilder, eller andre filer som lagres på en digital enhet. Det kan også være finansielle verdier og systemer. I denne oppgaven vil digitale verdier defineres som dokumenter, filer, digitale plattformer og systemer som virksomheten er avhengig av for å opprettholde sine funksjoner i form av oppgaver og leveranser innenfor virksomhetenes fysiske infrastruktur, administrative og organisatoriske forhold, samt regelverk (BIMCO, 2021). Eksempler på digitale verdier som blir forvaltet i maritim næring kan være kundefordringer, fraktavtaler eller kontrakter, personalopplysninger, ruteplaner, skipsmonitorering, back-up server, og så videre.

Digitaliseringen i den maritime sektoren skjedd både i systemer for informasjonsteknologi (IT-systemer) og i operasjonell teknologi (OT-systemer) i systemer for fremdrift, styring, automatisering og andre kontrollsystemer. Digitale hendelser som har en innvirkning på OT-systemer, kan føre til alvorlige konsekvenser for skipets drift og det omkringliggende miljøet.

De siste årene har det også vært en økning i utvikling av selvgående, ubemannede og autonome fartøy, noe som også underbygger viktigheten av økt fokus på digital sikkerhet. Maritim sektor operer i et internasjonalt marked hvor blant annet konkurransen rundt fraktoppdrag er høy. Dette medfører også at skipene seiler i internasjonalt farvann, noe som igjen innebærer at skipene må følge internasjonalt regelverk. Det har også vært en økning i digitalisering i havnene, hvor flere operasjoner nå er autonome (Sjøfartsdirektoratet, 2020).

2.2 Cybersikkerhetslæring i organisasjoner

I BIMCO (2021) sin liste over vanlige cyber sårbarheter, blir blant annet utilstrekkelig opplæring av personale nevnt. I tillegg trekkes frem utilstrekkelige ferdigheter i håndtering av cyberrisikoer, samt manglende eller ikke-testede beredskapsplaner og prosedyrer som medvirkende faktorer (BIMCO, 2021). Cybersikkerhet er en kontinuerlig og iterativ prosess, hvor de ansatte må gis kunnskap, motivasjon og en situasjonsforståelse som bidrar til å forsterke sikkerheten på arbeidsplassen (NSM, 2020).

DNV ga ut en rapport i 2023 med tittelen «*Maritime Cyber Priority*» hvor de hovedsakelig kartla holdninger og tilnærminger til cybersikkerhet hos nøkkelaktører i maritim industri. Der legger de frem fem nøkkelutfordringer som maritim sektor møter: investeringer, reguleringer, verdikjede, organisasjonskultur, og tilgang på ekspertise (DNV, 2023). De to sistnevnte vil inkluderes i videre redegjørelse.

2.2.1 Læring og opplæring

Rapporten vektlegger viktigheten av å hensynta hele verdikjeden når man adresserer cyberrisiko (DNV, 2023). Cyberrisikostyring bør ikke kun forbeholdes enkeltstående fartøy, men også det bredere aspektet som innebærer leverandører, partnere og interessenter. Det kommer også frem at sterk cybersikkerhetskultur innen maritime organisasjoner bør fremmes og jobbes aktivt med, gjennom å integrere cybersikkerhet i organisasjonens verdier, normer og adferd på alle nivåer, fra toppledelse til vanlige ansatte. De trekker frem viktigheten at å bygge en kultur hvor bevissthet rundt cybersikkerhet kan bidra til å redusere risiko og styrke robustheten mot cybertrusler. I tillegg understreker rapporten viktigheten av opplærings- og utviklingsprogrammer for å bygge kompetente ansatte som både har en økt forståelse og håndteringsevne i møte med cyberrisikoer (DNV, 2023).

For at læring i organisasjoner skal ha utbytte, bør det være en forankring i ledelsesorganet i den gitte virksomheten. BIMCO (2021) foreslår at ansvarsområdene rundt cyber risikostyring bør tilknyttes stillingsbeskrivelsene som finnes i den individuelle virksomhetenes sikkerhetsstyringssystem. Både planlegging og gjennomføring av risikostyringen involverer alle ansatte uansett stilling, og derfor vil en klar ansvarsoversikt være fordelaktig. IT-ansvarlig kan for eksempel være ansvarlig for cyberrisikostyring på sin avdeling, og har kanskje også et overordnet ansvar for virksomhetens IT-system. Likevel kreves det at vedkommende får støtte fra andre ledere og personal i resten av virksomheten, slik at ansvarsområdene blir mindre og mer spesifikke (BIMCO, 2021).

Det blir også nevnt at dårlig opplæring kan føre til at ansatte utilsiktet muliggjør cyberangrep på grunn av uforsiktighet. For å skape en mer risikobevisst ansattgruppe og en kultur for cybersikkerhet krever det mer konsistent opplæring. Rapporten trekker frem flere forskjeller i oppfattelse av virksomhetenes interne cyberrisikostyring og forståelse mellom de som er eksperter på området og de som har mindre kompetanse. Disse forskjellene går ut på at ekspertene gjerne ser en mangel på kompetanse i ansattstaben og at cybersikkerheten ikke blir håndtert godt nok, mens de med mindre kompetanse opplever sikkerheten som tilstrekkelig og føler seg trygge og ivaretatt av egne sikkerhetsstyringssystemer (DNV, 2023).

I en artikkel av Zhang et al. (2021) ble det sett nærmere på hvordan virksomheter kan tilrettelegge for best mulig praksis av cybersikkerhetsopplæring, da det i mange tilfeller er vanskelig å se det faktiske utbyttet av eksisterende programmer. Det er utfordrende å utvikle tilstrekkelig cyberrisikostyring i bedrifter, spesielt med tanke på utviklingen og frekvensen til cyberangrep. De enkleste formene for cyberangrep bruker metoder som phishing og skadelig programvare, siden mennesker ofte utgjør den svakeste lenken i en organisasjons cybersikkerhetskjede (Zhang, et al. 2021). I en annen artikkel av Khan (2011) ble effekten av informasjonssikkerhetskampanjer undersøkt. Her kom det frem at mange holdningskampanjer legger en større vekt på økt kunnskap, men at holdningsendringen kan bli neglisjert. Det blir poengtert at økt kunnskap og rett svar på konkrete spørsmål i læringsmoduler ikke nødvendigvis garanterer at ansatte vil anvende denne kunnskapen i sine handlinger. Det blir foreslått at kampanjer ikke bare informerer, men også aktivt engasjerer ansatte til å muligens endre atferd (Khan, 2011). Selv om denne artikkelen ble publisert for over ti år siden, er poenget likevel relevant i cybersikkerhetslæring for organisasjoner i dag.

Kompetanse, læring og risikooppfattelse har tilknytning til hverandre. For å kunne mene at noe er en risiko eller definere noe som en risiko, krever det at man har noen kunnskaper opp temaet (Bergsjø & Windvik, 2020). Eksempelvis er phishing e-poster en av de vanligste måtene å spre skadelig programvare eller innhente informasjon fra mottakeren på. For å kunne forstå risikoen ved å klikke på en lenke eller vedlegg i en sånn e-post, må de ansatte også være klar over muligheten for at det kan oppstå. Dette er dog ikke tilstrekkelig nok, da man også må ha kunnskap om hyppigheten av slike hendelser, oppdage kjennetegnene, og også forstå konsekvensene av de beslutningene man tar. Likevel er oppfattelse av risiko svært preget av subjektive faktorer (Bergsjø & Windvik, 2020).

2.3 Situasjonsbevissthet

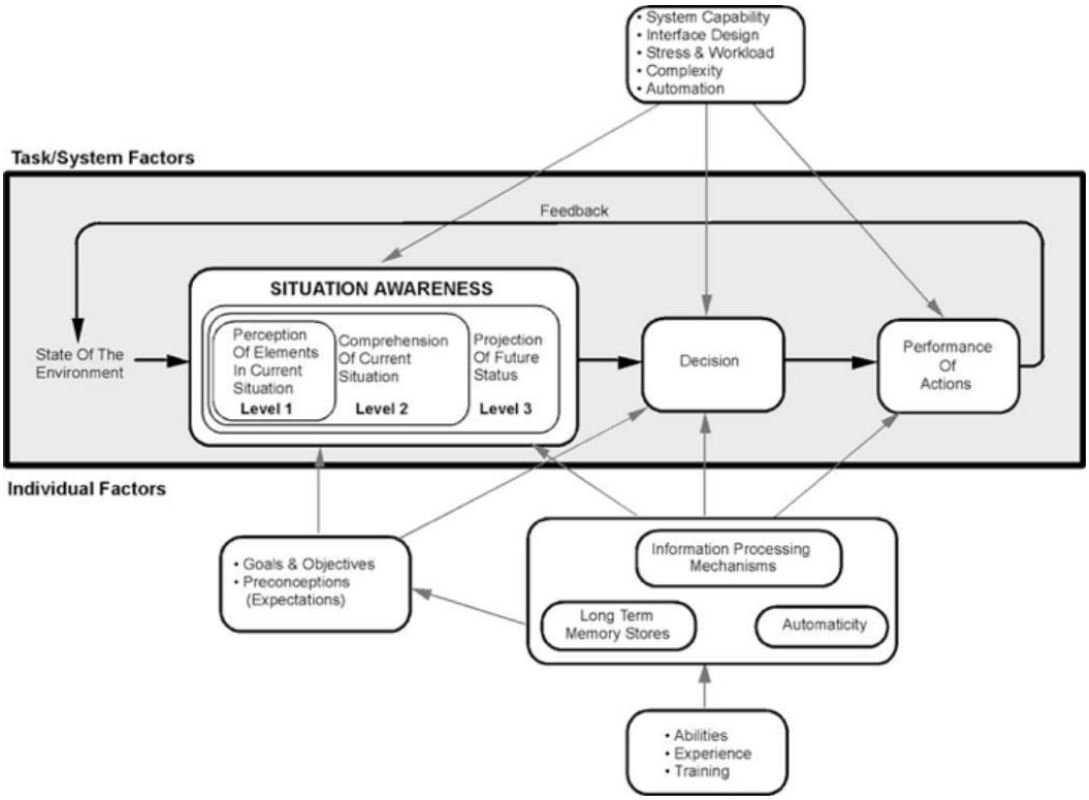
Situasjonsbevissthet er en viktig teori for å kunne forklare og forstå menneskelig oppførsel og for å unngå menneskelige feil. Opprinnelig ble situasjonsbevissthet introdusert som et konsept innen militær luftfart under første verdenskrig. Situasjonsbevissthet regnes som en kritisk faktor for at mennesker skal fungere effektivt i dynamiske miljø (Endsley, 2000). Innenfor akademia ble ikke konseptet diskutert ordentlig før på midten av 90-tallet. Det finnes mange definisjoner på situasjonsbevissthet, dog har det ikke blitt gjort en fullstendig enighet på hvordan dette bør defineres og illustreres (Aarset & Glomseth, 2019).

I forbindelse med denne oppgaven vil det bli redegjort for teori rundt situasjonsbevissthet, hovedsakelig med utgangspunkt i Endsley (2000) sin teori. Hovedfokuset vil ligge på de individuelle faktorene som har en innvirkning på oppnåelsen av situasjonsbevissthet, og det vil også bli redegjort for kritikk av modellen.

2.3.1 Presentasjon av modellen

Situasjonsbevissthet er en kritisk komponent i hvordan man kan forstå menneskelige faktorer og beslutningstaking i komplekse miljøer. Den påvirkes av kognitive evner, erfaring, trening og miljøfaktorer, og forståelse og måling av situasjonsbevissthet er viktig for å forbedre ytelse, effektivitet og sikkerhet på ulike områder, som for eksempel i maritime operasjoner (Endsley, 2015). Endsley (2000) sin definisjon er en som har fått mest oppmerksomhet på feltet de siste årene. Hun beskriver situasjonsbevissthet som operatørens indre modell av tilstanden i miljøet. Denne interne oppfattelsen gjør det mulig å bestemme hvilke handlinger som vedkommende

skal utføre basert på situasjonen, og videre gjennomføre de nødvendige handlingene. Menneskers situasjonsbevissthet er nødt til å tilpasse seg situasjoner hyppig, da hendelser er dynamiske og sjeldent helt like (Endsley, 2000).



Figur 2: Illustrasjon av Endsleys trestegs modell (Endsley, 2000)

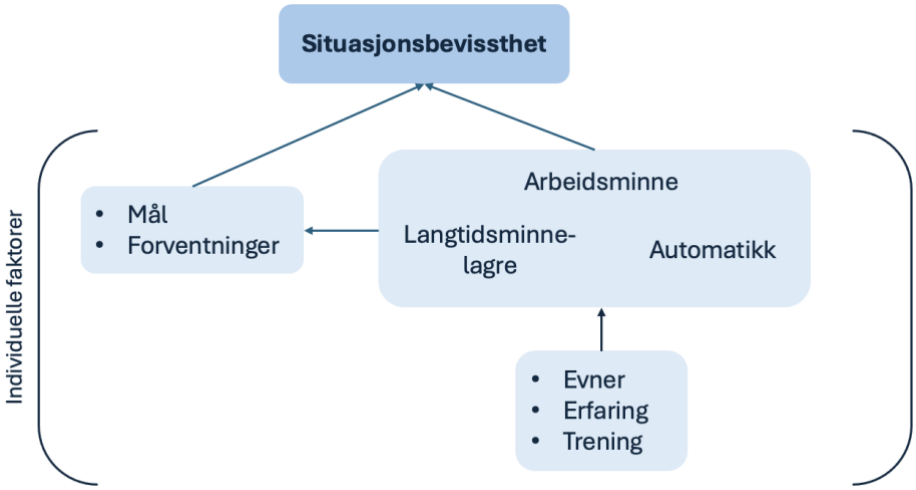
Modellen beskriver situasjonsbevissthet som en kognitiv prosess som innebærer tre stadier; persepsjon, forståelse og projeksjon. Persepsjon innebærer å innhente informasjon fra omgivelsene og tolke denne, og innebærer blant annet oppmerksomhet, analyse, langtidsminne og metakognitive prosesser. Når informasjonen er oppfattet, vil man forsøke å gjøre denne meningsfull og forståelig. Dette innebære prosesser som hukommelse, mentale modeller og egen tolkning av tilstanden. Projeksjon er det stadiet, basert på den oppfattede og forståtte informasjonen, hvor individer projiserer eller forventer fremtidige tilstander, gjør prediksjoner og dermed danner forventninger om den gitte situasjonen (Endsley, 2000).

Modellen fremstår som en relativt lineær prosess, hvor situasjonsbevissthet, avgjørelse og handling er som separate stadier. Endsley (2015) presiserer at modellen gir detaljene om hvordan de interne og eksterne faktorene samhandler med hverandre med å påvirke disse prosessene over tid for å skape en tilstand av situasjonsbevissthet i stadig utvikling. Situasjonsbevissthet som menneskelig faktor, innebærer blant annet kognitive prosesser, som oppmerksomhet, persepsjon og arbeidsminne, erfaring og trening i form av ekspertise og

mentale modeller, samt stress og tretthet, og delte mentale modeller for koordinasjon og samarbeid (Endsley, 2015).

2.3.2 Individuelle faktorers innvirkning på situasjonsbevissthet

De individuelle faktorene i modellen består av mål og forventninger, oppmerksomhet, automatikk, arbeidsminne og langtidsminnelagre, samt evner, erfaring og trening (Endsley, 2000). Disse faktorene virker på tvers av de tre stadiene som ble forklart tidligere.



Figur 3: Utdrag av de individuelle faktorene i situasjonsbevissthetsmodellen (Endsley, 2000)

Oppmerksomhet som en individuell faktor, vil kunne styre hvilken informasjon fra omgivelsene som oppfattes under det første stadiet, persepsjon. I tillegg vil arbeidsminne også spille en rolle, da dette kan begrense hvor mye informasjon som vil inntas og forstås videre på det andre og tredje stadiet. Automatikk vil for eksempel redusere arbeidsmengden og stress som finnes i systemfaktorene, men det kan også gjøre at uvanlige eller viktige ting blir oversett (Endsley, 2000). Eksempelvis vil nybegynnere være begrenset av arbeidsminnekapasitet i større grad enn noen med lengre og bredere erfaring. Stanton og Salmon (2017) nevner også at individuell situasjonsbevissthet er avhengig av kognitive prosesser og at automatisering teknologi både kan støtte og hemme situasjonsbevisstheten hos mennesker. Automatiserte systemer kan avlaste de kognitive belastningene, men også føre til tap av situasjonsbevissthet dersom brukerne blir altfor avhengige av dem (Stanton & Salmon, 2017)

Mål og forventninger vil også kunne være med på å styre situasjonsbevisstheten. Individuelle målsettinger styrer valget av relevante mentale modeller, som videre kan bestemme hvilken informasjon fra omgivelsene som vies oppmerksomhet. Disse vil filtrere oppfattet informasjon

basert på egen målsetting. Forventningsbaserte mål vil kunne forme hvilken informasjon man forventer å oppfatte, noe som kan gjøre at oppmerksomheten blir mer fokusert. Likevel kan «feil» forventninger føre til at signaler og informasjon blir mistolket (Endsley, 2000).

Evner, erfaring og trening er faktorer som kan være med på å opprettholde situasjonsbevisstheten. Som nevnt vil noen med lengre og bredere erfaring ha mer utviklede mentale modeller og bedre strategier for å kunne styre oppmerksomheten og tolke informasjon mer effektivt. Trening kan forbedre evnen til å kjenne igjen mønster i situasjoner og skape en mer nøyaktighet av de mentale modellene. Arbeidsminnekapasitet og perseptuelle ferdigheter kan påvirker de grunnleggende prosessene som er involver i å oppnå situasjonsbevissthet (Endsley, 2000).

Første stadiet i modellen om situasjonsbevissthet vil oppmerksomheten og persepsjon begrense informasjon som oppfattes i omgivelsene. Mål og forventninger basert på mentale modeller styrer hvor oppmerksomheten vil være mer fokusert. Arbeidsminnet kan begrense forståelsen under det andre stadiet, dog vil mentale modeller og mønstergjenkjenning tilrettelegge for bedre forståelse og videre tolkning av situasjonen. Det tredje stadiet om projeksjon vil også avhenge mer av mål og forventninger, men med en større vekting på de mentale modellene rundt situasjonen som utspilles (Endsley, 2000).

2.3.3 Kritikk av modellen

Ifølge Aarset og Glomseth (2019) vil selve prosessen påvirkes av flere omkringliggende faktorer som påvirker informasjonsinnhentingen og forståelsen, samt beslutningstakingen og oppførselen. Endsley (2000) sin modell illustrerer også de mer individuelle faktorene som mål, forventninger og egenskaper, arbeidskapasitet og kompleksitet, som alle påvirker situasjonsbevisstheten (Aarset & Glomseth, 2019).

Modellen har blitt omtalt som en ideell oppfattelse av hvordan vi som mennesker skal oppfatte miljøet rundt oss. Den er omdiskutert blant annet fordi den ikke inkluderer forforståelse og kunnskap og hvordan det kan påvirke situasjonsoppfattelsen, som igjen vil kunne påvirke hvilken informasjon individet oppsøker for å videre kunne gi mening til situasjonen. Modellen indikerer også en oppfattelse om at verden er full av all den informasjonen man måtte trenge, selv for en observerende aktør uten forforståelser.

Endsley (2015) uttrykker at den opprinnelige modellen på situasjonsbevissthet ble utviklet med formål om å bedre arbeidet til piloter, soldater og design av jagerfly med hensikt å øke sikkerheten og effektivisere militære operasjoner. I tillegg argumenterer hun for at modellen tok utgangspunkt i tidligere forskning og kunnskap rundt kognitive konstruksjoner, hvor poenget hovedsakelig var å gi en detaljert beskrivelse av situasjonsbevissthet via interaksjonene mellom kognitive mekanismer, erfaringer, forforståelse og målene til de involverte individene. Endsley adresserer også at modellen hennes ikke er komplett med å representere de detaljene som har blitt påpekt at mangler, men at den likevel gir en generell beskrivelse av situasjonsbevissthet (Endsley, 2015).

2.4 Heuristikker og bias

Når mennesker prøver å gi mening til verden for så å fatte en beslutning, vil det være farget av miljø, genetikk og kognitiv evne til å bearbeide informasjon (Cunningham, 2019). Kognitiv beslutningsteori brukes til å forklare og forstå hvordan mennesker faktisk fatter beslutninger, i motsetning til hvordan man ideelt sett skal gjøre det ifølge fastsatte modeller og teorier (Tversky & Kahneman, 1974). Gjennom å forstå beslutningsteori kan man i større grad bli bevisst egne begrensninger, og dermed forbedre egen beslutningstaking, eksempelvis under usikkerhet eller ved større beslutninger som skal tas.

Heuristikker er kognitive snarveier, og er noe mennesket bruker for å redusere kompleksiteten i problemer, observasjoner, interaksjoner og beslutninger til enklere og mer effektive oppfattelser som er adaptive i lignende situasjoner (Tversky & Kahneman, 1974). Bias blir definert som de spesifikke feilene eller mangelfulle vurderingene som oppstår når man legger altfor stor lit i de heuristiske strategiene uten å ta tilstrekkelig hensyn til annen informasjon som kan være relevant. Bias er tendensen til at mennesker velger en gruppe, person eller ting fremfor en annen, hvor det dermed skapes en urettferdig skjevhet (Tversky & Kahneman, 1974).

Tversky og Kahneman (1974) beskriver heuristikker som de generelle mentale snarveiene, mens bias er feilene som kan oppstå ved feilaktig bruk av disse snarveiene. Altså er heuristikker de kognitive strategiene som brukes ved vurdering av usikkerhet, mens bias er de feilene som kan forekomme når strategiene tas i bruk på en begrenset eller overforenklet måte, uten å hensynta andre viktige faktorer i den vurderingen (Tversky & Kahneman, 1974). I forbindelse

med denne oppgaven vil det derfor bli redegjort for tre heuristikker: Tilgjengelighet, representativitet og forankring (Tversky & Kahneman, 1974). Dette er også heuristikker som anses som relevante i sammenheng med cyberhendelser (Johnson & Gutzwiller, 2020).

2.4.1 Tilgjengelighet

Tilgjengelighetsheuristikken går ut på å vurdere hyppigheten av et tilfelle gjennom å hente ut informasjon og eksempler fra hukommelsen. Dette kan være at mennesker lettere husker de hendelsene som har gjort et stort inntrykk eller hatt en innvirkning på en selv, kontra de mindre og mer vanlige hendelsene som også har en tendens til å oppstå hyppigere. Denne heuristikken kan være svært nyttig, men kan også føre til feilvurderinger av sannsynlighet og frekvens ved en hendelse. Det er altså faktorer som hvor kjent eller sterkt assosiert noe er, som videre vil påvirke hvor lett det kommer frem i bevisstheten, uavhengig av hyppigheten (Tversky & Kahneman, 1974). Eksempelvis, dersom en person leser ofte på nyhetene om cyberangrep på virksomheter, kan de overvurdere sannsynligheten for å bli utsatt for lignende selv da de har disse hendelsene mer tilgjengelige i minnet. Dersom det oppstår en skjevhet, kan det bety at man heller tenker «dette skjer ikke meg», og også dette kan føre til feilvurderinger dersom det faktisk skulle oppstå.

2.4.2 Representativitet

Representativitetsheuristikken brukes til å vurdere sannsynligheten for at noe tilhører en bestemt kategori eller prosess, med utgangspunkt i representativitet. Altså viser denne heuristikken hvordan hjernen forholder seg til likhet. Det vil være mindre krevende å forholde seg til en situasjon eller person dersom man kan relatere til tidligere erfaring, likevel kan man derfor utelate statisk informasjon og heller bare basere seg på overfladiske likheter (Tversky & Kahneman, 1974). Denne heuristikken kan føre til flere skjevheter, som å blant annet ignorere generelle ting, som hvor vanlig noe er i den generelle befolkninger, og dermed tro at spesifikke hendelser eller betingelser er mer sannsynlige enn en generell betingelse (Tversky & Kahneman, 1974).

2.4.3 Forankring

Forankringsheuristikken brukes når man skal gjøre estimater eller prediksjoner med utgangspunkt i en gitt verdi, ofte ved bruk av tall som er lett tilgjengelig i minnet, og deretter justerer andre størrelser i forhold til dette. Dette kan føre til en skjevhet, eksempelvis ved å

overvurdere suksess i situasjoner med flere sammenhengende hendelser, og videre undervurdere suksess i situasjoner der hendelsene er uavhengige (Tversky & Kahneman, 1974).

Forankringsheuristikken er i stor grad en motsetning til de to andre heuristikken som er forklart, da de handler om å vurdere sannsynligheter ut ifra likhet, eller hvor lett noe kan relateres, mens denne i større grad tar utgangspunkt i en gitt eller individuell verdi som videre justeres når andre faktorer spiller inn før en beslutning skal tas (Tversky & Kahneman, 1974).

3 Metode

Betydningen av ordet metode er «veien til målet». Man bør derfor gjøre seg opp en mening om hva målet med prosjektet skal være, slik at man tidlig i prosessen kan bestemme seg for hvilken metode som er mest passende til valgt tema og problemstilling. Dette kapittelet vil ta for seg metoden som er brukt i oppgaven, hvor det først vil bli redegjort for bakgrunn for valg av metode, en beskrivelse av det vitenskapsteoretiske perspektivet, og en avklaring av egen forståelse. Videre vil det bli redegjort for planleggingen av studiet, utførelse og analysemetodikk, samt verifisering.

3.1 Valg av metode

I startfasen av arbeidet med oppgaven, ble det fastslått tema og mål for studiet, samt problemstilling og tilhørende forskningsspørsmål. Problemstillingen er som følger: «*Hvordan opplever skipsoperatører cybersikkerhet i sin arbeidshverdag?».* Formålet ved denne studien handler om å skape en større forståelse for hvordan cybersikkerhet har en innvirkning på den individuelle situasjonsbevisstheten til skipsoperatører i norske rederier.

Temaet er ute etter å belyse individers erfaringer, opplevelser og forståelse, noe som gjorde kvalitativ metode til et naturlig valg for studiets design (Kvale & Brinkmann, 2015). Valget av metode har derfor falt på semistrukturert intervju i et fortolkende perspektiv. Dette fordi samtalen er planlagt, dog fleksibel, med formål om å få frem beskrivelser av intervjupersonens egne erfaringer og inntrykk, med hensyn til fortolkning av meningen med de fenomenene som blir beskrevet i intervjuet (Kvale & Brinkmann, 2015).

Denne metoden forutsetter også at jeg som intervjuer har satt meg godt inn i temaet, slik at det blir en samtale mellom intervjuperson og forsker, men med forhåndsdefinerte spørsmål og tema som man ønsker å belyse. Ved å bruke kvalitativ metode kan man få en bred innsikt i hvordan virkeligheten former seg for intervjupersonen, fordi man underveis i intervjuet også kan plukke opp verbale uttrykk og kroppsspråk som ikke er mulig å fange opp ved for eksempel en spørreundersøkelse. (Tjora, 2017).

3.2 Avklaring av egen forståelse

Forskerens forståelse og forkunnskap vil kunne påvirke studiets resultater allerede i startfasen ved utformingen av tema, problemstilling og intervjuguide. Det vil også være fordelaktig å gå inn i en studie med et åpent sinn og en interesse for tematikken, samtidig som man forsøker å distansere seg fra forhåndskunnskap og inntrykk. Likevel kan egne erfaringer, perspektiver og empirisk forankring farge forståelsen og tolkningen av datamaterialet. Det er derfor viktig å være bevisst dette, slik at påvirkningen underveis, både i intervjuet og i forskningsprosessen, blir betydningsløs.

Som ung forsker og student stiller jeg med relativt blanke ark til tematikken, noe jeg tror vil kunne styrke oppgavens reliabilitet da den ikke vil være farget av forutinntatthet. Samtidig kan det være en svakhet da dette kan begrense evnen til å stille gode og relevante oppfølgingsspørsmål underveis i intervjuet.

3.3 Kvalitativt forskningsintervju

Intervju i kvalitative studier er en teknikk som brukes for å innhente perspektiver på verden sett gjennom intervjupersonenes øyne. Oppbygningen og gjennomførelsen av intervjuet kan gjøres på flere måter, dog vil det i dette tilfellet bli brukt semistrukturert intervju som er en mellomting mellom planlagt og ikke-planlagt intervju. En forhåndskonstruert intervjuguide vil ligge til grunn for de temaene som skal bli kartlagt, men det tillates stor grad av improvisasjon underveis i intervjuet. Både gjennom å utelate eller legge til spørsmål, men også stille oppfølgingsspørsmål eller konkretiserende spørsmål for å tydeligere få frem intervjupersonens faktiske opplevelse (Kvale & Brinkmann, 2015).

I dette intervjuet vil intervjupersonen bli spurt om egne opplevelser av cyber risikostyring på arbeidsplassen, noe som gjør at valget av kvalitativ metode vil være en passende tilnærming. Ved utformingen av intervjuguiden var det viktig å lage spørsmålene så åpne som mulig, dog innenfor tematikken for å kunne besvare problemstillingen. Hensikten med dette er å frigjøre intervjueren litt mer fra intervjuguiden, slik at oppfølgingsspørsmål og utdypelse av svar ikke blir begrenset av tidsbruk og det neste punktet på listen. På denne måten kan også intervjupersonen få mulighet til å fortelle fritt om sine erfaringer og opplevelser (Kvale & Brinkmann, 2015). Denne metoden for datainnsamling vil potensielt gi et sterkere datagrunnlag enn ved kvantitativ metode, da formuleringen av problemstillingen indikerer personlige

opplevelser. Dette vil komme tydeligere frem i intervju kontra spørreundersøkelse. Derfor vil valget av kvalitative intervjuer være en god beslutning, da jeg som intervjuer kan tilpasse og justere spørsmålene og samtalene underveis i intervjuet, og også foreta justeringer av intervjuteknikk mellom intervjuene.

Som det ble nevnt tidligere i kapittelet, er det viktig at forskeren drøfter og vurderer valgene som blir tatt underveis i prosessen. Planleggingen og utførelsen av studiet vil derfor bli gjort etter Kvale og Brinkmann (2015) sine syv faser ved gjennomføringen av en intervjuundersøkelse; tematisering, planlegging, gjennomføring av intervju, transkripsjon, analyse, verifikasjon og rapportering.

3.4 Tematisering

Tematisering innebærer å formulere formålet med undersøkelsen. Formålet ved dette studiet er formulert ved at det skal ses nærmere på hvordan skipsoperatører opplever cybersikkerhet på egen arbeidsplass, og hvordan deres situasjonsbevissthet påvirkes eller ikke påvirkes av dette.

Tidlig i prosessen ble studiets hvorfor, hva og hvordan avklart da dette er vesentlig for planleggingen av studiet og valgt metode. Det er viktig å innhente tilstrekkelig kunnskap om temaet, samt relevant teori og metode som senere skal skape grunnlaget til analysen og drøftingen som kommer senere. Forskeren bør med fordel forsøke å ikke planlegge studiet etter ønsket metode, da dette kan føre til skjevheter i datainnsamling og -behandling. Det ble derfor valgt kvalitativ metode da temaet innebærer å hente ulike aspekter av skipsoperatører erfaringer, noe som gjør kvalitativ metode mer velegnet (Kvale & Brinkmann, 2015).

I denne fasen gikk det en del tid til litterære søk, både for å kartlegge tidligere forskning, men også skape et bilde over hva som potensielt kunne inkluderes som teorigrunnlag for studien. Det ble også drøftet hvor solide de teoretiske antakelsene var, og om sammenhengen mellom forskningsspørsmål og teori virket logisk (Kvale & Brinkmann, 2015).

3.5 Planlegging

Som relativt ny og uerfaren forsker, var det svært nyttig å reflektere godt over valgene som ble tatt gjennom planleggingsfasen, både i forkant og underveis i gjennomførelsen av studiet. For

å sikre reliabilitet og validitet, ble studiet planlagt i forkant av arbeidet med intervjuene med utgangspunkt i de syv fasene.

Underveis i planleggingsfasen ble det sendt inn søknad til Sikt – Kunnskapssektorens tjenesteleverandør, for å sikre at studiet behandler personopplysninger i tråd med personregelverket. Det var nødvendig å få dette godkjent i forkant av gjennomførelsen av intervjuene for å sikre at intervjupersonene fikk tilstrekkelig informasjon om studiet og databehandlingen, samt innhente skriftlig samtykke til deltakelse i studiet. Det ble utformet et informasjonsskriv og en samtykkeerklæring som ble lagt ved forespørselen om å delta, hvor intervjupersonene fikk lest gjennom og signert i forkant av intervjuene. Både godkjennelsen fra Sikt og samtykkeerklæringen ligger som vedlegg under kapittel 8.

3.5.1 Beskrivelse av utvalg

Tidlig i prosessen ble utvalget begrenset til vessel managers. Dette defineres som et strategisk utvalg da intervjupersonene innehar direkte kunnskap på området som forskes på (Malterud, 2017). Underveis i arbeidet med det teoretiske grunnlaget, ble det også forsøkt opprettet kontakt med potensielle intervjupersoner. Responsen var varierende, og det ble derfor gjort et valg om å utvide utvalget ytterligere, og dermed inkludere andre personer med til dels tilsvarende stilling. Dette var blant annet trade planner, crew manager og prosjektleder. Disse hadde blant annet jobbet tett med vessel managers, eller hatt denne stillingen tidligere. Det var også ønskelig å intervjue personer som ikke var eksperter på cybersikkerhet, og som heller ikke hadde omfattende erfaring og kunnskap rundt tema. Siden utvalget ble utvidet, kan dette derfor beskrives som et bekvemmelighetsutvalg, da det ble valgt personer som det var mulig å få tak i. Arbeidsoppgavene deres er relativt like noe som kan indikere at de har ganske like opplevelser på området.

Det var ønskelig å ha minst fem intervjupersoner, med rom for et par ekstra dersom det skulle være behov. Det kan være stort nok til at resultatene kan bli generaliserbare, men det kan også bli for lite av samme grunn. Likevel kan et større utvalg gjøre analysen mer komplisert ved at datagrunnlaget blir for stort (Kvale & Brinkmann, 2015). Grunnet tidsbegrensningene ved studiet, ble det derfor avholdt fem intervjuer. Dette var også med på å sørge for at analysen ble grundig gjennomført, og at datamaterialet var en håndgripelig mengde som fikk tid til å modne i forkant av drøftingen.

Utvalget består altså av tre mannlige og to kvinnelige rederiansatte med en av stillingstitlene nevnt ovenfor. Aldersspennet er fra midten av 20-årene til midten av 50-årene. Det var ingen spesifikke kriteriet for å delta i studiet annet enn at vedkommende måtte jobbe i et rederi og inneha en stilling som vessel manager eller tilsvarende. Intervjupersonene hadde vært i nåværende stilling i alt fra 2 år til 15 år, og de hadde erfaring fra flere maritime næringer, både offshore, container og RoRo. Mengden arbeidserfaring var ikke et kriteria da dette ikke nødvendigvis har en innvirkning på deres situasjonsbevissthet rundt cybersikkerhet. Utvalget ble gjort gjennom tips fra veileder og intervjupersoner, søk på lokale rederiers hjemmesider, og eget nettverk.

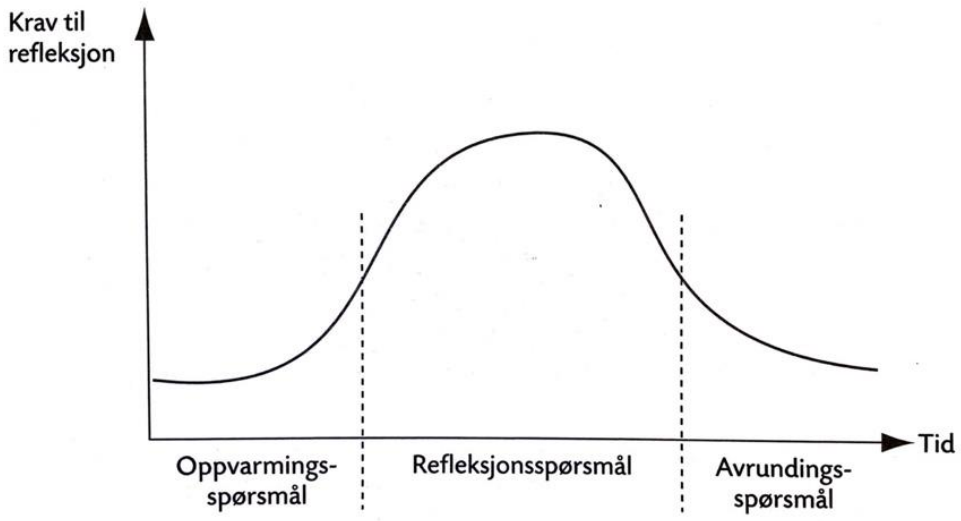
3.5.2 Intervjuguide

Underveis i teoriinnhentingen ble det også formulert en intervjuguide som ligger vedlagt under kapittel 8. Denne ble delt inn i temaer med utgangspunkt i teorikapittelet, hvor spørsmålsforslagene skulle forsøke å innhente informasjon som kunne analyseres i lys av teorien. Spørsmålene ble formulert på et lettbeint og dagligdags språk for å unngå misforståelser og opprettholde flyt i intervjuet. Det var viktig at jeg som intervjuer hadde en god forståelse av innholdet i teorigrunnlaget, slik at spørsmålene kunne utdypes ved usikkerhet hos intervjupersonen. Dette var også nødvendig dersom spørsmålene skulle bli misforstått sånn at informasjonen ble irrelevant eller lite presis.

Det ble tatt forbehold om at intervjuet kunne forandres underveis i intervjuet. Svarene til intervjupersonen kunne besvare flere enn ett spørsmål, og det ble derfor tatt i betraktning at spørsmålene kunne endre ordlyd, eller bare sløyfes helt. For å opprettholde flyten i intervjuet, ble det vekslet mellom fullstendige spørsmål og oppfølgings- eller utdypningsspørsmål. Dette for å oppnå målet om intervjuet som en intervjustyrt, asymmetrisk interaksjon (Tjora, 2017).
Oppbygningen av intervjuet tar utgangspunkt i dybdeintervjuets struktur: oppvarming, refleksjon og avrunding (Tjora, 2017). For å skape en uformell start av intervjuet, blir det satt av tid til småprat og en introduksjon av meg selv og prosjektet i forkant av opptaket. Når opptakeren blir skrudd på, startes intervjuet med generelle spørsmål om intervjupersonen, sånn som utdanning, stilling og arbeidserfaring. Dette vil bidra til å skape en trygg grunn for det videre intervjuet, slik at det fremstår mindre formelt og mer som en dagligdags samtale mellom to personer.

Videre blir refleksjonsspørsmålene stilt, noe som danner hoveddelen av intervjuet. Det er disse spørsmålene som skaper datagrunnlaget, og det er derfor viktig at de er presise dog åpne for å skape en stor dybde i svarene. Oppfølgingsspørsmål vil ikke bli planlagt på forhånd, men heller tilpasses intervjuet og informasjonen underveis. Mange av spørsmålene kan føre til at intervjupersonen beveger seg innenfor flere områder av intervjuguiden, og det vil være viktig å være oppmerksom og lytte aktivt.

Avslutningsvis i intervjuet vil det bli gjort en grov oppsummering av intervjuet, hvor intervjupersonen blir bedt om å tilføye mer informasjon om ønskelig, og også for å forsikre meg om at jeg har forstått vedkommende riktig. Dette for å skape en åpen refleksjon av intervjuet som har blitt gjennomført. Til slutt avsluttes lydopptaker, og intervjupersonen takkes for deltakelsen i prosjektet, og det informeres om at de kan ta kontakt dersom de skulle ønske å benytte seg av rettighetene sine.



Figur 4: Dybdeintervjuets struktur (Tjora, 2017)

3.6 Gjennomførelse av intervju

Utvalget ble i hovedsak kontaktet via e-post eller LinkedIn. Mailen inneholdt en kort beskrivelse av prosjektet, temaet for intervjuet og forespørsel om å delta. I tillegg ble samtykkeskjemaet fra Sikt lagt til som vedlegg, slik at mottakeren kunne lese om studiet og databehandlingen. Utvalget ble blant annet rekruttert via veilederen min, intervjupersonenes tips, samt eget nettverk og internettsøk. Intervjupersonene sto fritt til å bestemme hvorvidt intervjuet skulle gjennomføres fysisk eller digitalt. I utgangspunktet skulle alle intervjuene være ferdig gjennomført før påske, noe som ikke gikk helt etter planen. Både rekrutteringen,

intervjuene og transkriberingen tok lengre tid enn først antatt, noe som likevel var forventet, og hele prosessen endte opp med å ta rundt fem uker.

Det var viktig å skape en avslappet atmosfære som intervjupersonene var komfortable i, noe som kan være med på å skape grunnlaget for et vellykket intervju (Tjora, 2017). En av intervjupersonene ønsket å møte til fysisk intervju, mens de resterende ble gjennomført digitalt. Mengden og kvaliteten på datamaterialet var relativt likt uavhengig av fysisk eller digitalt intervju, likevel ble flyten i samtalen bedre ivaretatt i det fysiske intervjuet, noe som var forventet. Som ung forsker er intervjusituasjonen et ganske ukjent farvann å bevege seg ut på. De første intervjuene bar preg av mer stakkato og usikkerhet i spørsmålene, mens det etter hvert gikk seg til da man ble bedre kjent med intervjuguiden og situasjonen.

Som beskrevet i forrige delkapittel tok intervjuet utgangspunkt i Tjora sin modell av dybdeintervjuets struktur (Tjora, 2017). Intervjuene startet med en kort prat om bakgrunnen for prosjektet og at intervjuet ville fungere mer som en samtale. Intervjupersonene hadde signert informasjonsskrivet på forhånd, og vi tok en rask gjennomgang av databehandlingen. Lydopptaket ble deretter startet, og intervjuet ble satt i gang.

Intervjupersonene hadde relativt lik stilling, og hadde også derfor en ganske lik tilnærming til cyber risiko og hvordan det påvirket eller ikke påvirket egen arbeidshverdag. Jeg opplevde at intervjuene holdt seg innenfor tema, og at intervjupersonene delte rikt av sine erfaringer og synspunkter. Stillingen deres tilsa ikke at de skulle være eksperter på temaet, noe som også var ønskelig i utgangspunktet. Noen hadde en bredere forståelse og innsikt, men dette var mye på grunn av egne interesser og ekstra kursing. Tidvis ble spørsmålene besvart litt utenfor tema, noe som var naturlig og som det også var åpenhet for. Intervjuene ga også rom til oppfølgingsspørsmål og presisering av svarene dersom noe var uklart. Hensikten var uansett å få innsikt i intervjupersonenes erfaringer og opplevelser rundt deres tolkning av temaet, og tidvise avsporinger ble derfor godtatt innenfor rimelighetens grenser.

Sett i retrospekt av gjennomførelsen av intervjuene, mener jeg at valget av kvalitativ metode hjalp med å styrke oppgaven. Det ga også mulighet til å oppdage og avklare både ulikheter og likheter mellom funnene i intervjuene. I mitt møte med maritim bransje stiller jeg med relativt blanke ark, og cybersikkerhet er en verden jeg så vidt har vært innom i min studietid. Dette tenker jeg likevel har kommet til min fordel da intervjuene bærer lite preg av forutinntatthet. På

en annen side kunne jeg føle at det til tider var vanskelig å stille gode og relevante oppfølgingsspørsmål. Dette kan være på grunn av jeg ikke hadde grundig nok forståelse av temaet og bransjen, noe som kan være en svakhet i intervjuene.

3.7 Transkripsjon

Lydopptakene fra intervjuene ble transkribert til skriftlig tekst. Dette ble gjort for å gjøre de bedre egnet for den senere analysen, og det blir dermed lettere å få oversikt og begynne å strukturere innholdet. Det skal også nevnes at den skriftlige transkripsjonen er en gjenskapelse av muntlige uttalelser, og at den til tider kan fremstå som forvirrende og usammenhengende. Dette er fordi teksten i seg selv ikke kan gjengi følelser, ironi, toneleie og kroppsspråk. Den kan derfor anses som en omforming av den virkeligheten som utspilte seg under intervjuet mellom to personer. Kvale og Brinkmann (2015) omtaler transkripsjoner som «*kunstige konstruksjoner* [...] *av den levende muntlige samtalen* ...». Det er derfor viktig å ha i bakhodet underveis i transkriberingen at teksten skal være så nøyaktig lik virkeligheten som mulig for å få frem de opplevelsene intervjupersonen har til hensikt å dele.

Transkriberingen ble gjennomført kort tid etter intervjuet var gjennomført, både for effektivitetens skyld, men også for å notere ned de delene som kunne være nyttige for analysen mens samtalen fortsatt var friskt i minnet. Ved at jeg transkriberte intervjuene selv, er det med på å styrke validiteten i til datamaterialet. Prosessen var tidkrevende, og til tider komplisert da ord og setninger kunne bli utydelige på grunn av støy eller dialekt. Det ble tatt en avgjørelse på å transkribere alle intervjuene til bokmål uansett dialekt. Dette var for at målformen på datamaterialet skulle samsvare med språket brukt i resten av oppgaven. Det ble tatt en vurdering rundt oversettelsen av engelske ord og uttrykk, og noen av disse ble beholdt i sin opprinnelige form da oversettelsen kunne mistolkes eller var lite deskriptiv. I tillegg valgte jeg å utelate pauser og andre lyder som oppsto underveis.

3.8 Etikk

Etikk innen forskning innebærer personvern i form av anonymisering og konfidensialitet. Deltakelsen i intervjuet er frivillig, og intervjupersonene fikk mulighet til å trekke seg når som helst. I forkant av intervjuet fikk intervjupersonene utdelt et samtykkeskjema. Her ble de opplyst om databehandlingen og hva det betydde for de å delta i forskningsprosjektet. I tillegg ble det planlagt å informere de om anonymitet og databehandling i starten av intervjuet, før

lydopptaket ble startet. Intervjupersonene fikk også tilbud om å få analysedelen tilsendt da den var ferdigstilt nærmere prosjektslutt.

For å bevare anonymiteten, ble det ikke spurt om navn eller hvilken bedrift vedkommende tilhørte, noe som var viktig for å sørge for at svarene de ga skulle bli så ærlige som mulig. Det var tilfeller hvor intervjupersonene nevnte navnet på egen arbeidsplass eller andre, og dette ble anonymisert i transkriberingen og i den senere analysen. I forskningssammenheng er det viktig å bevare anonymiteten fordi temaet i intervjuet dreier seg om intervjupersonenes egen arbeidsplass, og det kan være en mulighet for at kolleger eller arbeidsgiver belyser kritikkverdige forhold (Tjora, 2017). Det skal dog nevnes at intervjuobjektene ikke ble spurt om noe som kunne knytte de til en spesifikk bedrift, da fokuset lå mer på deres opplevelser og erfaringer rundt forskningstemaet.

3.9 Analyse

Valg av analysemetode for å analysere de kvalitative dataene, vil også legge føringer for utarbeidelse av intervjuguiden, -prosessen og transkriberingen (Kvale & Brinkmann, 2015). Analysemetoden ble derfor valgt tidlig i studiet, allerede i planleggingsfasen, noe som skapte et tryggere grunnmur for meg som forsket da intervjuene skulle gjennomføres. Spørsmålene ble delt inn i temaer noe som hjalp meg med å bli mer bevisst hvilke deler som kunne sammenlignes og plukkes ut senere. Det var også viktig å fokusere på hvordan jeg skulle analysere det intervjupersonene fortalte, slik at min videreformidling ga en utdypende mening for leseren. Dette er også en del av de etiske sidene ved analysen, ved at datamaterialet skulle gjengis så nært intervjupersonenes mening som mulig. I tillegg vil analysen styres mye av forskerens modenhet, teoretiske forkunnskaper om temaet, og beherskelse av den valgte analysemetoden (Kvale & Brinkmann, 2015).

Mens jeg analyserte datamaterialet fikk jeg gått mer i dybden på svarene, og dermed skaffet en oversikt over hva som kunne brukes senere og hva jeg kunne luke ut. Analysemetoden jeg valgte å ta i bruk, var Malterud (2017) sin modifiserte teori, systematisk tekstkondensering. Hensikten med denne analysemetoden er å utvikle kunnskap på bakgrunn av den informasjonen intervjuobjektet formidler. Det er en tverrgående analyse som sammenslår informasjon fra flere intervjuobjekter, og består av fire trinn; lage foreløpige temaer ut fra helhetsinntrykk, samle meningsbærende enheter i koder, sortere kodene i undergrupper, og sammenfatte betydningen

av disse (Malterud, 2017). Disse trinnene vil bli nærmere beskrevet i de neste delkapitlene. Hele analysen skal sikre en grundig gjennomgang av materialet gjennom flere trinn, samtidig som den har en forankring i det teoretiske grunnlaget. Samtidig er det også viktig å vurdere relevans, gyldighet og refleksivitet gjennom hele analyseprosessen (Malterud, 2017).

Tabell 1: Kort beskrivelse av systematisk tekstkondensering (Malterud, 2017).

Trinn 1	Tema	**Foreløpige temaer** blir identifisert ved første gjennomlesing
Trinn 2	Koding	Temaene danner grunnlag for forhandlinger om **koder**, som danner grunnlaget for sortering av meningsbærende enheter i **kodegrupper**
Trinn 3	Kondensering	Kodegruppene deles igjen inn i **subgrupper** som synliggjør ulike aspekter av innholdet i kodegruppen som virkemiddel for sammenfatting ved hjelp av kondensat
Trinn 4	Kategori	Det utvikles **kategorier** ved sammenfatning av det sentrale meningsinnholdet for hver av kodegruppene, hvor utgangspunktet er kondensatet fra subgruppene. Kan videreføres til resultatkapittelet som underoverskrifter

Ovenfor er en oversikt over hvert trinn i systematisk tekstkondensering. Fremgangsmåten ble fulgt relativt slavisk, men det var likevel noen trinn som ble gikk litt mer inn i hverandre. Eksempelvis begynte jeg å plukke ut direkte sitater mens jeg jobbet med gjennomlesingen og tematiseringen. Disse ble deretter plassert under tilhørende tema i neste steg, og ble senere finpusset og gjort om til kondensat, og videre til mer sammenfattende kategorier. Hvert trinn av analysen fikk et eget dokument for å lettere holde oversikt, men også for å holde styring på egen tankerekke underveis i prosessen.

3.9.1 Tema

I det første trinnet er ikke detaljer det viktigste, men heller det helhetlige bildet. I tillegg bør man også huske på at temaene med skal samsvare med det teoretiske rammeverket, problemstillingen og forskningsspørsmålene. Dette innebærer å lese gjennom alle transkriberingene, samtidig som man noterer egen forståelse fortløpende (Malterud, 2017). Som nevnt ble dette påbegynt allerede underveis i transkriberingen, men måtte uansett gjøres grundigere da alle intervjuene var ferdig transkribert.

Figur 5: Stikkord notert fra gjennomlesingen av de transkriberte intervjuene.

Når alt er gjennomgått, skal egen oppfatning oppsummeres. Det skal dannes en oppfatning av potensielle temaer som kan hjelpe til å belyse problemstillingen gjennom å ta en helikoptertur over det innsamlede datamaterialet (Malterud, 2017). I løpet av denne prosessen noterte jeg syv temaer: Informasjonssikkerhet, bevisstgjøring, håndtering, tillit til rammeverk, styringssystem læring og opplæring.

3.9.2 Koding

Når de foreløpige temaene er gjennomgått, vil de videre danne grunnlag for kodegruppene i dette analysetrinnet. Det går ut på å skille relevant tekst fra mer irrelevant tekst, og dermed identifisere de meningsbærende enhetene, som videre skal kodes under de foreløpige temaene som ble identifisert i forrige steg. Denne kodingen er dekontekstualisering av teksten, der deler plukkes ut fra den opprinnelige sammenhengen for deretter å bli sett i sammenheng med lignende tekstutdrag og det teoretiske rammeverket (Malterud, 2017). I denne delen av analysen bør man ta seg god tid på å drøfte meningen ved de forskjellige temaene sett i lys av problemstillingen, og det er bedre å ta med litt for mye enn litt for lite.

Systematiseringen som beskrevet ovenfor ble gjort i tabeller i Word. De meningsbærende enhetene ble kopiert ut av transkripsjonen og deretter plassert under tilliggende tema i et separat Word-dokument. Jeg merket raskt at det ble mange temaer å forholde seg til, og at flere av de meningsbærende enhetene passet inn under flere kodegrupper. Jeg valgte derfor å snevre inn antallet temaer, noe som også bidro til at jeg ble bedre kjent med de meningsbærende enhetene. Dette var blant annet å slå sammen rammeverk og styringssystem til kategorien tillit. Da de endelige kodegruppene begynte å bli mer tydelige, la jeg også merke til at deler av datamaterialet ga ny mening og det ble oppdaget vinklinger jeg ikke hadde lagt merke til i de tidligere gjennomlesingene.

3.9.3 Kondensering

På dette stadiet av analysen er den empiriske dataen kondensert til et dekontekstualisert utvalg av meningsbærende enheter, og innholdet i kodegruppene skal sorteres ytterligere inn i subgrupper. Videre skal sitatene i subgruppene gjøres om til et kondensat som er en oppsummering av dataene som tar det viktigste fra hver del og omsetter dem til en mer generell form. Altså skal kondensatet gjenfortelle det som befinner seg i subgruppen på en mer sammenfattet måte, hvor spor av intervjupersonens ord og begreper fra de meningsbærende enhetene skal komme tydelig frem. Dette kondensatet vil bli brukt i oppsummeringen av resultat som vil bli utformet i neste kapittel. Deretter vil det bli valgt et gullsitat som illustrerer innholdet i kondensatet fra subgruppen (Malterud, 2017).

Kondensatet bidro til å se på problemstillingen og studiets tema med nye øyne. Underveis i arbeidet med datainnhentingen fikk teorimateriale modne, noe som bidro til at jeg lettere kunne trekke linjer mellom teori og empiri. Kodegruppene ble spisset ytterligere, og subgruppene kom tydeligere frem når de ble sett i sammenheng med utdrag fra datamaterialet og stikkordene gjort under gjennomlesingen.

3.9.4 Sammenfatning

I det siste trinnet av systematisk tekstkondensering, skal funnene sammenfattes og omformuleres til nye beskrivelser og begreper. Det er viktig å hensynta intervjupersonenes perspektiver i fortolkningen av datamaterialet, slik at gjenfortellingen gir innsikt og tillit i resultatene som skal bli presentert. Hver subgruppe får en egen omtale, og teksten vil skrives i tredjeperson (Malterud, 2017).

Temaene som ble identifisert av helhetsinntrykket i første trinn har videre blitt delt inn i kodegrupper og deretter subgrupper. Tekst fra transkriberingen ble transformert til kondensat og senere omgjort til gullsitat gjengitt i tredjeperson. Teksten har altså blitt sammenfattet til mer analytisk tekst som samsvarer med intervjupersonens uttalelser, og som bidrar til å støtte meningsinnholdet i transkripsjonen fra intervjuet. Dette vil bli presentert i et eget resultatkapittel.

3.10 Verifikasjon

I etterkant av analysen skal studiets funn tas videre til drøfting hvor også reliabilitet og validitet, objektivitet og overførbarhet skal hensyntas. Enhver forsker har et etisk ansvar om å rapportere kunnskap som er så sikker og verifiserbar som mulig, noe som også innebærer å sette spørsmålstegn ved denne kunnskapens gyldighet (Malterud, 2017).

3.10.1 Reliabilitet og validitet

Reliabiliteten i studiet handler om konsistens og pålitelighet i resultatene. Dette handler blant annet om å stille spørsmål ved om hvorvidt intervjuene skapte en god ramme for intervjupersonene til å fortelle hva de virkelig mener, og om påliteligheten til intervjuguide, transkribering og analyse opprettholdes kontinuerlig gjennom arbeidet (Kvale & Brinkmann, 2015).

Gjennom hele forskningsarbeidet skal man tilstrebe å opprettholde validiteten i arbeidet. Forskeren bør ikke bare sette spørsmålstegn om validiteten i hvert enkelte steg og valg som blir gjort, men også ta helhetlige vurderinger om studiets validitet underveis i arbeidet for å sikre at metoden undersøker det den har til hensikt å undersøke (Kvale & Brinkmann, 2015).

Ved bruk av kvalitative intervjuer vil man ta i bruk spørsmål som er mer ledende for å oppnå den informasjonen man ønsker. Intervjuguiden var lik i hvert intervju, noe som gjorde at alle intervjuene hadde samme utgangspunkt selv om spørsmålene ble tilpasset samtalen underveis. Ved å holde en viss kontinuitet og likhet i intervjuprosessen, kunne jeg lettere sammenligne informasjonen i den senere analysen. Som ung forsker har det vært viktig for meg å innhente nok forhåndskunnskap for å videre gjøre et riktig valg av metode da tema for studiet ble satt, samt videre planlegging og gjennomførelse av datainnhentingen. Dette ble gjort for å sikre at resultatene kunne gjenspeiles i studiets formål og tema, og videre gi en faktisk representasjon av virkeligheten formidlet av intervjupersonene. Likevel kan egen forforståelse og underliggende subjektivitet rundt studiets tematikk redusere validiteten og ha en effekt på resultatene.

Til tross for å være bevisst på validiteten og reliabiliteten i de valgene som har blitt gjort, vil det likevel kunne være faktorer som kan svekke dette (Kvale & Brinkmann, 2015). Dette kan blant annet være at intervjupersonene tilbakeholder informasjon eller begrenser seg, både

bevisst og ubevisst, da spørsmålene i stor grad dreier seg om deres opplevelser av cybersikkerhet på arbeidsplassen. I tillegg kan min egen forforståelse ha hatt en effekt på utarbeidelsen i intervjuguiden, noe som kan gi ringvirkninger videre i arbeidet. Det er likevel forsøkt å minimere feilkildene gjennom å tilstrebe god planlegging av metode og gjennomførelsen av den, samt være bevisst opprettholdelsen av valideringen gjennom hele arbeidsprosessen.

3.10.2 Objektivitet

I kvalitativ forskning vil reliabilitet og validitet omhandle de mer tekniske og konseptuelle utfordringene ved et forskningsprosjekt. Dette medfører også spørsmål om denne metodetypen kan være objektiv. Kvale og Brinkmann (2015) lister opp flere betydninger av objektivitet som kan tilknyttes kvalitativ forskning. Dette er blant annet frihet fra ensidighet, hvor kunnskap er noe som er etterprøvd og kontrollert, refleksiv objektivitet, der forskeren tilstreber objektivitet om subjektivitet, samt objektivitet som intersubjektiv enighet, og objektets evne og rettighet til å protestere. Disse beskrivelsene av objektivitet kan derfor hensyntas dersom det skulle bli stilt spørsmål ved studiets objektivitet og om kvalitative metoder kan være en objektiv forskningsmetode (Kvale & Brinkmann, 2015). For denne studien betyr dette at funnene ikke bare skal gjenspeile mine forventninger, tolkninger eller perspektiver, men også de komplekse og dybdegående opplevelsene til intervjupersonene på en måte som er tilnærmet lik deres beskrivelser.

3.10.3 Overførbarhet

Malterud (2017) skriver at generaliserbarhet legger opp til urealistiske assosiasjoner om allmenngyldig overførbarhet. Ordet generalisering krever en viss datamengde som man ikke kan anta at finnes i sin helhet i kvalitative studier. Derfor vil det i dette studiet være mer hensiktsmessig å bruke begrepet overførbarhet, da dette er et ord som i større grad hensyntar avgrensninger og betingelser for hvordan resultatene på en eller annen måte gir ny innsikt som kan relateres til andre tilsvarende sammenhenger (Malterud, 2017).

Kvalitative data kan åpne for alternative tolkningsmåter, men i en studie som dette bør man være varsom med å tro eller påstå at funnene kan overføres til en populasjon. Likevel er overførbarhet en forutsetning for kunnskap som skal kunne deles (Malterud, 2017). Utvalgets størrelse har blitt gjennomgått og vurdert tidligere, men vil også kunne være relevant å stille

spørsmål til i denne sammenhengen også. Målet ved den valgte metoden er å frembringe detaljerte beskrivelser av intervjupersonenes opplevelser rundt tema, og derfor vil beskrivelsene som har kommet frem være mulig å sammenligne med lignende beskrivelser for å fastslå overførbarhet (Kvale & Brinkmann, 2015).

3.11 Rapportering

Skriveprosessen er en integrert del av forskningsmetodologien ifølge Kvale og Brinkmann (2015). I dette studiet har skriving blitt anvendt som et verktøy for å utforske og utvikle tanker. Samtidig har det vært viktig å sikre at resultatene og metoden fremlegges på en måte som er lesbar og som er i tråd med vitenskapelige standarder (Malterud, 2017). Spesielt i denne fasen har etiske spørsmål, sånn som konfidensialitet, blitt svært vektlagt. I tillegg har det kontinuerlig blitt gjort overveielser knyttet til hvordan denne studien kan påvirke intervjupersonene.

4 Resultat

I dette kapittelet vil resultatene fra de kvalitative intervjuene bli presentert. Den systematiske tekstkondenseringen førte til tre kategorier som er listet nedenfor. Kategoriene med de tilhørende subgruppene, skal i samsvar med egen analyse og utformede gullsitat bidra til å besvare problemstillingen og tilhørende forskningsspørsmål. Dette kapittelet inneholder forskerens tolkninger av datamaterialet fra de kvalitative intervjuene, og danner et bilde av intervjupersonenes egne synspunkter og opplevelser på gitt tema.

Tabell 2: Kategorier og tilhørende subgrupper

Kategori	**Subgrupper**
Rammeverk	- Retningslinjer - Betryggende styringssystem - IT-avdeling og HSEQ
Bevisstgjøring	- Holdningskampanjer og opplæring - Økt fokus - Erfaringsbasert kunnskap
Informasjonssikkerhet	- Forståelse - Begrense informasjonsdeling - Kritisk bruk

4.1 Rammeverk

Denne kategorien handler om tillit til egen virksomhets rammeverk og retningslinjer, samt intervjupersonenes perspektiver på eget styringssystem rundt cybersikkerhet. Det var nyttig å vite mer om dette for å danne et bilde av hvilke rammer intervjupersonene arbeider innenfor og om dette er en sentral del av deres arbeidshverdag. Dette er også aspekter som kan ha en innvirkning på hvordan intervjupersonene forholder seg til cybersikkerhet i sin arbeidshverdag.

4.1.1 Retningslinjer

En av intervjupersonene uttalte at rammeverket bør forankres i ledelsen, slik at det i større grad blir gjeldende for hele organisasjonen. Vedkommende påpekte at det ofte kan nedprioriteres dersom pålegget om mer læring kun kommer fra personal- eller avdelingsledere, og at

nytteeffekten trolig vil være større dersom man ser en tydeligere forankring i hele organisasjonen. Dette mente vedkommende kunne være viktig for å sørge for at majoriteten av organisasjonen snakket samme språk, og hadde lik tilnærming til tema. Flere intervjupersoner nevnte også at cybersikkerhet er noe de fleste kun har assosiert med IT-avdelingen, men at det de siste årene har blitt skapt en mer helhetlig forståelse og at dette er noe som skal treffe alle ledd i organisasjonen, uavhengig av stilling.

Da det ble spurt om intervjupersonene hadde noen spesifikke retningslinjer eller regelverk rundt cyber sikkerhet som de måtte forholde seg til, svarte majoriteten ja. Dette var dog noe de ikke oppsøkte aktivt, hovedsakelig fordi det ikke hadde vært nødvendig enda. Det ble nevnt at dette også var tilfellet rundt andre regelverk og retningslinjer som bedriften følger, og at det ikke kun gjaldt cybersikkerhet. En av intervjupersonene med bakgrunn innenfor offshore, fortalte at de var en næring med svært mye prosedyrer, retningslinjer og regelverk, og at cyberfokuset på en måte forsvant litt i alt annet. Vedkommende mente at det for all del var bra med et solid regelverk og retningslinjer å forholde seg til, men at mye kunne endres. Dog er det lettere å legge til regelverk, enn å fjerne noe.

Gullsitat:

> *Retningslinjene er bare på et papir, eller et digitalt dokument, og jeg vet ikke hvor mange det er som faktisk har lest de perm til perm. De finnes, og jeg vet hvor jeg skal lete hvis det er noe jeg lurer på. I tillegg er det retningslinjer fra IMO og BIMCO som har blitt implementert i våre egne retningslinjer.*

4.1.2 Betryggende styringssystem

Intervjupersonene opplevde at sikkerhetsfunksjonene i systemene klarte å fange opp phishing e-post, og at innføring av tofaktorautentisering på flere plattformer skapte en større trygghet. Det var dog noen som opplevde dette som tungvint og slitsomt, og da hovedsakelig på hjemmekontor eller reise. Likevel hadde de en forståelse for viktigheten av tofaktorautentisering, og at arbeid over VPN-tilkobling kunne redusere hastighet ved opplasting og lignende.

Intervjupersonene hadde også hørt om tilfeller hos andre virksomheter som hadde blitt utsatt for dataangrep og løsepengevirus, men ikke opplevd noe på egen arbeidsplass. Et tilfelle som

hadde oppstått i virksomheten til en kjenning av en av intervjupersonene, var at all data og informasjon fra de siste 20 årene hadde blitt kontaminert i forbindelse med et cyberangrep. Vedkommende kunne også fortelle at de hadde mye fokuset på cybersikkerhet i en tidligere stilling, men at det ikke er på det nivået man ser i dag. Det vedkommende la i det, var skylagring, backup-løsninger, tofaktorautentisering, krypterte plattformer, og lignende.

De uttrykte også at de stolte på egne styringssystemer og at de var relativt sikre mot potensielle angrep i større eller mindre grad. Det skal likevel presiseres at intervjupersonene ikke fremsto som naive, men det kan likevel være vanskelig å forstå omfanget av et cyberangrep når man ikke har opplevd det selv. Dette gjelder ikke bare cyberangrep isolert sett, men også andre situasjoner som kan defineres som uønsket hendelse.

Gullsitat:

> *Jeg stoler på at vi har et system som er robust nok mot de truslene som finnes der ute, og at det klarer å håndtere problemer dersom de oppstår. Jeg opplever at de sikkerhetsfunksjonalitetene vi har i våre systemer fanger opp eventuelle cyber trusler.*

4.1.3 IT-avdeling og HSEQ

Av de intervjupersonene som hadde intern IT-avdeling, uttrykte nesten alle at de hadde stor tiltro til deres arbeid. De følte seg trygge på at IT opprettholdt et system som var trygt og at de kunne bistå dersom noe usikkert skulle oppstå. I de fleste tilfellene var det IT-avdelingen som tok seg av små og store problemer som skulle oppstå på datamaskinen. Siden ingen hadde opplevd en spesifikk hendelse som kunne kategoriseres som et cyberangrep, var det heller ingen som kunne fortelle om en håndteringsprosess som har blitt brukt i en sånn hendelse. De fortalte likevel at det fantes prosedyrer på hendelseshåndtering, men at dette ikke var noe de hadde hatt behov for å oppsøke.

Intervjupersonene nevnte også at dersom uønskede e-poster ikke ble fanget opp av spamfilteret, så pleide de å blokkere avsenderen selv i tillegg til å gi beskjed til IT slik at de kunne legge inn flere begrensinger på spamfilteret. Noen andre fortalte også at prosedyrene ved et angrep eller dersom noe mistenksomt skulle oppstå, så måtte man trekke ut ledningen, varsle nærmeste leder og kontakte IT, slik at «*ekspertene får gjøre det de er eksperter på*». Det fremsto heller ikke som at folk visste så mye om håndteringsprosessen til IT, bare at de ordnet opp. Dette vil jo

også være naturlig når man ikke har mye dybdekunnskap selv, og som nevnt tidligere så hadde intervjupersonene en stilling som allerede krevde mye jobb noe som reduserte evnen og lysten til å lære mer i dybden om cybersikkerhet.

Flere nevnte også at cyber sikkerhet ikke bare var isolert til IT-avdelingen deres, men at det fantes noen på de fleste avdelingene som hadde «litt mer peiling» enn de selv og som jobbet mer aktivt med det. Disse hadde ikke nødvendigvis kun cybersikkerhet som fokusområde. I tillegg fortalte de fleste at de hadde egen HSEQ-team som blant annet jobbet med prosedyrer rundt cybersikkerhet og risikostyring, men det var stort sett IT som ble nevnt da det var spørsmål om hendelseshåndtering, prosedyrer og tekniske problemer. Dette kan komme av at man mer naturlig knytter cybersikkerhet opp mot IT, da HSEQ har flere ansvarsområder rundt sikkerhet som ikke kun omhandler digital sikkerhet.

Gullsitat:

> *Det er som oftest IT-avdelingen som tar seg av ting, så det har på en måte løpt litt av seg selv i bakkant. Det er de som håndterer prosedyrene og systemene vi bruker, og hvis det er noe problemer med innlogging eller tilganger så kontaktes de. Jeg stoler på at de håndterer de problemene som skulle oppstå.*

4.2 Bevisstgjøring

Under intervjuene ble intervjupersonene spurt om hvordan bevisstgjøringen rundt cybersikkerhet blir praktisert på deres arbeidsplass, og hvordan de selv opplever at dette har fungert. Subgruppene til dette kapittelet er derfor holdningskampanjer og økt fokus som skal skape et bilde av hvordan bevisstgjøring blir praktisert på intervjupersonenes arbeidsplass. Formålet er å se nærmere på hva de involverte tenker om læringsprosessen, omfanget og foreløpige opplevelser av dette.

4.2.1 Holdningskampanjer og opplæring

Alle intervjupersonene kunne fortelle at deres arbeidsplass praktiserte øvelser og holdningskampanjer rundt cybersikkerhet, og at noen hadde disse på en intern digital plattform i form av app eller dataprogram hvor også andre opplæringsmoduler ble publisert med jevne mellomrom.

Holdningskampanjene rundt cybersikkerhet foregikk relativt regelmessig og formatet for disse var stort sett informasjonsvideoer eller tekst, med caseløsning og avsluttende kontrollspørsmål. Noen hadde også kortere informasjonsskriv, eller påminnelsese-poster, som ble tilsendt sporadisk, mens andre hadde i tillegg en større læringsmodul som måtte gjennomføres minst én gang i året. De fleste fikk ikke frist for gjennomførelse, bare at det måtte bli gjort. Noen rederier hadde for vane å sende ut dette i forbindelse med ferier da folk kanskje reiser mer og kobler seg til Wifi flere steder. Noen innrømte også at disse kursene ofte ble nedprioritert i en travel arbeidshverdag, og at de kunne finne på å utsette det litt for lenge ifølge dem selv. Det skal dog nevnes at de alltid gjennomførte på et punkt.

Intervjupersonene ble også spurt om de opplevde noe læringsutbytte av disse kampanjene, og om dette var noe som eventuelt kunne gjøres annerledes. De fleste uttalte at formatet var bra og at de ikke hadde noen store innvendinger på hvordan det kunne blitt gjort annerledes. De fleste ønsket ikke at det ble gjort på en annen måte, da lengre og mer krevende kurs eller holdningskampanjer kunne være både tidkrevende og energikrevende. Da kunne de føle at hensikten falt litt vekk, da konsentrasjonsevnen kunne dale.

Alle intervjupersonene forsto viktigheten av læringen, men at læringsutbyttet ikke nødvendigvis var det største. Det ble nevnt at kursene ga en dypere forståelse der og da, men at det forsvant i mengden av andre arbeidsoppgaver og gjøremål. Likevel hadde alle en forståelse for at cyberrelaterte risikoer er en realitet og at konsekvensene av disse kan være svært inngripende på egen virksomhet. Noen kunne likevel se for seg at en mellomting mellom klasseromsundervisning og en læringsmodell kanskje kunne skapt litt mer forståelse og kompetanse på området.

Gullsitat:

> *IT er flinke på å regelmessig kjøre kampanjer og opplæringspakker vi må gjennom. Det er ikke alltid jeg leser så nøye på dem, og det kan fort gå litt på automatikk, spesielt i travle perioder. Formatet bidrar ikke nødvendigvis til så mye refleksjon rundt tema, det blir bare å scrolle gjennom og godta for å få det gjennomført.*

4.2.2 Økt fokus

Som nevnt i det foregående delkapittelet, så viser intervjupersonene en generell forståelse for cybersikkerhet, men de ser også alvorligheten ved cyber relaterte hendelser og konsekvensene som kan medfølge. Av de intervjupersonene som hadde vært lenge i maritim næring, kunne de tydelig se et økende fokus. Noen nevnte også at cybersikkerhet er ikke lenger noe som er isolert til hver enkelt avdeling, lokasjon eller del av organisasjonen, men faktisk noe som gjelder hele verdikjeden. Flere av intervjupersonene hadde bakgrunn som styrmann, og noen fortalte at bevisstgjøringen rundt cyber ble tydeligere da de begynte å jobbe på land.

I maritime virksomheter har det lenge vært mye sikkerhetskrav og retningslinjer når nye fartøy skal bygges, og en av intervjupersonene fortalte at det er merkbart at cyberaspektet har blitt mer og mer relevant de siste årene. Det ble også påpekt at fokuset på cybersikkerhet ikke bare burde ses i sammenheng med IT og OT som to separate aspekter, men hvordan disse henger sammen i mye større grad. Vedkommende som for tiden jobbet på et prosjekt rundt digitalisering påpekte at de kobler inn cybersikkerhet i veldig mange ledd, noe som også har medført en større bevissthet rundt tema på et individuelt plan.

I tillegg kunne omtrent alle intervjupersonene fortelle at de hadde hørt om minst ett cyberangrep ved andre selskaper, men ikke hos eget. De nevnte også at skrekkhistoriene gjør at man blir mer obs selv og at man da tydeligere ser alvorligheten ved cyberangrep. I tillegg var det tilfeller hvor det blinket i innboksen, og før de rakk å åpne e-posten så hadde spamfilteret sendt den i søppelpost. Det var oftere disse mindre hendelsene som kunne oppstå og som de nevnte da de ble spurt om de hadde opplevd et cyberangrep. Noen trodde også at det kanskje hadde skjedd i deres virksomhet en gang, men at det ikke var noe som ble videreført til andre avdelinger. Som nevnt tidligere, fremstår ikke intervjupersonene som naive, og de er innforstått med at de selv som selskap og enkeltperson kan være utsatt for et cyberangrep. Noen fortalte også at de selv har tenkt «det skjer ikke meg», selv om de likevel forstår at det ikke er realiteten.

En av intervjupersonene trakk frem den nylige hendelsen med Baltimorebroen som kollapset da et containerskip kolliderte med en av støttebjelkene. Hendelsesforløpet er ikke konkludert ennå, og vedkommende trakk heller ingen konklusjoner på at det var cyberrelatert. Hendelsen ble brukt som et eksempel på hvor store konsekvensene kan bli dersom et skip mister kontroll over fremdriften.

Gullsitat:

> *Tidligere har cyber sikkerhet vært noe kun IT-folka har snakket om, mens det nå har blitt noe mer håndgripelig som de fleste vet noe om. Jeg har merket at det kommer flere og flere krav til nybygde båter, både til verft og leverandører, men også til oss på landsiden. I tillegg så hører man om større og mindre hendelser hos andre bedrifter, og da blir man litt mer obs selv.*

4.2.3 Erfaringsbasert kunnskap

Noen av intervjupersonene som tidligere hadde vært styrmenn, eller som jobbet med digitalisering, mente at rederiene har vært mer aktive i den teknologiske utviklingen. Dette på grunnlag av at de ganske tidlig startet med mer digitalisering, og at det stadig kommer nye krav og retningslinjer til nybygg. I tillegg vil dette i stor grad også påvirke landsiden og deres måte å jobbe på.

Likevel uttrykte noen andre at det har vært et skille mellom bevisstgjøringen på skipene og for de på land. For landkontorene var det holdningskampanjer og opplæringskampanjer, som i stor grad baserte seg på informasjonshåndtering og -distribuering. Vedkommende fortalte at mannskapet ombord på skipene hadde også en tilsvarende IT-opplæring, men at de kanskje ikke fikk samme forståelse som de på landkontorene. Skipene ble mer som en egen isolert avdeling, mens de på land gjerne hadde overvåkning og monitorering av hele flåten, i tillegg til all annen informasjon som finnes på serveren. Vedkommende presiserte også at bevisstgjøringen rundt cybersikkerhet kunne variere fra skip til skip ut ifra sektor.

Det fremsto også at intervjupersonene som hadde mer utbredt kunnskap rundt cyber sikkerhet, eller som jobbet aktivt med det, hadde en bredere forståelse for viktigheten av å øke kunnskapen rundt det, både for de på land og de på sjøen. Det var også disse som var tydeligst på å mene at mer opplæring og bevisstgjøring ville være nødvendig, slik at folk bedre kan forstå omfanget og viktigheten av det. Dette er trolig i stor grad preget av økt interesse sammenlignet med noen av de andre intervjupersonene, som heller mente at opplæringen og bevisstgjøringen allerede var tilstrekkelig nok.

Gullsitat:

> *Jeg tror rederiene ligger litt mer frempå i utviklingen, både fordi det har vært krav til det, men også fordi det har vært nødvendig. Jeg håper folk er litt paranoide fortsatt, for eksempel rundt mistenksomme e-poster eller tilkobling til ukjente nettverk. Det har vi uansett blitt mye strengere på de siste årene, og vi forstår at det kan ha reelle konsekvenser.*

4.3 Informasjonssikkerhet

Denne kategorien handler om hvordan intervjupersonene deler informasjon internt og eksternt på digitale plattformer, og deres forståelse rundt cybersikkerhet og potensielle risikoer de kan møte på i arbeidshverdagen. Kategorien bidrar til å danne et bilde over hvordan intervjupersonene håndterer informasjon digitalt, både med interne og eksterne aktører.

4.3.1 Forståelse

Intervjupersonene har ingen formell bakgrunn innenfor IT eller datasikkerhet, annet enn hva de har lært på egenhånd, i regi av arbeidsplassen, eller i nåværende og tidligere stilling. Likevel oppleves det at alle har en grunnleggende forståelse om hva cybersikkerhet innebærer, og at de forstår viktigheten av å være varsom i hva man deler over digitale plattformer. I tillegg var de godt innforstått med at egen virksomhet forvaltet store verdier som kunne være attraktivt for eksterne aktører.

Det fremsto som at intervjupersonene var godt kjent med retningslinjene rundt hva som kunne deles og ikke i direkte kontakt med en annen aktør. I tillegg fortalte alle at de jobbet over VPN eller koblet til arbeidsplassens server da de var på hjemmekontor eller reise. Flere nevnte også at de heller bruker mobildata fra privat telefon i stedet for å koble til offentlige nettverk, uavhengig av passordbelagte nettverk eller ikke. Dette var både fordi det gikk raskere og var mer forutsigbart å bruke eget mobilnett, men også for å redusere den potensielle risikoen ved å koble til et ukjent nettverk. Når det kom til å koble mobilen til offentlig USB-port, var dette også noe de ikke gjorde. Dette var noe de fleste hadde lært via de holdningskampanjene og læringsmodulene arbeidsplassen pålagte de å ta.

Tofaktorautentisering og adgangskontroll er noe alle arbeidsplassene praktiserte. Til tross for at dette til tider kunne oppfatter som keitete og tungvint, var det absolutt noe de anså som nødvendig og noe de opplevde som en ekstra trygghet. Noen hadde det kun på e-post, mens andre fortalte at det ble innført ved flere programmer og plattformer. En av intervjupersonene nevnte også at å miste datamaskinen kunne være tålelig, men mobilen var gjerne den enheten som sto mellom serveren på arbeidsplassen og en selv, og at å miste kunne være mer kritisk. Dette var ikke bare av jobbmessige grunner, men også private. Vedkommende kunne fortelle at mobilen var med overalt, og på den så var alt, og «litt for mye egentlig», koblet sammen. Mobilen var også den enheten som verifiserte identitet i tofaktorautentisering, noe som dermed gjorde den til et veldig viktig verktøy.

Gullsitat:

> *Cyber sikkerhet for meg handler om at utenforstående ikke skal få tilgang til våre systemer og at man er bevisst på egne handlinger om det så bare er å koble til USB eller WiFi. I tillegg så er det viktig å forstå at det ikke kun er det jeg holder på med på min pc, men at det er en lengre verdikjede med systemer og aktører som kan påvirkes dersom noe skulle inntreffe.*

4.3.2 Begrense informasjonsdeling

Intervjupersonene kunne fortelle at e-post var det verktøyet som ble brukt mest i deres arbeidshverdag ved informasjonsdeling. De fleste kunne fortelle at de også brukte egne plattformer til å laste opp dokumenter og behandle oppgaver, men at kommunikasjonen ellers hovedsakelig foregikk over e-post. En av intervjupersonene fortalte at norsk skipsfart benytter seg blant annet av Kystverkets SafeSeaNet som er en meldeportal hvor skipene bestiller los eller andre myndighetspålagte opplysninger til norske havner og myndigheter. I andre land er det vanligere å bare bruke Excel-ark som sendes ubeskyttet og ukryptert via e-post. Vedkommende nevnte også at man ikke skal lenger enn til Storbritannia for å finne aktører som gjør dette, og at «*det kan være noen bugs i den filen som man ikke oppdager*».

Korrespondansen med eksterne over e-post kunne være mer begrenset av åpenbare grunner, mens den var mer åpen med interne. Likevel uttrykte flere at mailtråder med mange på kopi kunne skape mer støy i hverdagen dersom det ikke hadde direkte relevans til en selv eller eget arbeid. Dette var også for å redusere informasjonsdelingen og ta en vurdering på hvor mye som

faktisk er relevant å dele med andre. En av intervjupersonene fortalte også at i større prosjekter var de nødt til å gå over til SharePoint eller bruke delingsdokumenter for å begrense mailutvekslingen hver gang en liten endring ble gjort i et dokument. Dette vil jo igjen begrense informasjonsdelingen da dokumentene ble forbeholdt de som hadde tilgang, uten at dokumenter ble videresendt fra mottakeren til andre personer.

Noen kunne også fortelle at de hadde opplevd minst én anledning hvor noen hadde utgitt seg for å være noen andre, men at dette ble oppdaget relativt raskt. Dette var et tilfelle hvor noen utga seg for å være en skipsagent og etterspurte mannskapslister. I e-posten var skipets navn og posisjon riktig, men navnet skipsagenten signerte med var en person som ikke eksisterte. Sånne tilfeller kan ofte bare være tilfeldigheter, og denne hendelsen var ikke noe vedkommende ville definere som et cyberangrep.

Av annen informasjon som ble distribuert internt på arbeidsplassen, ble dette også gjort over egne plattformer. Tilganger på den interne serveren ble adgangsbegrenset ut ifra relevans og deltakende personer. Dette var blant annet for å begrense skadeomfanget dersom man skulle bli utsatt for et cyberangrep. Noen uttrykte at de hadde opplevd misnøye blant andre kollegaer da dokumentbibliotekene var lite tilgjengelige, dog var det forståelig at informasjonsdelingen måtte begrenses av sikkerhetsmessige grunner.

Gullsitat:

> *Vi begrenser tilganger der det trengs. Hvis man skulle være så uheldig å bli hacka så er det fordelaktig å begrense det potensielle skadeomfanget. I tillegg så skal man være påpasselig med å dele informasjon i mailkorrespondanse med eksterne, for man vet aldri for sikkert hvem som faktisk sitter på andre enden.*

4.3.3 Kritisk bruk av digitale plattformer

Som det har blitt nevnt, så baserte informasjonsdelingen seg stort sett på e-post. Mange bransjer innen maritim sektor bruker også egne plattformer for informasjonsdeling. Her nevnte en av intervjupersonene at dette fort kunne bli forvirrende og energikrevende da man stadig måtte sette seg inn i nye digitale plattformer til de forskjellige kundene. Noen av de faste kundene ble det dog dannet noe tilsvarende teamsgrupper med, men det var ikke nødvendigvis for sikkerheten sin del, men mer for å lette trykket på innboksen.

I tillegg fortalte de fleste at de opererte på interne plattformer og at store deler av den konfidensielle informasjonen ble distribuert på disse, og da med adgangsbegrensning. Ekstern kommunikasjon foregikk i stor grad på e-post, og noen uttrykte at de alltid forsøker å være litt kritiske til e-poster fra ukjente personer. Det samme gjaldt e-posttråder som potensielt ble videresendt til andre, og at man fort kunne miste oversikt over hva som hadde blitt sendt og kommunisert tidligere.

En av intervjupersonene fortalte at de i e-postkorrespondanse rundt kunderelevant informasjon, graderte e-postene inne i Outlook gjennom en funksjon som krypterer og utelater filer som ikke er åpne for alle. De forsøkte i stor grad å holde den mer overfladiske dialogen på e-post. Dette kom ikke direkte frem i alle de andre intervjuene, men ut ifra den informasjonen som er gitt rundt kommunikasjon via e-post ved de andre rederiene, kan det tolkes dit hen at de også benytter seg av kryptert e-post og fildeling.

Gullsitat:

> *Alle bruker forskjellige plattformer, så noen ganger kan det være vanskelig å sette seg inn i de nye systemene. Store deler av kommunikasjonen foregår via e-post, både internt og eksternt, men det er jo ikke alltid man vet hvem som sitter på andre enden, eller hva de sender til hvem. Så det må man i stor grad prøve å tenke litt mer over, plutselig sitter det noen på andre enden som ikke skal motta den informasjonen.*

4.4 Oppsummering av funn

I dette kapittelet har resultatene fra de kvalitative intervjuene blitt presentert. Den systematiske tekstkondenseringen ga fire kategorier med tilhørende subgrupper som sammen med det teoretiske grunnlaget skal forsøke å belyse problemstillingen:

> «*Hvordan opplever skipsoperatører cybersikkerhet i sin arbeidshverdag?*».

Resultatene fra samtalene med intervjupersonene viser at alle har en ganske grunnleggende forståelse rundt cybersikkerhet, og har gjennom regelmessige holdningskampanjer og opplæringsmoduler fått den innsikten de anser selv som nødvendig i en ellers travel

arbeidshverdag. Noen av intervjupersonene hadde mer kunnskap grunnet egen interesse og frivillig kursing, eller gjennom nåværende eller tidligere stilling.

Alle visste at arbeidsplassen hadde utarbeidet egne retningslinjer rundt cybersikkerhet, dog var ikke dette noe de hadde oppsøkt aktivt da det foreløpig ikke hadde vært nødvendig. Det økende fokuset rundt cybersikkerhet som har skjedd de siste årene hadde også medført relativt strengere rutiner rundt pålogging, tilkobling og tilganger på diverse interne plattformer, servere og nettverk. De hadde tillit til at arbeidsplassen og IT-avdelingen skapte et robust styringssystem, som skapte trygghet og sikkerhet mot cyberrelaterte hendelser.

Selv om ingen hadde opplevd noen store cyberangrep eller hendelser selv, hadde de hørt om andre rederier som hadde blitt utsatt. Intervjupersonene var på ingen måte naive, og var innforstått med at de selv kunne være utsatt. Likevel kan det være vanskelig å forstå omfanget av et cyberangrep når man ikke har opplevd det selv. Dette kan også relateres til risiko rundt uønskede hendelser på et generelt nivå, ved at man ofte ikke forstår omfanget fordi man har en grunnleggende antakelse om at det ikke skjer en selv. I tillegg var det ikke mange som opplevde at cybersikkerhet påvirket arbeidshverdagen i stor grad, men at det kanskje var mer ubevisst noe som skjedde i bakgrunnen, og heller noe de bare hadde blitt vant til over tid. Dette var eksempelvis med interne digitale plattformer, tofaktorautentisering, adgangsbegrensning, også videre.

Som nevnt uttrykte intervjupersonene at de ikke var eksperter på området, og foreslo andre kollegaer med «mer peiling» som jeg kunne ta kontakt med. Dette kunne vært en mulighet for å få en større dybdeforståelse i virksomhetenes arbeid med cybersikkerhet, og også få innsikt i konkrete handlingsplaner og strategier. På en annen side var målet med studiet å prate med rederienes «mannen på gata». Dette var for å få innsikt i deres erfaringer og opplevelser rundt cybersikkerhet, og derfor var det ikke nødvendig at intervjupersonene hadde mye kunnskap og ekspertise på feltet.

5 Drøfting

Dette kapittelet vil inneholde drøfting av resultatene fra de kvalitative intervjuene opp mot de teoretiske grunnlaget sett i lys av problemstillingen og de tilhørende forskningsspørsmålene som ble presentert innledningsvis i denne oppgaven. De er som følger:

«Hvordan opplever skipsoperatører cybersikkerhet i sin arbeidshverdag?»

- *Hvordan erfarer skipsoperatører at rammeverk rundt cybersikkerhet virker inn på deres arbeid?*
- *Hvordan kan læring påvirke skipsoperatørers situasjonsbevissthetet rundt cybersikkerhet?*
- *Hvordan opplever skipsoperatører nødvendigheten for informasjonssikkerhet i eget rederi?*

For å tydeliggjøre sammenhengen mellom drøfting og resultat, vil delkapitlene tilsvare kategoriene fra forrige kapittel. I dette kapittelet vil intervjupersonene bli omtalt som skipsoperatør. Til slutt vil det bli lagt frem en oppsummering av hovedfunnene.

5.1 Rammeverk

IMOs retningslinjer for cybersikkerhet påpeker viktigheten av risikovurdering, beskyttelsestiltak, policy og ansvar, opplæring og bevissthet, og overvåking og evaluering (IMO, 2022). Alle virksomheter skal ha et cyberrisikostyringssystem og følge de retningslinjene og rammeverket som er satt. Skipsoperatørene var bevisste på arbeidsplassens egne retningslinjer rundt cybersikkerhet, dog var ikke dette noe de hadde oppsøkt aktivt da det foreløpig ikke hadde vært nødvendig. Det økende fokuset rundt cybersikkerhet som har skjedd de siste årene hadde også medført relativt strengere rutiner på hvordan de koblet seg opp til servere og andre systemer. Folk flest har et lite bevisst forhold til risiko. Dette kan være fordi man som oftest forbinder risiko med de store katastrofene, mens det i virkeligheten er de mange små hendelsene som til slutt har størst påvirkning (Aarset, 2010).

5.1.1 Cyberrisikostyring

Alle virksomheter skal i teorien jobbe aktivt med cyberrisikostyring. Det krever at flere ledd i virksomheten engasjerer seg i prosessen for å sørge for at det faktisk er gjennomførbart. Med tanke på at ingen av skipsoperatørene var sentrale i utviklingen av cyberrisikostyringsprosessen på deres arbeidsplass, er det naturlig at innsikten ikke er veldig dyptgående. Likevel er det nyttig å vite mer om deres inntrykk av organisasjonens arbeid med cyberrisikostyring og hvordan de selv påvirkes eller ikke påvirkes av den. Risikostyring er ikke et engangstiltak, men noe som bør jobbes med kontinuerlig gjennom å vurdere trusler, sårbarheter, sannsynligheter, påvirkninger og risikoer, og om de tidligere iverksatte tiltakene fortsatt er hensiktsmessige (BIMCO, 2021). Skipsoperatørene kunne bekrefte at de hadde et styringssystem for cyberrisiko, dog ble dette tolket som at det var på grunnlag av holdningskampanjer og læringsmoduler de ble tilsendt fra IT og forskjellige ledelsesorganer i organisasjonen.

En av skipsoperatørene som hadde dybdeforståelse, kunne fortelle at det var vanskelig å overbevise kollegaer om reelle trusler og det helhetlige bildet rundt cybersikkerhet. Vedkommende mente dette kunne komme av at interessen ikke var like stor, og at omfanget av cybersikkerhet dermed kan oppfattes som uhåndgripelig eller bare veldig begrenset. Det vil dermed oppstå en skjevhet i cybersikkerhetskulturen dersom et fåtall fatter interesse og oppsøker mer dybdegående informasjon. Selv om de resterende skipsoperatørene forsto viktigheten av økt fokus på cybersikkerhet, ble det uttrykt at dette ikke var noe de trengte mer fokus eller læring om grunnet allerede travle arbeidsdager.

Noen at cybersikkerhet i stor grad var noe IT-avdelingen tok seg av, og dette ikke var noe de selv følte et umiddelbart behov for å lære mer om selv. DNVs rapport (2023) presiserer at cybersikkerhetskultur innen maritime organisasjoner bør jobbes aktivt med, gjennom å gjøre cybersikkerhet til en del av organisasjonens verdier, normer og adferd på alle nivåer, fra topp til bunn. De trekker frem viktigheten av å bygge en kultur hvor bevissthet rundt cybersikkerhet kan bidra til å redusere risiko og styrke robustheten mot cybertrusler (DNV, 2023). Det kan likevel være vanskelig å skape en gjennomgående og trygg sikkerhetskultur hvis forståelsen blant de ansatte oppleves å være mer overfladisk. I tillegg kan det også være problematisk dersom hverken interessen eller nysgjerrigheten er til stede blant de ansatte, dog kan dette igjen bunne i en cybersikkerhetskultur som ikke har fått slått rot i organisasjonen.

Skipsoperatørene fremsto som godt innforstått med viktigheten av fokus på cybersikkerhet, og de hadde en relativt lik beskrivelse og tilnærming til hva cybersikkerhet var for dem selv. I grove trekk ble det beskrevet som et viktig og svært nødvendig fokusområde, som krevde kritiske øyne da de forsto at dette var noe som kunne treffe hvem som helst når som helst. Det kan tolkes dithen at de forstår viktigheten av det, og at rederiet har dette som en prioritet. På en annen side kan det også fremstå som en mer overfladisk beskrivelse og tilnærming, og at de likevel ikke hadde noe særlig eksplisitt forståelse eller bredere definisjon av temaet. Noen nevnte også at man til tider kunne bli naiv og tenke at det ikke skjer en selv, men de forsto at dette ikke var tilfellet. De uttrykte at de forsøkte å være bevisst cybersikkerhet i arbeidshverdagen, men at det kunne være vanskelig å opprettholde et kontinuerlig fokus parallelt med andre ansvarsområder. Som forsker, må jeg likevel presisere at de ikke fremsto som naive under intervjuet, men at det heller er dybdekunnskapen og forståelsen som skapte et skille mellom skipsoperatørene.

Det kom frem i intervjuene at alle hadde retningslinjer de skulle følge, men at disse ikke var lest nøye gjennom. Det var i all hovedsak fordi det ikke hadde vært nødvendig å lese regelverket, men at de visste hvor de skulle lete og hvem de skulle spørre dersom noe oppsto eller var uklart. Det ble også presisert av et par skipsoperatører at de opplevde selv at forståelsen og viktigheten av retningslinjene måtte ha en tydelig forankring i ledelsen for at folk faktisk skulle ta de på alvor, noe som også har blitt presisert i rapport fra DNV (2023) og retningslinjene fra IMO (2022). Dette kan videre forklares teoretisk gjennom representativitetsheuristikken, der sannsynligheter vurderes basert på likhet og kjennetegn, ved at skipsoperatørene stoler på robustheten ved retningslinjene uten å gå særlig i dybden selv (Tversky & Kahneman, 1974).

Som intervjuer oppfattet jeg at alle respekterte de rammeverkene og retningslinjene som fantes på arbeidsplassen, men inntrykket var likevel at dette ikke var noe de fleste hadde dypdykket inn i. De uttrykte at grunnen til dette var at det ikke hadde vært nødvendig enda. På en annen side vil det være lettere å gjenkjenne potensielle cybertrusler dersom den grunnleggende forståelsen blir mer dyptgående, slik at bevisstheten forbedres ytterligere. Med tanke på at de oppfattet opplæringen som mer overfladisk, kan det være at forankringen i ledelsen og organisasjonen ikke blir tydeliggjort godt nok. Dette var noe de fikk tilsendt fra IT-avdelingen, uten noe mer forklaring på hvorfor det er viktig med utvikling av forståelse rundt cybersikkerhet.

5.1.2 Interne styringsorganer

En av skipsoperatørene jobbet for øyeblikket på et prosjekt rundt digitalisering og trakk frem en økt forståelse rundt sammenhengen mellom IT- og OT-systemer. Dette var ikke noe de andre skipsoperatørene trakk tydelig frem og som dominerte intervjuet, det var likevel ikke noe som ble spurt nærmere om så det er naturlig å heller ikke trekke det frem ytterligere. Vedkommende som trakk opp sammenhengen med IT og OT, nevnte blant annet at dette var noe som ble fokusert mer på, da de i stor grad blir ansett som to separate systemer. Dette var noe vedkommende mente burde bli sett på i en helhet da de de senere årene har blitt mer integrert og samhandler mye mer, eksempelvis gjennom fjernstyring fra land (Lund & Larsen, 2021). Ved å kontinuerlig jobbe med og inkorporere cybersikkerhet i flere ledd i arbeidet sitt, hadde vedkommende fått et nytt syn på cybersikkerhet da sårbarhetene ville treffe et mye bredere spekter enn kun innenfor IT-systemene på land.

Ansvaret rundt IT-systemene blir i stor grad tilegnet IT-avdelingen, hvor intervjupersonene også viser stor tillit. Det fremsto som at cybersikkerheten og IT-sikkerheten i stor grad var tilegnet IT-avdelingen, og at dersom et problem oppsto ble IT kontaktet umiddelbart. Skipsoperatørene nevnte at de var «ekspertene», og at de dermed stolte på at de kunne løse problemet. Likevel kan dette ha en negativ innvirkning på tolkningen av cyberhendelser og videre forståelse, da hendelsene likevel bare blir sendt videre til IT for behandling ganske raskt etter de oppstår. Dette vil igjen påvirke situasjonsbevisstheten negativt.

BIMCOs retningslinjer presiserer at cyberrisikostyring krever klare ansvarsområder og støtte på tvers av virksomheten for å lykkes (BIMCO, 2021). Det kom ikke eksplisitt frem hos alle skipsoperatørene at HSEQ-avdelingen og ledelsen hadde stor innvirkning på virksomhetens cyberrisikostyring, men det kan tolkes som at dette likevel var noe som foregikk mer i bakgrunnen uten at de ansatte fikk stor innsikt i styringsstrategien og den ønskede effekten av iverksatte tiltak. Dette er ikke noe som kan fastlås da hverken kvaliteten eller de ansvarlige rundt cyberrisikostyringen ble undersøkt i denne studien, likevel kan det tolkes dit hen at den ikke blir vektlagt godt nok på et organisatorisk nivå, slik at det dermed ikke når ut til alle ansatte. På en annen side igjen, kan den grunnleggende kompetansen og forståelsen hos de ansatte ikke være tilstrekkelig nok for å faktisk endre atferd og kompetanse gjennom optimalisert trening og opplæring.

Forankring i ledelsen ble trukket frem i et av intervjuene, og vedkommende mente at dette kunne være med til å skape en helhetlig cybersikkerhetskultur som kunne nå hele veien fra topp til bunn. Dette er også noe som ble vektlagt i rapporten fra DNV (2023) og i BIMCOs (2021) retningslinjer. Hensikten med læringsmodulene og bevisstgjøringen bør trolig presiseres ytterligere for å skape mer meningsfull tolkning av innholdet i læringsstoffet. Selv om skipsoperatørene opplevde at andre arbeidsoppgaver gjerne tok mer plass enn cybersikkerhetslæring, kan det være fordelaktig med en større inkludering i risikostyringsprosessen. Ved å la de ansatte være mer delaktige i risikostyringsprosessen, kan de føle på mer eierskap som dermed kan redusere kompleksiteten de opplever i møtet med temaet cybersikkerhet. Dette kan også forbedre evnene og arbeidsminnegjenkjenningen, som er individuelle faktorer som har en innvirkning på persepsjon og forståelse i prosessen for å oppnå situasjonsbevissthet (Endsley, 2000).

Skipsoperatørene har som nevnt ikke opplevd noen store hendelser selv, og dermed er sjansen stor for at det kan oppstå skjevheter i både persepsjon og forståelse, som videre kan ha en innvirkning på projeksjon (Endsley, 2000). Dette kan forklares gjennom forankringsheuristikken som brukes når man skal gjøre estimater eller prediksjoner med utgangspunkt i en gitt verdi, ofte ved bruk av tall som er lett tilgjengelig i minnet, og deretter justerer andre størrelser i forhold til dette (Tversky & Kahneman, 1974). De uttrykte også at forståelsen av retningslinjene var tilstrekkelige nok da det likevel ikke var de som håndterte de. I tillegg kunne de ikke presisere hvordan noe kunne bli gjort annerledes da de hverken hadde opplevd store cyberangrep selv eller på egen arbeidsplass. Dette kan være fordi cyberrisikostyringsprosessen ikke har vært tilgjengelig for de annet enn gjennom holdningskampanjer og læringsmoduler, og at de kanskje ikke har fått opplæring som er tilstrekkelig nok for å skape en helhetlig forståelse og videreutvikle kompetansen på et organisatorisk nivå.

5.2 Bevisstgjøring

Med utgangspunkt i resultatene og rapporten til DNV (2023) kan man se likheter i oppfattelsen rundt at dybdekunnskapen forblir hos «ekspertene» og at denne kunnskapen potensielt kan ha mindre spredning til resterende deler av virksomheten. I forbindelse med teori som omhandler risikostyring, cybersikkerhet, eller generell læring i organisasjoner, så blir det i de fleste tilfellene presisert at en forankring i ledelsen er nødvendig for å kunne se endring og skape en

bærekraftig sikkerhetskultur (IMO, 2022). Endsleys (2000) situasjonsbevissthetsmodell illustrerer at evner, erfaring og trening har en innvirkning på automatikk og langtidsminnet, noe som igjen har en direkte involvering i prosessen rundt å oppnå situasjonsbevissthet.

Resultatene fra de kvalitative intervjuene viste at økt opplæring i form av holdningskampanjer og læringsmoduler bidro til at intervjupersonene ble mer bevisst cybersikkerhet i sin arbeidshverdag. Det var også verdt å bemerke seg at de som jobbet tettere rundt cyber og digitalisering hadde det som en mer sentral del av sin arbeidshverdag, sammenlignet med de resterende skipsoperatørene. Hovedfokuset i denne drøftingsdelen vil ikke nødvendigvis være hvordan skipsoperatørenes situasjonsbevissthet fungerer i deres beslutningstaking, men heller hvordan den påvirkes av individuelle faktorer.

5.2.1 Cybersikkerhetslæring og holdningskampanjer

Rapporten til DNV (2023) vektlegger opplæring og tilgang på ekspertise som en kritisk del av virksomheters cyberrisikostyring. Det kom også frem i denne rapporten at det tilsynelatende var en splittelse mellom de som hadde en bredere forståelse gjennom sin stilling, de som var HSEQ-ledere eller hadde andre nøkkelroller i forbindelse med cybersikkerhet, og de som ikke hadde et spesielt forhold til det (DNV, 2023). Dette kan også relateres til resultatene fra de kvalitative intervjuene, hvor skipsoperatørene også hadde forskjellig grad av dybdekunnskap rundt cybersikkerhet. Dette er noe som potensielt kan ha en innvirkning på hvordan de forholder seg til cybersikkerhet i arbeidshverdagen og som videre kan påvirke deres situasjonsbevissthet i møte med cyberhendelser.

Evner, erfaring og trening er faktorer som kan være med på å opprettholde situasjonsbevisstheten (Endsley, 2000). Som nevnt vil noen med lengre og bredere erfaring ha mer utviklede mentale modeller og bedre strategier for å kunne styre oppmerksomheten og tolke informasjon mer effektivt. Trening kan forbedre evnen til å kjenne igjen mønster i situasjoner og skape en mer nøyaktighet av de mentale modellene. Arbeidsminnekapasitet og perseptuelle ferdigheter kan påvirker de grunnleggende prosessene som er involvert i å oppnå situasjonsbevissthet (Endsley, 2000). Skipsoperatørene hadde egen opplæring rundt cybersikkerhet, og måtte stadig gjennom læringsmoduler og holdningskampanjer i forbindelse med dette og andre stillingsrelevante ting. De uttrykte at de følte en økt bevissthet rundt cybersikkerhet da læringen fortsatt var friskt i minnet, men at dette kunne bli glemt i mengden

av andre arbeidsoppgaver. Holdningskampanjer kan til tider vektlegge kunnskapsøkning, fremfor holdnings- og atferdsendring. Økt kunnskap og rett svar på konkrete spørsmål i læringsmoduler vil ikke nødvendigvis garantere at ansatte vil anvende denne kunnskapen i sine handlinger. Kampanjer bør ikke bare informere, men også aktivt engasjerer ansatte til å endre atferd (Khan, 2011).

En av skipsoperatørene hadde utbredt kunnskap grunnet et kurs om cybersikkerhet, og hadde dermed en bredere forståelse for de sårbarhetene og risikoene ved seg selv og arbeidsplassen. Vedkommende hadde også fått presentert både store og små eksempler på cyberhendelser, og opplevde selv at egen bevissthet hadde økt betraktelig i etterkant av et sånn kurs. Zhang (2021) legger frem at cybersikkerhetslæring generelt sett er effektivt for å forbedre bevissthet og atferd rundt dette. Ved å gi konkrete eksempler kan de ansatte lettere gjenkjenne cybersikkerhetstrusler og reagere på en passende måte (Zhang, 2021). De andre skipsoperatørene hadde blitt eksponert for cyberangrep gjennom media og historier fra kollegaer og bekjentskaper, noe som kan føre til at konteksten blir amputert og at forståelsen blir begrenset til skrekkeksemplene og ikke de mindre hyppigere hendelsene. Med tanke på at de ikke ble pålagt ytterligere kursing eller kompetanseutvikling, kan det derfor være vanskeligere å se hvordan de selv og deres arbeid kan ha en relevans i cyberrisikostyring. Dette kan også relateres til DNV rapporten (2023) hvor det ble uttrykt at læringsutbyttet rundt intern opplæring kunne være snevert dersom egen stilling ikke hadde direkte relevans til cybersikkerhet. Denne skjevheten kan dermed gjøre det vanskelig å skape endring og utvikle kompetanse på et organisatorisk nivå, ved at noen får en grundigere forståelse gjennom eget initiativ og interesse.

Artikkelen til Zhang (2021) trekker også frem at kontinuitet og regelmessig læring gjør de ansatte mer bevisste og at den totale organisatoriske risikoen potensielt kan reduseres. Ansatte er ofte de som blir utsatt for cyberangrep, og derfor vil det være fordelaktig å legge ressurser i cybersikkerhetsopplæring for å øke ansattes evne til å identifisere disse (Zhang, 2021). På en annen side kunne skipsoperatørene fortelle at holdningskampanjene og læringsmodulene dukket opp med variert hyppighet basert på arbeidsplass, hvor noen blant annet hadde en større læringsmodul én gang i året. Arbeidsminnekapasitet og mønstergjenkjenning kan også relateres til forankrings- og representativitetsheuristikken. Dette er mentale snarveier som kan bidra til å ta raske beslutninger, og dersom mennesket kan relatere situasjonene til tidligere erfaring eller referansepunkt, kan beslutningene i de fleste tilfeller være gode nok (Tversky & Kahneman,

1974). Det kan være vanskelig å fastslå om dette er hyppig nok, men ut ifra de resultatene som er presentert, kan det tolkes at det ikke er tilstrekkelig nok for å forbedre bevissthet, endre atferd, og bygge en mer solid cybersikkerhetskultur. Igjen vil det være både individuelle faktorer som interesse og åpenhet, samt organisatoriske faktorer som tilrettelegging og ressursallokering som også vil kunne ha en innvirkning på atferdsendring og kulturbygging.

5.2.2 Situasjonsbevissthet og individuelle faktorers påvirkning

Mål, forventninger og erfaringer påvirker mennesker oppmerksomhet og informasjonstolkning (Endsley, 2000). Skipsoperatørener selv uttalte at de hadde merket et større fokus på arbeidsplassen siden de begynte, men at forståelsen av omfanget ble klarere i nyere tid. Det skal sies at det er vanskelig å si noe konkret om hvordan det har vært tidligere da dette ikke var noe som ble fokusert på i studien. Dog kan det potensielt forklares på grunnlag av nyere retningslinjer og rapporter innenfor maritim næring rundt cybersikkerhet som har kommet de siste årene, fra blant annet IMO (2022) og BIMCO (2021), at det kan tyde på at skipsoperatørene har opplevd et økende fokus. Dette økende fokuset kan derfor skape en større bredde i hva som vektlegges i opplæringen, noe som videre kan påvirke forventningene og målsettingen til både rederiet og de ansatte. Likevel kan feilaktige forventninger basert på manglende erfaring føre til feiltolkninger, da referansepunktet i stor grad vil være lærte eksempler og ikke egne opplevelser (Endsley, 2000). Det er ikke dermed sagt at situasjonsbevisstheten til skipsoperatørene er feil, eller at de har feilaktige forventninger, men det kan være at det ikke når opp til sitt fulle potensiale da den nåværende opplæringen i stor grad bare berører overflaten av cybersikkerhet, og at eksemplene som blir presentert kan være vanskelig å relatere til.

Erfaring er en faktor som påvirker situasjonsbevissthet, hvor bredere erfaring vil gi mentale modeller som bedre kan styre oppmerksomheten og tolke informasjonen i omgivelsene (Endsley, 2000). En av skipsoperatørene med mer dybdekunnskap trakk frem at opplæringsprogrammene de hadde bidro til å øke bevisstheten rundt cybersikkerhet, dog så vedkommende for seg at de foreløpige programmene kunne med fordel suppleres med mer dybdegående læring. Vedkommende så for seg at en mellomting mellom klasseromsundervisning og en læringsmodul kanskje kunne skapt litt mer forståelse og kompetanse på området, da den eksisterende opplæringen fremsto som veldig generell og ikke noe som ga stort utbytte til de ansatte. Resten av skipsoperatørene forsto viktigheten av

læringen, men også de uttrykte at læringsutbyttet var relativt lite. Det ble nevnt at kursene ga en bredere forståelse der og da, men at dette fort ble glemt eller nedprioritert i en ellers travel arbeidshverdag. Selv om de opplevde læringsutbyttet som lite, mente de likevel at læringen var tilstrekkelig nok og at de selv ikke følte på noe behov for å gå grundigere inn på tema.

Arbeidsmengde er også en faktor som har en innvirkning på situasjonsbevissthet, dog blir dette omtalt som en del av systemfaktorer og ikke individuelle faktorer. Det kan likevel tenkes at stress og arbeidsmengde vil ha en innvirkning på arbeidsminnekapasitet, forventninger og prosessering av informasjon, som er å finne under individuelle faktorer som påvirker situasjonsbevissthet. Eksempelvis kunne læringen vinkles til å være noe som blir en større del av arbeidshverdagen, uten at det påvirker arbeidsmengden ytterligere. I tillegg kan en bredere forståelse som et resultat av mer dybdegående læring, redusere stress i møte med problemstillinger knyttet til cybersikkerhet, noe som igjen vil ha en positiv innvirkning på situasjonsbevissthet. Som også Khan (2011) trakk frem så vil læring som fører til atferdsendring være en mer langsiktig sikkerhetsstrategi, som også kan føre til at persepsjon og forståelse blir mindre energikrevende i forkant av projeksjon under en cybersituasjon.

Alle skipsoperatørene hadde en forståelse for at cyberrelaterte risikoer er en realitet og at konsekvensene av disse kan være svært inngripende på egen virksomhet, og denne forståelsen er noe som stemmer overens med både steg 1 og steg 2 av Endsleys (2000) situasjonsbevissthetsmodell. Likevel er de individuelle faktorene som blir illustrert i modellen veldig varierende fra person til person, som det har blitt beskrevet tidligere. Dette kan videre føre til feilaktige forventninger i en cyberhendelse, og dermed vil situasjonsbevisstheten rundt cybersikkerhet være svekket. Det betyr ikke at dette er realiteten, men på grunnlag av datainnhentingen og tolkningen av materialet, kan det indikere at situasjonsbevisstheten ikke er optimalisert og at den dermed ikke har oppnådd sitt fulle potensiale. Som sagt opplevde jeg som intervjuer et større skille mellom de to med dybdekunnskap og de resterende skipsoperatørene. I tillegg til at de uttrykte det selv, var det veldig forskjell på hvor bevisst de var cybersikkerhet i de fleste arbeidsoppgaver, fritids- eller jobbreiser, samt i det private. Det er ikke dermed sagt at de resterende ikke var bevisst cybersikkerhet, men det ble tolket dit hen at dette ikke var noe som ble spesielt vektlagt i hverdagen, uavhengig av jobb eller fritid. Det kan likevel være at de var varsomme uten å tenke over det selv, men at de med dybdeforståelse gjerne så handlingene sine i en større sammenheng.

5.3 Informasjonssikkerhet

Skipsoperatørene hadde en tilsynelatende god forståelse av viktigheten rundt informasjonssikkerhet, og var innforstått med konfidensialitet og begrensning i dokumentdeling. Mange brukte egne digitale plattformer i sin arbeidshverdag, og kommunikasjon foregikk hovedsakelig på e-post. Noen nevnte at mange av tiltakene de gjør både bevisst og ubevisst har kommet i etterkant av holdningskampanjer og læringsmoduler. Likevel er dette mer forhåndsregler som de ble pålagt å følge, og noen uttrykte at mye av dette var selvforklarende. De opplevde at rederiet hadde en cyberrisikostyringsstrategi som fungerte, men som stadig var under utprøving.

Noen kunne dele opplevelser om et stort antall autentiseringsapper, som føltes mer tyngende og slitsomt, og at hensikten med de forsvant i det styret disse appene medførte. Dette var fordi de forskjellige appene autentiserte tilgang til forskjellige plattformer igjen, slik at det ble rotete og vanskelig å holde oversikt over nye apper og hvilke som var utgående. Igjen kan det trekkes tråder til situasjonsbevissthet, da et dårlig utformet brukergrensesnitt i apper og systemer, som egentlig bare oppleves som komplekst og vanskelig å forstå, kan ha en negativ innvirkning på situasjonsbevisstheten hos brukerne av disse systemene (Endsley, 2000).

5.3.1 Systemfaktorers påvirkning av situasjonsbevissthet

Zhang (2021) nevner blant annet at mennesker ofte utgjør det svakeste leddet i verdikjeden når cybersikkerhet blir diskutert, og at de dermed utgjør den største risikoen i en virksomhet. Som det ble diskutert i forrige kapittel, så er det mange faktorer som spiller inn på situasjonsbevisstheten og menneskelig atferd i cybersikkerhet. Det er dermed ikke nødvendigvis slik at mennesket i seg selv er et svakt ledd, men at systemene rundt gjør de til et svakere ledd. Mennesket er en ressurs, som blir opplært etter en viss standard og tilegner seg egenskaper og kunnskap det trenger for å gjøre en god jobb (Bergsjø & Windvik, 2020). Dette kan videre forklares med situasjonsbevissthet, da både systemkapasitet, brukergrensesnitt og arbeidsmengde som systemfaktorer, og evner, erfaring og trening som individuelle faktorer, har en direkte innvirkning på den totale situasjonsbevisstheten, noe som innebærer de tre individuelle stegene (Endsley, 2000). På en måte kan det stemme at mennesket utgjør en stor risiko og er det svakeste leddet, men det bør presiseres at dette i større grad er på grunn av de omkringliggende organisatoriske faktorene som gjør mennesker mindre robuste ved å begrense evnen til persepsjon, forståelse og projeksjon i møte med cyberhendelser.

Kompetanse og risikooppfattelse har tilknytning til hverandre. For å kunne definere noe som en risiko, kreves det også noen kunnskaper om temaet. Phishing e-poster er en av de vanligste måtene å spre skadelig programvare eller innhente informasjon fra mottakeren på. For å kunne forstå risikoen ved å klikke på en lenke eller vedlegg i en sånn e-post, må de ansatte også være klar over muligheten for at det kan oppstå (Bergsjø & Windvik, 2020). Noen av skipsoperatørene kunne fortelle om opplevelser hvor de hadde blitt utsatt for noe de vil anse som phishing. Dette ble i stor grad filtrert ut av spamfilteret, men de få som kom gjennom var i de fleste tilfellene åpenbare phishing e-poster. Andre hadde opplevd at en avsender utleverte seg for å være en person som ikke eksisterer. Selv om vedkommende i denne e-posten ikke etterspurte noe de definerte som veldig konfidensielt, var det likevel noe som ble plukket opp som mistenksomt da dette ikke er vanlig kutyme å kontakte skipsoperatører for denne informasjonen. Kunnskap om hyppigheten av slike hendelser vil være fordelaktig for å kunne oppdage kjennetegnene og også forstå konsekvensene av de beslutningene man tar, altså vil denne kunnskapen også ha en innvirkning på optimaliseringen av situasjonsbevisstheten gjennom persepsjon, forståelse og projeksjon. Dersom de konstant blir skjermet for disse mindre tilfellene, kan det også være vanskelig å kjenne igjen mønster eller utforming de gangene de havner i innboksen.

Oppfattelse av risiko svært preget av subjektive faktorer noe som dermed kan føre til forskjellige tolkninger av risikoen (Bergsjø & Windvik, 2020). Risikooppfattelse på lik linje som situasjonsbevissthet vil også være preget av ferdigheter, erfaringer og læring, i tillegg til forventninger, langtidsminne, automatikk og arbeidsminnekapasitet slik som det har blitt diskutert nærmere i forrige delkapittel (Endsley, 2000). I tillegg vil risikooppfattelsen bli påvirket av systemdesign, kompleksitet og brukergrensesnitt. Et velutviklet og robust spamfilter på e-posten vil selvfølgelig være positivt da man tidlig kan eliminere de mindre risikoene fra phishing og spam e-post. Likevel vil det være vanskelig å gjenkjenne disse e-postene når man ikke blir eksponert for hverken de eller andre eksempler på phising e-posters utforming. Spamfilteret kan redusere stress og arbeidsmengde, men dersom de faktisk dukker opp i innboksen, kan det være en fare for at de ansatte ikke kjenner igjen faremomentene. Skipsoperatørene kunne trekke frem et eller to skrekkeksempler som de hadde lest om eller blitt fortalt ved en tidligere anledning. De hadde ikke opplevd at noe de selv har delt har kommet på avveie eller lignende, i så fall var ikke dette noe de visste om. Likevel bidrar disse eksemplene på å gjøre de mer varsomme, noe som kan være påvirket av tilgjengelighetsheuristikken

(Tversky & Kahneman, 1974). Eksponering av disse skrekkeksemplene bør også gjelde for de mindre hendelsene. Det er ikke dermed sagt at forståelsen vil økes betraktelig, men det vil trolig være med på å skape et mer nyansert syn på de cybertruslene som eksisterer.

Noe annet som også ble nevnt avskipsoperatørene da de fikk spørsmål om intern informasjonsdeling og bevissthet rundt cyberrisikoer i arbeidet, kunne de fleste bekrefte at dette var noe de ikke tenkte så mye over, da det var noe som gikk mer på automatikk. Automatikk er en del av de individuelle faktorene i situasjonsbevissthetsmodellen, og sammen med informasjonsprosesseringsminnet og langtidsminne, kan dette gi en indikasjon på at de innehar situasjonsbevisstheten rundt cybersikkerhet. Likevel skal man ikke anta at dette er tilfellet, automatikk vil videre påvirkes av ferdigheter, erfaringer og læring, og det er vanskelig å fastslå at disse faktorene faktisk har påvirket automatikken i arbeidet deres.

Representativitesheuristikken vil også kunne være relevant når skipsoperatørenes forhold til informasjonssikkerhet drøftes. Siden de mindre hendelsene eller problemene i stor grad sendes videre til behandling hos IT-avdelingen, vil lignende hendelser være vanskelig å behandle av skipsoperatørene selv, dersom IT-avdelingen ikke skulle være tilgjengelig. En kan også si at representativitetsheuristikken er til stede i de mindre hendelsene, som når e-post kommer gjennom spamfilteret og rapporterer videre til IT. Det kan også trekkes paralleller til situasjonsbevissthet og hvor persepsjon og forståelse er begrenset, eller nærmest utelatt, før steg tre settes i gang ved å sende problemet videre til IT-avdelingen (Endsley, 2000). Mangel på erfaring med cyberhendelser kan gjøre at det oppstår en skjevhet på grunn av at skipsoperatørene ikke ser det totale omfanget på lik linje som IT-avdelingen, noe som kan sees i sammenheng med representativitet. Det kan også oppstå en skjevhet da fiendtlige aktører stadig endrer angrepsmønster og omfang, og at noe blir oversett. Det er ikke bare phishing e-post som blir brukt, men også hotspot nettverk, tilkobling av USB på offentlige steder, klikke på lenker på mobilen og koble mobilen til nettleser, og så videre.

Stanton og Salmon (2017) nevner at problemet med automatisering og mer intelligente systemer, i verste fall bare kan forverre problemet i stedet for å forminske det. Dette fordi at informasjonsstrømmen mennesker møter er ganske stor, og at man dermed ikke evner å se tydelige sammenhenger for å videre kunne tolke den faktiske informasjonen og dermed handle deretter. Dette kan også være en forklaring på hvorfor cybersikkerhetslæringen kan fremstå som overfladisk, da de systemene siler ut potensielle cyber trusler for å redusere arbeidsmengden.

Automatiserte systemer kan avlaste kognitive belastninger, men også føre til tap av situasjonsbevissthet hvis brukerne blir altfor avhengige av dem (Stanton & Salmon, 2017).

5.4 Oppsummering

Kapittelet har tatt for seg en drøfting av det teoretiske grunnlaget opp mot resultatene fra de kvalitative intervjuene. Drøftingen har tatt utgangspunkt i problemstillingen *«Hvordan opplever skipsoperatører cybersikkerhet i sin arbeidshverdag?»,* samt tilhørende forskningsspørsmål.

Alle virksomheter skal jobbe aktivt med cyberrisikostyring, noe som vil kreve engasjement og ressurser fra flere ledd i en organisasjon. Selv om skipsoperatørene kunne bekrefte at arbeidsplassen hadde et cyberrisikostyringsssystem, var dybdeforståelsen av dette og retningslinjene mer varierende. De var bevisst viktigheten av økt fokus på cybersikkerhet, men dette var likevel noe de ikke følte stort eierskap til selv, med mindre de hadde mer dybdeforståelse grunnet stilling eller egen interesse. Det kunne derfor tolkes dit hen at resten av skipsoperatørenes forståelse av cybersikkerhet var mer på overflaten, og i stor grad noe de ble kurset om regelmessig fordi det var et krav. De med mer dybdekunnskap følte i større grad at cybersikkerhet var en stor del av arbeidshverdagen sammenlignet med de resterende skipsoperatørene.

Generelt sett overlates store deler av ansvaret til IT-avdelingen, noe som kan ha en negativ innvirkning på situasjonsbevisstheten rundt cybersikkerhet ved at de ikke kan gjenkjenne, forstå eller tolke trusler dersom de skulle oppstå. Videre kan forankring i ledelsen og organisasjonen være viktig for at cyberrisikostyringen skal nå ut til flere ledd og dermed bidra til en mer helhetlig atferdsendring. Inkludering av ansatte i risikostyringsprosessen og kontinuerlig opplæring vil bidra til å skape en større robusthet i ansattes situasjonsbevissthet rundt cybersikkerhet.

Ingen av skipsoperatørene hadde opplevd store cyberhendelser, noe som kan føre til skjevheter i persepsjon og forståelse, og videre deres evne til å forstå risikoer. De opplevde retningslinjene som tilstrekkelige, men kunne spesifisere forbedringer eller endringer for å optimalisere de ytterligere. Dette kan komme av at helhetlig forståelse og dybdekunnskap ikke er like stor hos alle intervjupersonene, og at det dermed oppstår et skille mellom disse. Dette tyder også på at

retningslinjene rundt opplæring og cyberrisikostyring bør styrkes og utvikles for å skape et mer universalt utgangspunkt og kompetansenivå som har organisatorisk forankring.

DNV (2023) understreker viktigheten av opplæring og tilgang til ekspertise i cyberrisikostyring. Som nevnt kom det frem i intervjuene at det var et skille mellom de med utbredt kompetanse og de med grunnleggende forståelse. Slike forskjeller kan ha en innvirkning på deres situasjonsbevissthet ved cyberhendelser. De med mer kunnskap vil ha en bredere forståelse av temaet, og dermed lettere oppdage, tolke og forstå en situasjon som de deretter må håndtere. Dette vil skape en skjevhet i hvordan organisasjonen i sin helhet forholder seg til cybersikkerhet, noe som ikke er optimalt for å kunne oppnå en gjennomgående og robust cybersikkerhetsstyring.

Endsley (2000) trekker frem evner, erfaring og læring som avgjørende individuelle faktorer for å oppnå situasjonsbevissthet. Intervjupersonene kunne fortelle at cybersikkerhetslæringen gjennom holdningskampanjer og læringsmoduler gjorde de mer bevisst cybersikkerhet i etterkant av gjennomførelsen. Skipsoperatørene uttrykte at denne læringen var lite dybdegående og mer overfladisk, men at de likevel ikke så behovet for mer læring da arbeidshverdagen var travel nok i utgangspunktet. På en annen side kan regelmessig og kontinuerlig læring som vektlegger atferdsendring ha en større effekt enn sporadisk og generell læring. Dette kan føre til at cybersikkerhet blir en større del av arbeidet i stedet for et ekstra element skipsoperatørene må hensynta.

Mye av eksemplene på cyberhendelser blant skipsoperatøene kom i stor grad av medieoppslag og fortellinger fra kollegaer og bekjente. Disse hendelsene var gjerne store og ekstreme tilfeller. Det kan dermed være vanskelig å forstå at dette kan skje en selv, og at mange små hendelser kan akkumulere til en større hendelse som kan ha store konsekvenser. Ansatte er ofte ansett som et mål for cyberangrep og derfor vil det være viktig for virksomheter å investere i god og gjennomgående opplæring av sine ansatte. I mange tilfeller blir mennesket omtalt som det svakeste ledd og organisasjoners største risiko. Det skal dog sies at det i større grad er systemet rundt som fører til disse feilene og svakhetene da tilretteleggingen og opplæringen av den menneskelige ressursen ikke er tilstrekkelige nok. I tillegg kan økt automatisering og teknologiutvikling bidra til å avlaste kognitive belastninger, dog er det en fare for at menneskene taper situasjonsbevissthet da de blir altfor avhengige av systemene rundt (Stanton & Salmon, 2017).

Skipsoperatørene viste forståelse for viktighetene av informasjonssikkerhet og var klar over behovet for konfidensialitet og begrenset informasjonsdeling. De opplevde selv at denne varsomheten var et resultat av holdningskampanjer og læringsmoduler, men at noen av disse tiltakene likevel var noe selvforklarende. De fleste mente også at sikkerhetsstyringssystemet fungerte godt, men at det stadig var under utvikling. Noen påpekte imidlertid at antallet autentiseringsapper opplevdes som overveldende og gjorde arbeidshverdagen mer komplisert, grunnet dårlig brukergrensesnitt. Det kan videre redusere situasjonsbevisstheten da systemene kan være vanskelig å forstå og håndtere effektivt. Dette er også et eksempel som kan underbygge at dårlige styringssystemer gjør mennesker til et svakere ledd og dermed mer sårbare for risikoer. Mennesker er ressurser som tilegner seg kunnskap gjennom læring og erfaring for å kunne effektivisere arbeidet.

Uønskede e-poster som phishing og lignende ble i stor grad fanget opp av spamfilteret. I de tilfellene hvor noe slapp gjennom ble det gitt beskjed til IT, og mailene ble blokkert og slettet. Likevel kan lite eksponering for disse eller andre mindre cyberhendelser svekke gjenkjenningen av sånne tilfeller. Gjenkjenning og forståelse er viktig for å kunne handle riktig. Oppfattelsen av risiko vil være subjektiv og påvirket av individuelle faktorer som ferdigheter og erfaringer. Dette er også noe som kom frem i intervjuene hvor dette skillet mellom de med dybdeforståelse og de andre ble tydeligggjort. Spamfilter og lignende kan redusere risiko og arbeidsmengde, men likevel svekke risikoforståelsen. Når majoriteten av eksemplene de blir presentert kun er store skrekkeksempler, kan det være vanskelig å forstå at også mindre og hyppige hendelser kan gi store konsekvenser. Effektiviteten i håndtering vil også være svekket når forståelsen ikke er tilstrekkelig nok.

6 Avslutning

I dette avsluttende kapittelet vil det kort bli redegjort for hvilke implikasjoner for praksis dette studiet kan ha, samt en del om forslag til videre forskning.

6.1 Implikasjoner for praksis

Resultatene som har blitt presentert har omhandlet skipsoperatørers opplevelse av cybersikkerhet i sin arbeidshverdag, herunder rammeverk, cyberrisikostyring, læring og informasjonssikkerhet. Studiet har belyst hvordan dette og individuelle faktorer har hatt en innvirkning på situasjonsbevisstheten rundt cybersikkerhet hos skipsoperatører i norske rederier. Organisasjoner med styringssystem og opplæringsprogram som ikke lærer opp og gjør ansatte mer robuste i møte med cyberrisikoer, gjør menneskene til en større risiko enn ressurs. Studiet gir en implikasjon på hvilke individuelle faktorer og systemfaktorer som i større eller mindre grad påvirker skipsoperatørers situasjonsbevissthet rundt cybersikkerhet. Det kan dermed argumenteres for at mer dybdegående opplæring av ansatte og tilrettelegging i styringssystemene kan gi en større atferdsendring på et organisatorisk nivå, som igjen kan styrke cybersikkerheten hos rederiene.

6.2 Videre forskning

Det vil stadig være mer behov for ytterligere forskning rundt det menneskelige aspektet innenfor cybersikkerhet, uavhengig næringstilhørighet. Videre kan det være viktig tilrettelegge for en bredere og mer dyptgående kompetanseutvikling rundt cybersikkerhet i flere ledd av organisasjoner, og sørge for en opplæring som ikke bare gir forståelse og kunnskapsutvikling, men også holdnings- og atferdsendring på sikt. I tillegg kan det være hensiktsmessig å se hvordan cyberrisikostyring blir praktisert og hvordan dette kan forankres i organisasjonen.

7 Referanser

Aarset, M. (2010). *Kriseledelse.* Bergen: Fagbokforlaget.

Aarset, M., & Glomseth, R. (2019). *Police Leadership during Challenging Times.* NTNU.

Aarset, M., Glomseth, R., & Juvkam, P. C. (2021). Situational awareness during a crisis. I J. Albrecht, & G. Heyer, *Enhancing Police Service Delivery, Global Perspectives and Contemporary Policy Implications.* Sveits: Springer Cham.

Bergsjø, H., & Windvik, R. (2020). *Datasikkerhet for ledere - hvordan beskytte din virksomhet* (1. utg.). Oslo: Universitetsforlaget.

BIMCO. (2021). *The Guidelines on Cyber Security Onboard Ships.* Hentet november 15, 2023 fra BIMCO: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Cunningham, M. (2019). *Thinking About Thinking: Exploring Bias in Cybersecurity with Insights from Cognitive Science.* Forcepoint.

Datatilsynet. (2024). *Ordliste*. Hentet mai 8, 2024 fra Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/#I

DNV. (2023). *MARITIME CYBER PRIORITY 2023.* DNV.

DNV. (2024). *Maritime Cyber Security*. Hentet april 29., 2024 fra DNV: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/

Dvergsdal, H. (2021, desember 1). *Digitalisering*. Hentet mai 20, 2024 fra Store Norske Leksikon: https://snl.no/digitalisering

Endsley, M. (2000). Theoretical Underpinnings of Situation Awareness: A Critical Review. *Situation Awareness Analysis and Measurement*.

Endsley, M. (2015, februar 24). Situation awareness misconceptions and misunderstandings. *Journal of Cognitive Engineering and Decision Making*.

IMO. (2022, juni 7). *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.* International Maritime Organization. London: International Maritime Organization. Hentet mars 17, 2023 fra International Maritime Organization: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

IMO. (2024). *Introduction to IMO*. Hentet april 30, 2024 fra International Maritime Organization: https://www.imo.org/en/About/Pages/Default.aspx

Johnson, C. K., & Gutzwiller, R. S. (2020). *A Cyber-Relevant Table of Decision Making Biases and their Definitions.* ResearchGate.

Kaschner, H. (2021). *Cyber Crisis Management: The Practical Handbook on Crisis Management and Crisis Communication.* Berlin, Tyskland: Springer International Publishing.

Kessler, G. C., & Shepard, S. D. (2022). *Maritime Cyber Security - A Guide for Leaders and Managers* (2. utg.). Wroclaw: Amazon Fulfillment.

Khan, B. (2011, oktober 28). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*.

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

Lund, M. S., & Larsen, M. H. (2021). Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review.

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

NSM. (2020). *NSMs grunnprinsipper for IKT-sikkerhet.* Sandvika: Nasjonal Sikkerhetsmyndighet.

Sjøfartsdirektoratet. (2020). *Overordnet strategi for maritim digital sikkerhet.* Sjøfartsdirektoratet og Kystverket.

Stanton, N. A., & Salmon, P. M. (2017, februar 06). State-of-science: situation awareness in individuals, teams and systems. *Ergonomics*.

Tjora, A. (2017). *Kvalitative forskningsmetoder i praksis* (3. utg.). Oslo: Gyldendal.

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, ss. 1124-1131.

Zhang, Z. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management + Data Systems*, ss. 613-636.

8 Vedlegg

VEDLEGG 1: Vurdering fra Sikt

Sikt

Vurdering av behandling av personopplysninger

Referansenummer
248692

Vurderingstype
Automatisk

Dato
10.02.2024

Tittel
Masteroppgave

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

Prosjektansvarlig
Idun Bakken

Student
Idun Bakken

Prosjektperiode
08.01.2024 - 23.06.2024

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 23.06.2024.

Meldeskjema

Grunnlag for automatisk vurdering
Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
  - Rasemessig eller etnisk opprinnelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - Genetiske data
  - Biometriske data for å entydig identifisere et individ
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

Informasjon til de registrerte (utvalgene) om behandlingen må inneholde

- Den behandlingsansvarliges identitet og kontaktopplysninger

- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)
- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)
- Hvor lenge personopplysningene vil bli behandlet
- Retten til å trekke samtykket tilbake og øvrige rettigheter

Vi anbefaler å bruke vår mal til informasjonsskriv.

Informasjonssikkerhet
Du må behandle personopplysningene i tråd med retningslinjene for informasjonssikkerhet og lagringsguider ved behandlingsansvarlig institusjon. Institusjonen er ansvarlig for at vilkårene for personvernforordningen artikkel 5.1. d) riktighet, 5. 1. f) integritet og konfidensialitet, og 32 sikkerhet er oppfylt.

Vedlegg 2: Informasjonsskriv og samtykkeskjema

Forespørsel om deltakelse i forskningsprosjektet:

"Cyber risikostyring og situasjonsbevissthet"

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

Bakgrunn og formål

I dette studiet ønsker jeg å finne ut av hvordan cyber risikostyring har påvirket skipsoperatørers situasjonsbevissthet knyttet til behandling av sensitiv informasjon internt i rederiet. På bakgrunn av dette ønsker jeg å intervjue fem crew managers/vessel managers for å tilegne meg kunnskap om erfaringer med overstående tema.

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

Hvem er ansvarlig for forskningsprosjektet?

NTNU i Ålesund er ansvarlig for prosjektet.

Hva innebærer det for deg å delta?

Jeg ønsker å gjennomføre et intervju med deg som tar ca. 30-60 minutter. Dette er tenkt som en samtale der du kan fortelle fritt om dine erfaringer rundt overstående tema. Spørsmålene vil ha fokus på dine erfaringer og perspektiver på temaet. Samtalen vil bli tatt med lydopptaker, og opptaket vil bli slettet ved prosjektets slutt.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake 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

Jeg vil bare bruke opplysningene om deg til de formålene som er nevnt i dette skrivet. Opplysningene vil bli behandlet konfidensielt og i samsvar med personvernregelverket.

Opplysningene fra deg, samt de andre intervjuobjektene, vil kun benyttes som grunnlagsmateriale for drøfting i min mastergradsoppgave. Opplysninger som kan kobles til deg vil anonymiseres eller utelates for å bevare din anonymitet. Personopplysningene vil holdes adskilt fra øvrige data, og det er kun jeg som kommer til å ha tilgang til disse. Lydopptaket og transkriberingen vil bli lagret passordbeskyttet på ekstern minnepenn. I arbeidet med datamaterialet vil jeg anvende fiktive navn på intervjupersoner. Det skal ikke være mulig å gjenkjenne deg i den ferdige publikasjonen.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Prosjektet vil etter planen avsluttes i utgangen av juni 2024. Da vil alt datamaterialet bli slettet, og utskrevne intervju makulert.

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

På oppdrag fra NTNU i Ålesund har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

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

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- NTNU i Ålesund ved Marie Haugli-Sandvik (veileder), e-post: marie.h.sandvik@ntnu.no
- Idun Bakken (student), telefon: 901 35 228 eller e-post: idunba@ntnu.no
- Vårt personvernombud: Thomas Helgesen, e-post: thomas.helgesen@ntnu.no

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via: e-post: personverntjenester@sikt.no eller telefon: 739 84 040.

Med vennlig hilsen

Idun Bakken

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «*Cyber risikostyring og* situasjonsbevissthet», og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervjuundersøkelsen

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet ved utgangen av juni 2024.

(Signert av prosjektdeltaker, dato)

Vedlegg 3: Intervjuguide

Hva jeg ønsker å vite	Forslag til spørsmål
Informasjon før opptak	Fortelle kort om tema (bakgrunn og formål) Fortelle hva intervjuet skal brukes til, samt taushetsplikt og anonymitet Spørre om noe er uklart, få samtykke til å sette i gang intervjuet
Personalia	Utdanning Hvor mange år i arbeidslivet/arbeidsplassen? Nåværende stilling
Tanker rundt cyber risiko	Hva er cyber risiko for deg? Hvordan påvirker, eller påvirker ikke, cyber risiko din arbeidshverdag?
Formelle retningslinjer	Har arbeidsplassen egne retningslinjer for cyber risikostyring? Hvordan opplever du at disse fungerer i praksis? Opplever du at disse retningslinjene bidrar til å skape en større trygghet?
Personlige opplysninger og digitale verdier	Hva slags digitale verdier er det du håndterer? Hvordan vurderer dere cyber risikoer i forhold til de verdiene dere håndterer
Cyber situasjonsbevissthet	Har du opplevd hendelser som du vil kategorisere som cyberangrep? Hvordan oppdaget/vurderte/håndterte du denne hendelsen? Tror du at du kan være utsatt for et cyberangrep?

	Hvorfor tror du den informasjonen du sitter på kan være attraktiv for eksterne aktører?
Bevisstgjørelse og læring	Hva gjør arbeidsplassen for å unngå at uønskede hendelser i form av cyber angrep skal oppstå? Hvordan skal sånne typer hendelser håndteres?
Oppsummering og avrunding	Er det noe mer du ønsker å tilføye? Tanker eller opplevelser rundt det som har blitt snakket om? - Hvorfor er det viktig? Hva kan gjøres? Oppsummere hovedmomentene i intervjuet

Vedlegg 4: KI-deklarasjon

NTNU

Deklarasjon om KI-hjelpemidler

Har det i utarbeidingen av denne rapporten/avhandlingen blitt anvendt KI-baserte hjelpemidler?

- ○ Nei
- ◉ Ja

Hvis *ja*: spesifiser type av verktøy og bruksområde under.

Tekst

- ☑ **Stavekontroll.** Er deler av teksten kontrollert av: *Grammarly, Ginger, Grammarbot, LanguageTool, ProWritingAid, Sapling, Trinka.ai* eller lignende verktøy?
- ☐ **Tekstgenerering.** Er deler av teksten generert av: *ChatGPT, GrammarlyGO, Copy.AI, WordAi, WriteSonic, Jasper, Simplified, Rytr* eller lignende verktøy?
- ☐ **Skriveassistanse.** Er en eller flere av ideene eller fremgangsmåtene i oppgaven foreslått av: *ChatGPT, Google Bard, Bing chat, YouChat* eller lignende verktøy?

Hvis *ja* til anvendelse av et tekstverktøy - spesifiser bruken her:

Stavekontroll i form av hjelp til formuleringer og setningsoppbygging, samt oversettelse av tekst fra engelsk til norsk. Brukte ChatGPT.

Koder og algoritmer

- ☐ **Programmeringsassistanse.** Er deler av koden/algoritmene som i) fremtrer direkte i rapporten eller ii) har blitt anvendt for produksjon av resultater slik som figurer, tabeller eller tallverdier blitt generert av: *GitHub Copilot, CodeGPT, Google Codey/Studio Bot, Replit Ghostwriter, Amazon CodeWhisperer, GPT Engineer, ChatGPT, Google Bard* eller lignende verktøy?

Hvis *ja* til anvendelse av et programmeringsverktøy - spesifiser bruken her:

Bilder og figurer

- ☐ **Bildegenerering.** Er ett eller flere av bildene/figurene i rapporten blitt generert av: *Midjourney, Jasper, WriteSonic, Stability AI, Dall-E* eller lignende verktøy?

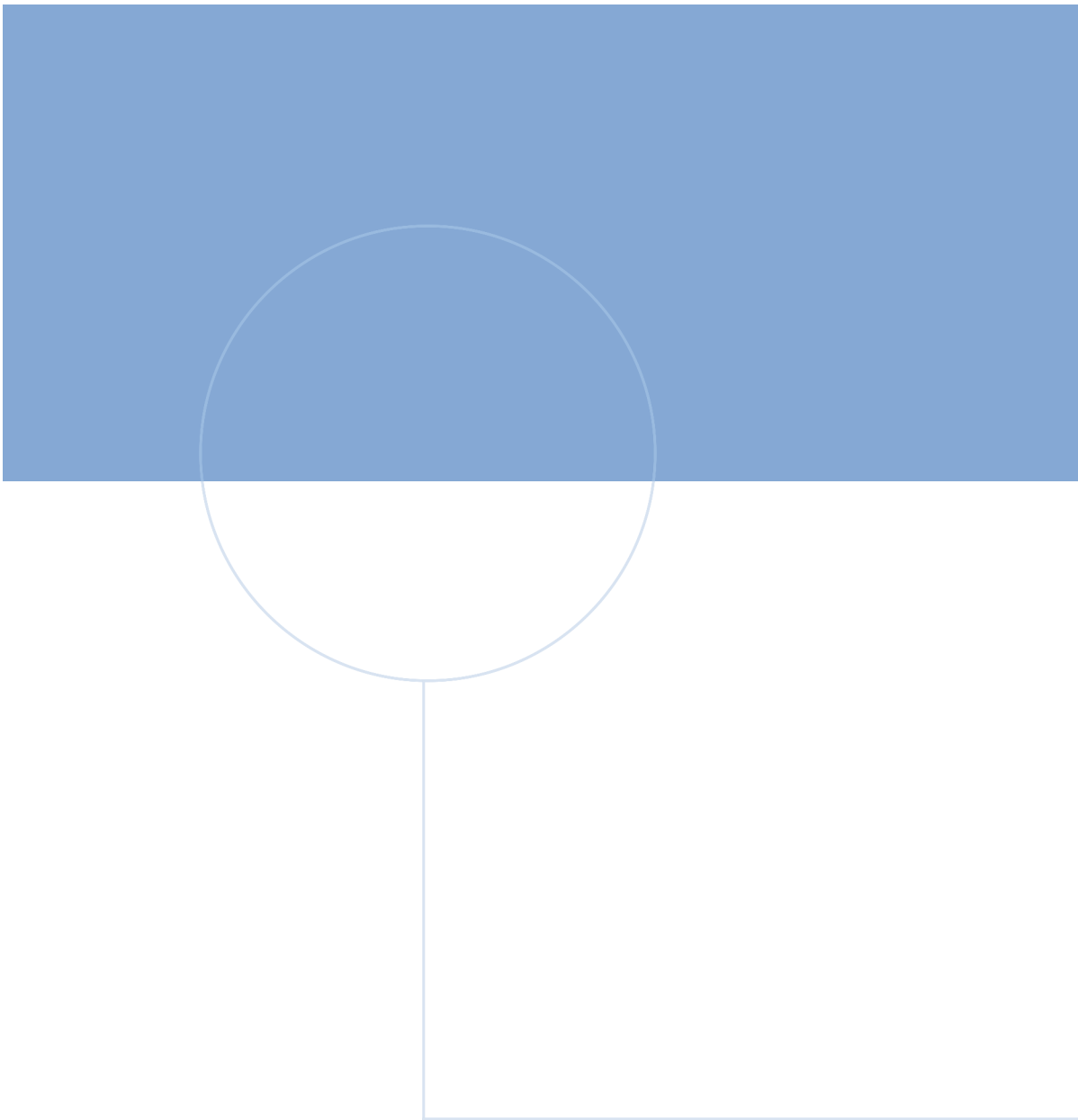
Hvis *ja* til anvendelse av et bildeverktøy - spesifiser bruken her:

Andre KI-verktøy. Har andre typer av verktøy blitt anvendt? Hvis *ja* spesifiser bruken her:

- ☑ Jeg er kjent med NTNUs regelverk for bruk av kunstig intelligens. *Jeg har redegjort for all anvendelse av kunstig intelligens enten i) direkte i rapporten eller ii) i dette skjemaet.*

Idun Bakken, 23.05.24, Ålesund

Underskrift/Dato/Sted



NTNU

Kunnskap for en bedre verden