Universitetet
i Stavanger

Operatørselskapene i petroleumssektoren sitt syn på sikringskultur

- Bruk eller ikke bruk av begrepet sikringskultur

Master i Samfunnssikkerhet
Institutt for medie-, kultur- og samfunnsfag
Universitetet I Stavanger

Caroline Østensjø & Caroline Irwin Larsen
Våren 2015

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I
SAMFUNNSSIKKERHET

MASTEROPPGAVE

SEMESTER:
Våren 2015

FORFATTER:
Caroline Østensjø & Caroline Irwin Larsen

VEILEDER:
Sissel H. Jore

TITTEL PÅ MASTEROPPGAVE:
Operatørselskapene i petroleumssektoren sitt syn på sikringskultur
- Bruk eller ikke bruk av begrepet sikringskultur

EMNEORD/STIKKORD:
Security, safety, sikring, sikkerhet, sikringskultur, sikkerhetskultur, trussel, verdi, sikringsrisiko, sikringsnivå, organisasjonskultur, kultur, usikkerhet, operatørselskaper, petroleumssektoren

SIDETALL: 116

STAVANGER ……..
DATO/ÅR

Sammendrag

Et endret risikobilde i Norge samt en rekke alvorlige hendelser internasjonalt og nasjonalt, har medført til et økt fokus på sikring og risiko for intenderte uønskede hendelser i petroleumssektoren og samfunnet forøvrig. I lys av dette har kulturens betydning for sikringsnivået blitt fremhevet i en rekke sammenhenger og begrepet security culture, på norsk sikringskultur, har blitt løftet frem. Dette fremkommer blant annet i Statoil sin gransknings rapport *Angrepet mot In Amenas* (Statoil, 2013). Operatørselskaper i petroleumssektoren har lang erfaring med utvikling av en sikkerhetskultur og har et godt rykte på seg når det gjelder sikkerhet mot uintenderte uønskede hendelser. Likevel er det begrenset forskning omkring sikringskultur både som begrep og fenomen. Avhandlingen tar dermed sikte på å undersøke hvilket syn operatørselskapene i petroleumssektoren har på utvikling av en optimal sikringskultur og hvorvidt begrepet sikringskultur fremstår som hensiktsmessig i arbeidet med å utvikle en slik kultur.

For å være i stand til å besvare avhandlingens problemsstilling ble det benyttet en kvalitativ metode. Dette fordi det var lite forskningsbasert kunnskap omkring sikringskultur og fordi vi ønsket å få en dybdeforståelse for temaet. Det ble gjennomført 14 intervjuer med 12 ulike operatørselskaper i petroleumssektoren, med fagpersoner innen security/HMS feltet. Grunnet begrenset litteratur innen sikringskulturfeltet, ble det i stor grad benyttet teori om sikkerhetskultur som har blitt presentert i samfunnssikkerhetsstudiet. I tillegg har det vært nødvendig å inkludere tilgjengelig litteratur om Information security culture, som vi anså som svært relevant for vår problemsstilling.

Avhandlingen viser at rundt halvparten av operatørselskapene har tatt i bruk sikringskulturbegrepet, hvor organiseringen av sikringsarbeidet i virksomheten ikke synes å være avgjørende for hvorvidt begrepet benyttes eller ikke. Det fremgår en uenighet og begrepsforvirring i oppfatning av begrepene sikkerhet og sikring, noe som kan synes å ha betydning for om begrepet er tatt i bruk. Studien indikerer at de som benytter begrepet synes å ha et mer reflektert forhold til hva som legges i begrepet. Her vektlegges bevissthet, kompetanse, ansvarsfølelse og forståelse for

sikring, hvor kunnskapsdimensjonen må vektlegges. Sikringskultur omfatter dermed antagelser, holdninger, verdier, oppfatninger og atferd som kan ha betydning for sikringsnivået i virksomheten.
Med utgangspunkt i vårt teoretiske rammeverk, viser studien at forpliktelse, fleksibilitet, læring og tillit vektlegges i utvikling av en optimal sikringskultur. Studien belyser en rekke ulikheter og utfordringer knyttet til elementene som i ulik grad skiller seg fra sikkerhetskultur-feltet. Dette knyttes til at sikring har noe særegne karakteristika; at det er en trusselaktør som kan opptre internt og eksternt, det er høy grad av usikkerhet og ofte et fravær av intenderte uønskede hendelser. Et av hovedfunnene i studien er at begrenset informasjonsdeling og åpenhet utgjør en stor utfordring i forhold til muligheter for læring og forståelse for truslene virksomheten står ovenfor, samt å skape tillit, aksept og forståelse for sikringstiltak blant ansatte.

Studien viser enighet blant operatørselskapene om at kultur er viktig for å oppnå et høyt sikringsnivå. Likevel eksisterer det ulike syn på hvorvidt det er nødvendig med et eget sikringskulturbegrep. På engelsk skilles det mellom safety og security, hvor forskjellen ligger i intensjonsbegrepet. Dermed gir det også mening å snakke om henholdsvis safety culture og security culture. Problematisk blir det når man har oversatt safety culture, som dreier seg om uintenderte uønskede hendelser, til sikkerhetskultur og HMS kultur på norsk, hvor både safety og security inngår. Det argumenteres at dersom man ikke benytter sikringskulturbegrepet, kan dette medføre at sikringselementet blir glemt. Dette gjelder spesielt dersom virksomheten ikke har en klar begrepsavklaring av de norske begrepene, hvor man har tydelig definert sikringsbegrepet. I denne sammenheng forstås sikkerhetskultur og sikringskultur ikke som separate kulturer, men begrepene brukes konseptuelt for å omhandle de aspektene av organisasjonskulturen som har betydning for sikkerhets- og/eller sikringsnivået.

Studien konkluderer med at det er behov for en tydelig begrepsavklaring for å få frem de ulike karakteristikaene ved sikring og sørge for at disse samt relaterte utfordringer blir tatt hensyn til i kulturbyggingen. Ved å gjøre sikring til et eget kulturbegrep kan det tenkes at man i større grad tar hensyn til disse særegenhetene og hvordan kulturen kan bidra til enten å forsterke eller svekke sikringsnivået i virksomheten.

FORORD

Arbeidet med avhandlingen har både vært en krevende og lang prosess, men også en svært interessant og lærerik erfaring som vi ville ikke vært foruten. Vi startet prosjektet med lite kunnskap omkring sikring, grunnet at dette er et område som fått lite fokus på masterprogrammet i samfunnssikkert. Dette var også en av grunnen til at vi ønsket å utforske dette området nærmere og bidra med økt kunnskap og innsikt omkring et svært aktuelt tema.

Først og fremst vil vi takke vår veileder fra Universitetet i Stavanger, Sissel H. Jore, for gode innspill og konstruktive tilbakemeldinger gjennom hele prosessen. Vi vil også takke alle våre informanter som har bidratt med svært nyttig informasjon, samt vært veldig positive til forskningsprosjektet vårt. Avslutningsvis vil vi takke Joakim Barane og Ronald Barø ved Falcknutec for gode faglige innspill.

Stavanger, 15 juni 2015

Caroline Østensjø & Caroline Irwin Larsen

Figurer, tabeller og vedlegg

Terminologi

Begrep	Definisjon
Safety	*"Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter" (NOU, 2000)*
Security	*"Sikkerhet mot uønskede hendelser som er resultat av overlegg og planlegging" (NOU, 2000)*
Risiko	*"Uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value." (NOU, 2000)*
Sikkerhetskultur	*The product of individual and group values, attitudes, perceptions, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's health and safety management (ACSNI,1993 i Antonsen, 2009)*
Sikringsrisiko	*"Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen" (NS 5832, 2014)*
Sikringsnivå	*"Summen av menneskelige, organisatoriske og tekniske tiltak, utover grunnsikring som er ment til å iverksettes for en tidsbegrenset periode, eller for å møte en definert trussel." (Norsk Olje og Gass, 2003)*
Sikringstiltak	*"Tiltak for å redusere risiko forbundet med tilsiktede uønskede handlinger. Tiltakene kan grupperes i teknologiske, organisatoriske eller menneskelige tiltak." (Norsk Olje og Gass, 2003)*
Fysisk sikring	*"Tiltak som iverksettes for å oppdage, hindre eller forsinke inntrenger, inntil vakt eller politi ankommer stedet. Kan omfatte tekniske, organisatoriske eller personellmessige tiltak." (Norsk Olje og Gass, 2003)*
Personell sikring	*"Bruk av ID-kort, tilgangsautorisasjon og sikringsopplæring, foruten lederes, ansattes og innleides særlige plikter I sikringssammenheng." (Norsk Olje og Gass, 2003)*

Informasjonssikkerhet	*"Tiltak iverksatt for å sikre at informasjon ikke er tilgjengelig uten autorisasjon (konfidensialitet), at informasjon ikke uautorisert endres eller ødelegges (integritet), og at informasjon er tilstede og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres (tilgjengelighet).''(Den Norske Dataforening)*
Trusselbilde	*"Tidsavgrenset beskrivelse av identifiserte trusler mot en bestemt entitet." (Norske Olje og Gass, 2003)*
Trussel	*''Mulig uønsket handling som kan gi e negativ konsekvens for entitetets sikkerhet." (Norsk Olje og Gass, 2003)*
Verdi	*''Ressurs som hvis den blir utsatt for en uønsket påvirkning vil medføre en negativ konsekvens for den som forvalter eller drar fordel av ressursen." (NSM, 2014)*
Sårbarhet	*''Manglende evne til å motstå en uønsket hendelse eller opprette en ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning." (Norsk Olje og Gass, 2003)*

Innholdsfortegnelse

1.0 Innledning

1.1 Motivasjon for valg av tema

De siste årene har hendelser både i Norge og internasjonalt medført til et økt fokus på sikring og risiko for intenderte uønskede hendelser blant virksomheter i petroleumssektoren. Både terrorangrepene i Norge 22. juli 2011 og på Statoil sitt anlegg i In Amenas 2013, var hendelser som illustrerte et manglende fokus på sikring (Jore & Moen, 2015) samt en mangelfull kultur som støtter opp sikringen. Med sikring menes "*sikkerhet mot intenderte uønskede hendelser*" (NOU 2006). Til tross for at petroleumssektoren alltid har vært pålagt å beskytte seg mot intenderte handlinger, har disse hendelsene medført at temaet sikring har fått større oppmerksomhet i Norge den siste tiden (Ptil, 2013). Blant annet ble Petroleumstilsynet (Ptil) delegert myndighetsansvar for Petroleumsloven 9-3 *Beredskap mot bevisste anslag* i 2013 (Ptil, 2013). Denne endringen understreker viktigheten av at selskapene har kjennskap til dagens trusselbildet og tilrettelegger sitt sikringsarbeid for å imøtekomme dette.

Samtidig som risikostyring i forhold til intenderte uønskede hendelser har fått økt fokus i petroleumssektoren og samfunnet forøvrig, har også kulturens betydning for sikringsnivået blitt fremhevet i en rekke sammenhenger. Blant annet påpekes betydningen av organisasjonskulturen for å forebygge og håndtere intenderte uønskede hendelser i både *Rapporten fra 22.juli kommisjonen* (NOU 2012) og i Statoils granskningsrapport *Angrepet mot In Amenas* (Statoil, 2013). I sistnevnte ble det påpekt at Statoils helhetlige evne og kultur måtte forsterkes for å kunne respondere på sikringsrisiko knyttet til operasjoner i komplekse omgivelser (Statoil, 2013). Rapporten vektlegger en *security culture* hvor et sett med felles antagelser, holdninger, praksis og atferd er gjennomgripende og delt på tvers av lokasjoner, enheter og nivåer i organisasjonen. Her påpekes det et behov for en generell anerkjennelse at sikring er alle sitt ansvar (Statoil, 2013). Statoil har på bakgrunn av granskningsrapporten iverksatt en rekke initiativer, deriblant økt bemanning og kompetanse innenfor sikring (Lewis, 2015). I tillegg er mer oppmerksomhet rettet mot

bevisstgjøring i organisasjonen og holdningene til de ansatte i forhold til sikringsrisiko.

I forbindelse med utgivelsen av In Amenas rapporten blir det løftet frem en begrepsforvirring knyttet til sikkerhetsbegrepet (Helgesen & Taraldsen, 2013). Mens man på engelsk har klare forskjeller mellom begrepene safety og security, benyttes ofte sikkerhet som et overordnet begrep på norsk. Når kun sikkerhetsbegrepet benyttes kan det dermed oppstå uklarheter hvorvidt man snakker om safety eller security. Security culture kan på norsk oversettes til sikringskultur, men i den norske versjonen av rapporten blir dette omtalt som sikkerhetskultur. Det blir videre problematisert hvorvidt man kan bygge en kultur uten å ha en klar begrepsavklaring (Helgesen & Taraldsen, 2013). Likevel fremkommer det i rapporten at kulturen må forsterkes dersom virksomheten skal oppnå et forbedret sikringsnivå (Statoil, 2013).

Kulturens betydning for sikringsnivået kan ses i lys av behovet for å ta hensyn til de myke barrierene i organisasjonen, noe som er vanlig innenfor safetyfeltet hvor fokus er på "*sikkerhet mot uintenderte uønskede hendelser"* (NOU, 2006). Operatørselskaper i petroleumssektoren har god kjennskap og erfaring med utvikling av en sikkerhetskultur, noe de blant annet er pålagt gjennom lover og forskrifter. Sikkerhetskultur kan forstås som aspekter av organisasjonskulturen som påvirker sikkerheten i positiv eller negativ forstand (Nordby & Hansen, 2005). Innenfor securityfeltet derimot, er trenden at man i større grad vektlegger teknologiske sikringstiltak, der hensikten er å forhindre at eksterne aktører får tilgang til virksomhetens verdier (Falcknutec, 2015), noe som kan innebære at menneskefaktoren blir glemt (Thomson, Von Solms & Louw, 2006). Samtidig for å oppnå et høyt sikringsnivå i petroleumssektoren krever det at man ser de strukturelle og kulturelle aspektene i en sammenheng (Nordby & Hansen, 2005). På lik linje med safetyfeltet blir en helhetlig tilnærming til sikringsarbeidet helt sentralt, hvor en tar hensyn til de myke sikringshjelpemidlene, herunder en såkalt sikringskultur. Dette kan forstås som aspekter av organisasjonskulturen som kan påvirke sikringsnivået i positiv eller negativ forstand. En helhetlig tilnærming vil være spesielt viktig for å kunne imøtekomme blant annet den økte terrortrusselen i Norge og en vedvarende etterretningstrussel (NSM, 2015).

Sikring i petroleumssektoren er sentralt ved at sektoren utgjør en betydelig andel for norsk økonomi, og er viktig både med hensyn til verdiskapning og sysselsetting. Til tross for at petroleumssektoren ikke er utpekt som kritisk infrastruktur (Helgesen, 2013), påstår Relf og Stubblefield (2000) likevel at sektoren står ovenfor et bredt spekter av trusler, blant annet terrorisme og tap av eiendeler. Dette kan videre ramme verdier som mennesker, økonomi, miljø og virksomhetens omdømme. Videre stiller det krav til blant annet en høy grad av sikringsbevissthet i virksomheten (Relf & Stubblefield, 2000), noe som kan knyttes til de "myke" sikringshjelpemidlene.

Til tross for at kulturens betydning for sikringsnivået har blitt belyst i forbindelse med de overnevnte hendelsene, fremstår security culture, på norsk sikringskultur, som et relativt umodent begrep. Det fremgår likevel i litteraturen at sikringskultur anses som et viktig element i organisasjonens helhetlige risikostyring (Talbot & Jakeman, 2009). Tilgjengelig forskning omkring fenomenet synes å hovedsakelig være rettet mot informasjonssikring, hvor utvikling av en *information security culture* blir vektlagt for å oppnå et tilstrekkelig sikringsnivå i forhold til beskyttelse av informasjon (Ruighaver, Maynard & Chang, 2006). Utover dette viser likevel en nøye litteraturgjennomgang at forskning omkring sikringskultur både som begrep og som fenomen er svært begrenset.

1.2 Problemstilling

Basert på litteraturgjennomgangen fremstår det et behov for økt forståelse og innsikt omkring sikringskultur både som begrep og som fenomen. Et nært beslektet og langt mer utforsket begrep er sikkerhetskultur eller safety culture. Dette er noe petroleumssektoren har god kjennskap til og erfaring med. Blant annet er operatørselskaper i petroleumssektoren pålagt å kontinuerlig forbedre sin HMS kultur (Ptil, 2013) og kan dermed forventes å ha et forhold til kulturbegrepet. Det vil i den forbindelse være interessant å undersøke hvilket syn operatørselskapene i petroleumssektoren har på utvikling av en såkalt "optimal" sikringskultur, og basert på dette vurdere hvorvidt begrepet sikringskultur fremstår som hensiktsmessig i arbeidet med å utvikle en slik kultur.

På bakgrunn av dette har vi kommet frem til følgende problemsstilling:

> *Hva er operatørselskapene i petroleumssektoren sitt syn på utvikling av en optimal sikringskultur og hvorvidt fremstår begrepet sikringskultur som hensiktsmessig i arbeidet med å utvikle en slik kultur?*

Med "syn" menes operatørselskapenes oppfatninger, meninger, forståelser, tolkninger og synspunkt om begrepet og fenomenet sikringskultur. For å besvare problemstillingen må vi undersøke hvorvidt selskapene benytter seg av begrepet i sikringsarbeidet og hva de legger i begrepet. Videre må vi utforske hvilke elementer oppfattes som sentrale ved utvikling av en såkalt "optimal" sikringskultur og mulige tilhørende utfordringer som selskapene opplever. Med "optimal" mener vi en organisasjonskultur som bidrar positivt til sikringsnivået til virksomheten. På denne måten vil vi forsøke å få frem operatørselskapenes syn og tolkninger rundt arbeidet med å utvikle en slik kultur, og med tanke på at begrepet er relativt umodent, kunne si noe om hvorvidt begrepet fremstår som hensiktsmessig i arbeidet med å utvikle en sikringskultur.

1.3 Avgrensninger og presisering av problemstilling

Vi har valgt å avgrense avhandlingen til å undersøke petroleumssektoren, nærmere bestemt operatørselskaper. Et operatørselskap kan defineres slik: "*Selskap som har rett til å lete etter olje og gass i en blokk og bygge ut et felt for produksjon ved et kommersielt funn. Operatøren opptrer gjerne på vegne av et partnerskap av selskaper"* (Ptil, 2015). Årsaken til valg av operatørselskaper er at de har god kjennskap til begrepene sikkerhetskultur og HMS kultur, blant annet fordi dette er pålagt gjennom lover og krav (Ref. Rammeforskriften paragraf 15, Ptil, 2013). Bransjen har dermed i lengre tid gjennomført programmer rettet mot å utvikle virksomhetens sikkerhetskultur, og kunnskapsnivået på dette feltet gjenspeiles i tilgjengelig litteratur og forskning på området. Likevel har fokus tradisjonelt vært rettet mot uønskede hendelser som er et resultat av tilfeldigheter (NOU, 2006). Grunnet operatørselskapenes forhold til sikkerhetskulturbegrepet, samt økt fokus på sikring i bransjen, forventes det at selskapene kan bidra med å gi økt innsikt og forståelse omkring temaet sikringskultur. Uavhengig om virksomhetene benytter

begrepet, kan det tenkes at de i ulik grad arbeider med kulturbygging tilknyttet virksomhetens sikringsarbeid, og kan bidra med relevant kunnskap og informasjon.

Grunnet begrenset forskning om temaet samt at kultur er et krevende forskningsområde, inntar vi en ydmyk tilnærming til temaet. Med dette vil vi presiserer at vi er ikke ute etter å måle kulturen blant operatørselskapene, da vi ser at det er et behov for økt kunnskap om sikringskultur både som begrep og som fenomen. I avhandlingen er vi derfor ute etter å utforske aktørenes meninger, tolkninger og forståelser omkring det å utvikle en "optimal" sikringskultur, for deretter å kunne vurdere hvorvidt begrepet fremstår som hensiktsmessig i arbeidet med å utvikle en slik kultur.

På norsk er det vanlig å oversette begrepene *safety* og *security* til henholdsvis *sikkerhet* og *sikring.* De norske og engelske begrepene vil dermed bli brukt om hverandre i avhandlingen, hvor sikring blir brukt for det engelske begrepet security og dreier seg om beskyttelse mot intenderte uønskede hendelser som tyveri, sabotasje, spionasje, terrorisme og andre typer kriminelle handlinger. Vi har videre ikke avgrenset sikring til ett bestemt område, og sikring omfatter dermed alt fra fysisk sikring, personell sikring og informasjonssikring. Dette fordi sikringskultur kan ses som et aspekt av organisasjonskulturen som påvirker sikringsnivået i positiv eller negativ retning, og er dermed knyttet til alle aspekter ved sikring. Dermed kan sikringskultur ses som relevant uavhengig av hvilke typer tiltak operatørselskapene benytter eller hvilke sikringsområder de fokuserer på.

1.4 Oppbygning og struktur

Etterfulgt av innledningen vil vi i kapittel 2 presentere teoretiske perspektiver som anses som nødvendig for å kunne besvare problemstillingen på en tilstrekkelig måte. Deretter vil vi i kapittel 3 redegjør for vårt valg av metode som ble benyttet for å innsamle og analysere funn. I kapittel 4 presenteres funn fra intervjuene, som videre blir drøftet opp mot det teoretiske rammeverket i kapittel 5. Avslutningsvis redegjøres konklusjoner av studien og anbefalinger til videre forskning presenteres.

2.0 Teori

For å utforske operatørselskapenes syn omkring utvikling av en optimal sikringskultur og vurdere hvorvidt et slikt begrep fremstår som hensiktsmessig i arbeidet med å utvikle en slik kultur, vil vi i det følgende presentere en teoretisk ramme som vår analyse vil bygge på.

Temaet for oppgaven er fenomenet sikringskultur, som referer til det engelske begrepet *security culture*. Sikringskultur er et relativt nytt begrep som ikke har noe entydig definisjon og har i liten grad blitt forsket på (Malcolmson, 2009). Security culture og safety culture er nært beslektede begreper, hvor safety culture har vært gjenstand for mye forskning. Før vi går inn på teori knyttet til disse fenomenene, starter vi med en begrepsavklaring i forhold til hva som menes med begrepene safety og security samt en redegjørelse for vårt valg av oversettelse til norsk.

Etter begrepsavklaringen vil vi presentere en modell som demonstrerer viktigheten av å ta hensyn til de kulturelle aspektene i forhold til styring av sikringsrisiko i petroleumssektoren. Deretter vil vi kort gjennomgå kulturbegrepet og presentere relevant litteratur om organisasjonskultur. Dette er nødvendig ettersom både sikkerhetskultur og sikringskultur kan ses som aspekter av virksomhetens organisasjonskultur, som påvirker sikkerhets- eller sikringsnivået i positiv eller negativ retning. Vi vil i stor grad benytte forskning omkring sikkerhetskultur i avhandlingen. Dette henger sammen med at sikringskultur er et fremvoksende konsept og det er gjort lite forskning innen feltet, samtidig som det er flere likheter mellom sikring og sikkerhet (security og safety). Sikkerhetskultur er et omfattende fenomen og derfor vil vi avgrense teori til det som tenkes å kunne være anvendelig i en sikringskontekst og nødvendig for å besvare vår problemsstilling. Deretter vil vi beskrive tilgjengelig litteratur om fenomenet sikringskultur. Til tross for at det er gjort begrenset forskning om fenomenet, finnes det en del litteratur om "Information Security Culture." Dette vil sammen med teori om sikkerhetskultur i stor grad danne vårt teoretiske rammeverk. Avslutningsvis, vil vi basert på gjennomgått teori oppsummer hva sikringskultur er, og hva som kan forventes å være elementer ved en optimal sikringskultur.

2.1 Safety og security

2.1.1 Begrepsavklaring

I litteraturen skilles det ofte mellom de engelske begrepene safety og security. Ettersom det er ingen entydig oversettelse av disse til norsk, vil vi først gjennomgå hvordan de engelske begrepene defineres, før vi redegjør for vårt valg av oversettelse til norsk.

Piètre- Cambacèdes og Chaudet (2010) viser til viktigheten av å redusere tvetydigheten mellom begrepene safety og security, hvor det understrekes at betydningen av de engelske begrepene er uklar og overlappende. Hvilken betydning begrepene har varierer ut ifra hvilken kontekst de benyttes i, noe som kan medføre potensielle tvetydigheter, feiltolkninger og misforståelser når personer fra ulike tekniske miljøer samhandler. De påpeker dermed at det er spesielt viktig å skape forståelse og klarhet i begrepene i beskyttelse av kritisk infrastruktur som involverer en rekke aktører (Piètre - Cambacèdes & Chaudet 2010).

Albrechtsen (2003) har foretatt en begrepsavklaring av safety og security og hevder at begge begrepene fokuserer på et ønske om å beskytte verdier mot mulige farer/trusler og etablere sikre forhold. Safety innebærer at en er beskyttet mot farer, mens security handler om å være utenfor fare. Til tross for likheter, blir flere ulikheter belyst i litteratur og forskning. Blant annet påpeker Piètre - Cambacèdes & Chaudet (2010) to viktige forskjeller mellom safety og security. Den første dreier seg om intensjonsbegrepet; om handlingene er intenderte eller uintenderte. Her knyttes *security* til intenderte handlinger som har et formål om å forårsake skade, mens *safety* knyttes til uønskede hendelser som er tilfeldige og ikke-intenderte. Den andre forskjellen ligger i forholdet mellom systemet og omgivelsene og hvor risikoen stammer fra. Securitytrusler kommer fra omgivelsene og har potensialet til å påvirke systemet, mens safety-relaterte hendelser skapes i selve systemet og har potensiale til å påvirke omgivelsene (Piètre- Cambacèdes & Chaudet, 2010).

I likhet med Piètre - Cambacèdes & Chaudet (2010), hevder Reniers, Cremer og Buytaert (2011) at et sentralt skille mellom security og safety ligger i intensjonsbegrepet. Security knyttes til intenderte handlinger, noe som innebærer at en aggressor er tilstede som påvirkes av det fysiske miljøet og personlige faktorer.

Aggressoren kan både opptre internt i organisasjon, men også eksternt, hvor det påpekes at dette bør inkluderes i virksomhetens security vurderinger. Et annet viktig skille mellom safety og security er i forhold til hvilken proaktiv tilnærming virksomheter anvender for å identifisere farer og trusler. I sikkerhetsvurderinger eller risikoanalyser benyttes i stor grad kvantitative metoder, hvor en beregner risiko ved hjelp av sannsynlighet og konsekvens. I security vurderinger, eller såkalte trusselvurderinger, anses bruken av sannsynlighet som mindre egnet, og trusler er identifisert og analysert ved hjelp av konsekvenser, sårbarheter og målets attraksjon (Reniers et al., 2011). Samtidig som det påpekes ulikheter i tilnærminger, fremheves det at håndtering av konsekvenser av hendelser behandles likt i safety og security, uavhengig om hendelsen er intendert eller tilfeldig. Her vises det til en brannhendelse som eksempel. Likevel påpeker forfatterne viktigheten av å ta hensyn til at en trusselaktør vil bevisst søke de beste strategiene for å nå sitt mål om å forårsake skade. Videre nevnes det at det kan oppstå konflikter mellom sikkerhetstiltak og sikringstiltak, hvor i enkelte tilfeller kan sikkerhetstiltak påvirke sikringen negativt (Reniers et al., 2011).

Reniers et al. (2011) viser til en tabell som oppsummerer noen av de ovennevnte ulikhetene mellom safety og security:

Safety	Security
The nature of an incident is an inherent risk	The nature of an incident is caused by a human act
Non – intentional	Intentional
No Human aggressor	Human aggressor
Quantitative probabilities and frequencies of safety-related risks is available	In case of less common security risks (e.g terrorism), only qualitative (expert – opinion based), likelihood of security-related risks may be available
Risks are of rational nature	Threats may be of symbolic nature

Tabell 1: *Non-exhaustive list of differences between safety and security.*

Albrechtsen (2003) hevder at usikkerhetsdimensjonen er større innen securityfeltet sammenlignet med safetyfeltet. Denne usikkerheten omkring trusler og konsekvenser kommer som følge av; at de eksterne truslene er vanskelig å forutse og kontrollere, man står ovenfor et bredt spekter av trusler, trusler kan være fjerne og uobserverbare, og det er liten grad av kunnskap omkring innside trusler.

På norsk benyttes sikkerhet ofte som et overordnet begrep for både safety og security. Sikkerhet er et bredt begrep som kan ha ulike betydninger avhengig av hvilken kontekst det brukes i (Aven, Boyesen, Olsen & Sandved, 2004). Ifølge Aven et al. (2004), kan sikkerhet defineres som følgende:

> *Forebyggende tiltak der hensikten er å redusere sannsynligheten for at noe uønsket skal skje eller redusere konsekvensene ved uønskede hendelser.* (Aven et al., 2004, s. 17).

På lik linje fremkommer det i NOU (2006) at safety og security ofte benyttes som hjelpeord for å illustrere to aspekter ved sikkerhet. Safety referer til sikkerhet mot uønskede hendelser som er tilfeldige av natur, eksempelvis gasslekkasjer, løfteulykker osv. Derimot refererer security til sikkerhet mot uønskede hendelser som er et resultat av overlegg, for eksempel tyveri, sabotasje og terrorangrep (NOU, 2006). Videre påpekes det at det ikke eksisterer noen leksikal distinksjon mellom de to typene uønskede hendelser på norsk. Bruk av tilsvarende ord på norsk kan derimot stipuleres når det oppstår et faglig behov for det (NOU, 2006).

På bakgrunn av ulikhetene mellom *safety* og *security* har vi valgt å oversette begrepene til henholdsvis *sikkerhet* og *sikring* gjennom avhandlingen, noe som også er vanlig i norsk praksis (NOU, 2006). Vi vil dermed benytte de norske begrepene med samme betydning som de engelske. Vi mener dette skaper klarhet og konsistens både i forhold til bruk og hva som legges i begrepene, hvor skillet knyttes som nevnt ovenfor til intensjonsbegrepet. Videre tydeliggjør dette skillet mellom *sikkerhetskultur* og *sikringskultur*. Likevel kan det tenkes at operatørselskapene kan ha ulike forståelser av begrepene og ikke nødvendigvis skiller mellom sikkerhet og sikring slik som beskrevet ovenfor. Dette er noe vi tar hensyn til i vår metode, for å unngå misforståelser. Gjennom avhandlingen vil dermed sikkerhetskultur referere til

safety culture, og sikringskultur referere til security culture, hvor den engelske betydningen er ivaretatt. Ettersom store deler av litteraturen vi benytter bruker de engelske begrepene, innebærer en slik oversettelse at vi beholder begrepenes betydning uavhengig av språkbruk.

2.1.2 Organisatoriske motsetninger mellom security og safety

Forskning innen luftfart har fremhevet utfordringer og ulikheter mellom hvordan safety og security er organisert i luftfartsindustrien (Pettersen & Bjørnskau, 2014). Blant annet påpekes at både formål og den institusjonelle logikken til beskyttelse er forskjellig. Safety-ulykker er ofte til dels karakterisert av systemet, og utgjør en del av den erfaringsbaserte læringen i industrien. Security-risiko er derimot generelt relatert til potensielle ukjente eksterne aktører som kan gjennomføre tilfeldige angrep basert på sitt formål om å utøve terror. Dermed kan man si at safety er organisert for å håndtere interne trusler, mens security er hovedsakelig rettet mot eksterne trusler. Tiltak og atferd i organisasjonen vil dermed være relatert til trusselens natur og formålet med beskyttelsen. I en safety kontekst er truslene interne og dermed relativt kjente, noe som muliggjør en vurdering av hvor egnet sikkerhetstiltakene er. Derimot opptrer security hendelser sjeldent og det er derfor vanskelig å evaluere tiltakenes effektivitet (Pettersen & Bjørnskau, 2014).

Ifølge Pettersen og Bjørnskau (2014) krever safetyfeltet et sosialt klima som er preget av tillit for at systemet skal fungere effektivt. Tillit forstås her som et sett av holdninger og forventninger om andre mennesker og det organisatoriske systemet som de er en del av. Man må stole på at aktørene har utført sine oppgaver på en tilstrekkelig måte og i henhold til gjeldende normer og standarder (Pettersen & Bjørnskau, 2014). Innen security derimot er det sosiale klimaet preget av mistenksomhet. I forskningen kommer det blant annet frem at security reguleringer hindrer muligheten for utveksling av informasjon og kommunikasjon som kan være relatert til flysikkerheten. I tillegg at security reglene oppfattes som ulogiske, urettferdige og basert på mistillit. Til tross for at forskningen er fra luftfartsindustrien, påpekes det at funnene også kan være relevante for andre kritiske infrastrukturer (Pettersen & Bjørnskau, 2014).

2.2 Harde og myke sikkerhetshjelpemidler

Tradisjonelt innenfor sikkerhetsarbeidet har det i stor grad blitt benyttet såkalte "harde og strukturelle" sikkerhetshjelpemidler, som teknologiske løsninger, lover, prosedyrer og regelverk (Nordby & Hansen, 2005). I de senere årene har virksomheter i større grad også begynt å se på de myke sikkerhetshjelpemidler, som omfatter holdninger, kunnskap, sikkerhetsatferd og sikkerhetskultur. Sistnevnte forstås som aspekter ved organisasjonskulturen som påvirker sikkerheten i en eller annen retning. Nordby og Hansen (2005) understreker at for å oppnå et godt sikkerhetsarbeid, må man både se de "harde" og "myke" sikkerhetshjelpemidlene i en sammenheng. Dette samspillet illustreres i følgende modell:

Figur 1: Komplementære prinsipper i et harmonisk sikkerhetsarbeid (Kufås & Mølmann (2003) i Nordby og Hansen (2005))

I forhold til vår problemstilling anser vi modellen som anvendbar også i en sikringskontekst, hvor sikringskultur kan anses som et mykt sikringshjelpemiddel. Forfatterne understreker at et harmonisk sikkerhetsarbeid krever at man inkluderer både de "myke" og "harde" sikkerhetsvirkemidlene, og at sikkerhetsnivået bestemmes av et flertall av virkemidler og egenskaper, samt interaksjonen mellom disse. Hvordan virksomheten organiserer sitt sikkerhetsarbeid påvirkes videre av en rekke andre forhold, blant annet konteksten virksomheten opererer i, produktivitet og økonomiske forhold. Dermed påpekes det at det er viktig å inneha en forståelse for hvilke forhold

som spiller inn på sikkerhetsarbeidet (Nordby & Hansen, 2005). I forhold til vår problemsstilling, retter vi fokuset mot de myke sikringshjelpemidlene, herunder sikringskultur. Samtidig vil det også være viktig å se dette i samspill med de strukturelle hjelpemidlene, da styring av sikringsrisiko krever en holistisk tilnærming på lik linje som innenfor sikkerhetsarbeidet.

2.3 Organisasjonskultur

Det finnes ingen bestemt og universell forståelse av begrepet kultur, og det rådes lite enighet både innen og på tvers av ulike disipliner. I litteraturen eksisterer det en rekke ulike definisjoner, likevel er det noen felles tråder som går igjen. Innen sosiologien refererer kulturbegrepet som regel til de verdier som medlemmene i en gruppe deler, normene som de følger og de materielle objektene de lager (Giddens, 1994 i Antonsen, 2009).

På lik linje som kultur er organisasjonskultur mye omtalt og det fremkommer ingen entydig definisjon. Begrepet organisasjonskultur ble først tatt i bruk på 1980 tallet, hvor en sterk kultur ble ansett som nøkkelen til bedriftens ytelsesevne, og det ble lagt vekt på ledelsesengasjement og etablering av felles mål og verdier (Haukelid, 2001). I litteraturen er det derimot stor debatt omkring hvorvidt kultur er noe som kan styres og kontrolleres (Haukelid, 2001). Innen forskning har organisasjonskultur blitt adressert ut ifra både et antropologisk, sosiologisk og psykologisk perspektiv, og det finnes en rekke definisjoner av organisasjonskultur.

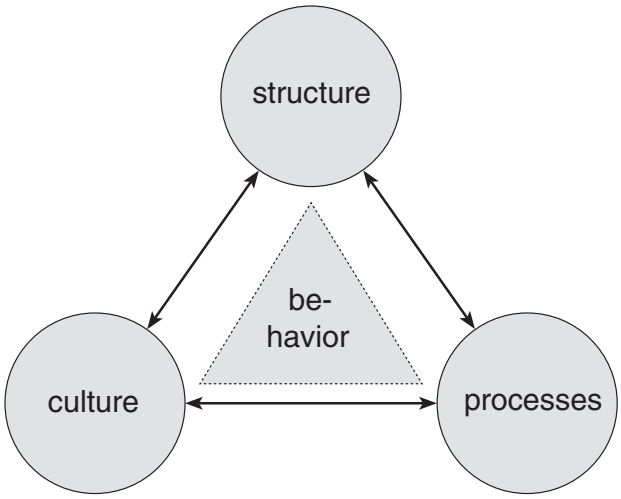
Edgard Schein (2010) fremhever at organisasjonskultur er mer enn kun det ytre synlige lag og definerer organisasjonskultur slik:

> "*A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems". (Schein, 2010, s. 18)*

Thicke og Beyer (1993, i Bang, 2013, s. 329) definerer organisasjonskultur som et system av ideer, symboler og meninger som binder sammen kulturen, mens en annen

utbredt definisjon er "*The way we do things around here.*" (Deal & Kennedy, 1982, i Bang, 2013, s. 237).

Guldenmund (2000) påpeker at det ikke kun er organisasjonskulturen som påvirker hvordan en organisasjon presterer, men at organisasjonens strukturer og prosesser også er medvirkende faktorer. Uttal (1983, i Reason, 1997) beskriver kultur som delte verdier og antagelser som samspiller med organisasjonens strukturer og systemer for å skape atferdsmessige normer. På samme måte hevder Antonsen (2009) at kultur ikke kan studeres separat fra strukturer og interaksjoner, da disse er sammenvevde og påvirker hverandre. Igjen blir det viktig å se de kulturelle og strukturelle aspektene i en sammenheng. Dette kan illustreres ved hjelp av Guldenmunds (2010) modell:



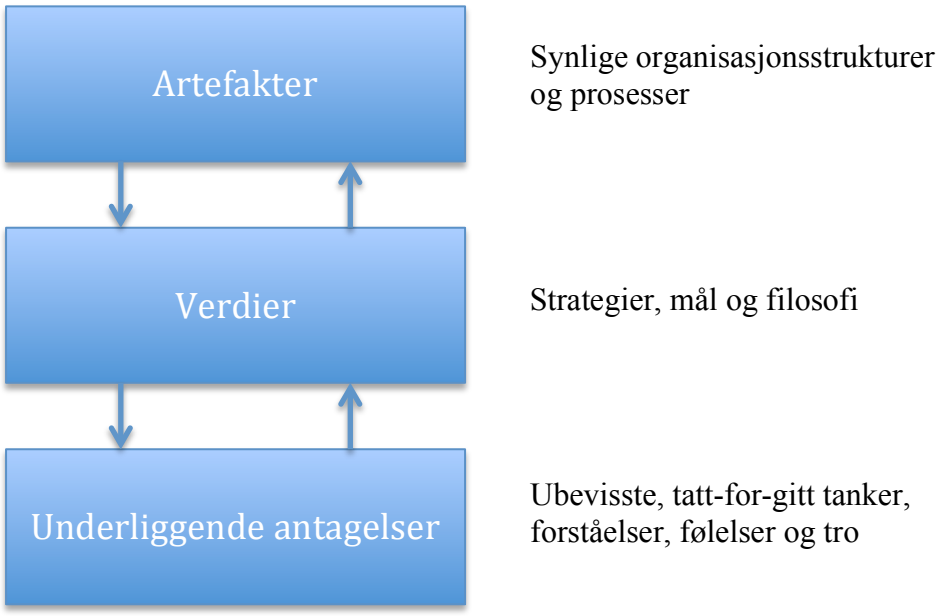
Figur 2: The organizational triangle (Guldenmund, 2010).

Bang (2013) har forsøkt å inkorporere kjerneelementene som går igjen i de ulike definisjonene i litteraturen og presenterer følgende definisjon:

> *Organisasjonskultur er de sett av felles normer, verdier og virkelighetsoppfatninger som utvikles i en organisasjon når medlemmene samhandler med hverandre og omgivelsene, og som kommer til uttrykk i medlemmenes handlinger og holdninger på jobben.* (Bang, 2013, s. 327)

2.3.1 Nivåer av organisasjonskultur

Ifølge Schein (1984) er det nyttig å forstå kultur, fordi kultur er et sett med latente og ubevisste krefter som er med på å bestemme individuell og kollektiv atferd, fortolkninger, tankemønstre og verdier. Han skiller mellom tre ulike nivåer av kultur, hvorav de øverste nivåene er mer tilgjengelige og synlige, mens de dypere nivåene er vanskeligere å observere og dermed vurdere.



Figur 3: Scheins tre nivåer av organisasjonskultur (Schein, 2010)

Artefakter

På toppnivået i modellen representeres de observerbare artefaktene, som kan ses på som en overflate manifestasjon av organisasjonskulturen (Nordby & Hansen, 2005). Dette omfatter blant annet det fysiske miljøet i organisasjonen, dens arkitektur, teknologi, språk, samt atferdsmønstre og offentlig dokumentasjon (Schein, 2010). Ut ifra artefaktene kan man beskrive ”hvordan” en gruppe konstruerer sitt miljø og ”hvilke” atferdsmønstre som er synlige blant medlemmene. Likevel er det vanskelig å forstå den underliggende logikken – hvorfor en gruppe oppfører seg slik som den gjør. For å kunne svare på dette spørsmålet må man identifisere hvilke verdier og normer som styrer atferden, som utgjør det andre nivået i modellen (Schein, 2010).

Uttrykte verdier

Uttrykte verdier og normer er uskrevne regler og prinsipper som er utviklet og fremmet av organisasjonens ledelse, og sier noe om hvilken atferd som anses som akseptabel og hva medlemmene anser som viktig (Bang, 2013). Disse manifesteres ofte i organisasjonens mål, filosofi og strategier (Nordby & Hansen, 2005) De uttrykte verdiene reflekterer imidlertid hvordan man ønsker å fremstå, og det er dermed ikke sagt at de ansatte handler i henhold til disse (Bang, 2013)

Grunnleggende antagelser

For å virkelig forstå organisasjonskultur og kunne fastslå helheten av gruppens verdier og åpenbare atferd, er det avgjørende at man fordyper seg i de underliggende grunnleggende antagelsene (Schein, 2010). Disse "tatt for gitt" antagelsene er ofte ubevisste og utgjør selve kjernen i organisasjonskulturen ved at de er avgjørende for medlemmers atferd, holdninger og oppfatninger. Ved å analysere de grunnleggende antagelsene, vil man enklere kunne tyde de observerbare handlingene som organisasjonskulturen gir uttrykk for, og dermed kunne forstå helheten av organisasjonens verdier og atferd (Schein, 2010).

Kjernen i kulturbegrepet er noe som er felles og deles i gruppen, det vil si at det ofte legges vekt på kultur som noe harmonisk og enhetlig. Likevel tyder mye av forskningen på at organisasjoner ikke utvikler en enhetlig organisasjonskultur, men at flere subkulturer kan utvikle seg (Richter & Koch, 2004). Innenfor subkulturen vil medlemmene handle på basis av verdier, normer og virkelighetsoppfatninger som har utviklet seg innenfor gruppen (Bang, 1995). Bang (1995) hevder at organisasjonens medlemmer kan tilhøre flere subkulturer samtidig. Videre blir det fremhevet at subkulturer ikke nødvendigvis følger de sosiale strukturene i organisasjonen, men kan gå på tvers av profesjoner, yrker og avdelinger (Richter & Koch, 2004).

2.3.2 Tilnærminger til kulturbegrepet

Det er store variasjoner og uenigheter blant kulturforskere i forhold til hva kultur er og hvordan det bør studeres. Slike uenigheter knytter seg ofte til spørsmålet om kultur er noe en organisasjon *har* eller *er*.

En funksjonell tilnærming til organisasjonskultur ser på kultur som noe en organisasjon *har*, det vil si som en variabel eller komponent (Antonsen, 2009). Tilnærmingen er "top-down" ved at det antas at kultur kan endres gjennom ledelsens intervensjoner for å tjene organisasjonens interesser (Glendon & Stanton, 2000). Fokuset er på å finne ut hvordan man kan forme den interne kulturen på bestemte måter og hvordan man kan endre kulturen i tråd med ledelsesmessige formål (Smirchich, 1983). Det argumenteres at organisasjoner med kulturer som støtter opp dens strategier vil trolig være mer vellykkede (Smirchich, 1983). Forfatteren Edgard Schein blir ofte plassert innenfor denne tilnærmingen da fokus er på å identifisere de underliggende antagelsene som påvirker atferden i organisasjonen, for deretter å kunne påvirke kulturen i organisasjonen (Nordby & Hansen, 2005).

En fortolkende tilnærming ser på kultur som noe organisasjonen *er* og representerer en "bottom - up" tilnærming (Glendon & Stanton, 2000). Dette betyr at organisasjonskulturen ikke "eies" av en bestemt gruppe, men skapes og gjenskapes gjennom interaksjonene mellom medlemmene i organisasjonen (Richter & Koch, 2004). Fokuset er på hvordan medlemmer av en kultur oppfatter deres verden og hvordan de fortolker og forstår deres opplevelser (Antonsen, 2009). Målet er å beskrive og tolke kulturen, heller enn å endre den (Nordby & Hansen, 2005). Tilnærmingen kritiserer den funksjonelle tilnærmingen for sitt optimistiske syn på muligheten for kulturell endring (Antonsen, 2009).

De to ovennevnte tilnærmingene representerer to ytterpunkter og det er få som har en ren fortolkende eller funksjonell tilnærming (Antonsen, 2009). Ved at vår problemsstilling omhandler utvikling av en "optimal" sikringskultur blant operatørselskaper vil dette medføre at vi inntar en tildels funksjonell tilnærming til kultur. Dette fordi tanken om en "optimal" sikringskultur er basert på antagelsen om at kulturen kan påvirke sikringsnivået positivt eller negativt og at ved å identifisere kjennetegn ved en slik kultur kan en forsøke å påvirke kulturen i "ønskelig" retning. En slik tilnærming har videre lagt føringer for vårt valg av teori i avhandlingen.

2.4 Sikkerhetskultur

2.4.1 Bakgrunn for konseptet

Sikkerhetskultur-begrepet har vokst frem på bakgrunn av Chernobyl-ulykken i 1986 (Guldenmund, 2010) og har i ettertid blitt implisert i en rekke storulykker (Antonsen, 2009). Samtidig som det har vært en økt interesse for sikkerhetskultur konseptet, er det fortsatt mye forvirring rundt hva konseptet egentlig betyr. Slik som i litteraturen om organisasjonskultur, finnes det ingen entydig definisjon av begrepet eller enighet om hvordan det bør studeres.

2.4.2 Hva er sikkerhetskultur?

I følge Antonsen (2009) kommer den mest siterte definisjonen av sikkerhetskultur fra kjernekraftindustrien, hvor sikkerhetskultur blir definert som:

> *The product of individual and group values, attitudes, perceptions, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's health and safety management. Organisations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures (*ACSNI, 1993 i Antonsen, 2009, s.16).

Sikkerhetskultur omhandler en kollektiv forståelse for hva som er farlig, samt hvordan man kan bidra til å redusere disse farene (Aven et al., 2004) Det fremheves i litteraturen at sikkerhetskulturen kan ha betydning for om medlemmer i organisasjonen velger snarveier og lettvinte løsninger på bekostning av sikkerheten, grunnet økonomiske og tidsmessige hensyn (Aven et al., 2004).

Det finnes en rekke forståelser av hva sikkerhetskultur er. Et fellestrekk er at det er noe som er kollektivt og delt av flere individer, og som over tid har blitt manifestet i organisasjonen (Nordby & Hansen, 2005). Dermed påpekes det at sikkerhetskultur er noe mer enn summen av holdninger. Uavhengig av hvordan sikkerhetskultur er definert, er det stor enighet om at en god eller dårlig sikkerhetskultur vil virke inn på sikkerhetsnivået (Nordby & Hansen, 2005).

Det er flere teoretikere som velger å ikke skille mellom sikkerhetskultur og organisasjonskultur. På lik måte anser vi ikke sikkerhetskultur som en enhet eller noe separat fra organisasjonskultur, men heller som en integrert del av denne. Begrepet sikkerhetskultur benyttes dermed konseptuelt for å omhandle de aspektene av organisasjonskulturen, herunder verdier, oppfatninger, holdninger og atferdsmønstre, som kan påvirke sikkerhetsnivået til organisasjonen enten positivt eller negativt (Antonsen, 2009). Dette fordi de underliggende antagelsene vil gjennomsyre hele organisasjonen inkludert aspekter knyttet til sikkerhet (Guldenmund, 2000). Dette er videre i tråd med Schein (1984) sin definisjon og kulturmodell som beskrevet ovenfor. En slik forståelse av sikkerhetskultur medfører at det er noe alle organisasjoner har, men at den kan være mer eller mindre "optimal" i forhold til om den bidrar til å forbedre sikkerheten eller ikke. Dermed blir det også relevant å snakke om hva som kjennetegner en "optimal" sikkerhetskultur.

I litteraturen skilles det ofte mellom sikkerhetskultur og sikkerhetsklima. Det har vært stor debatt angående definisjon og differensiering av begrepene, og ofte brukes de om hverandre. Sikkerhetsklima anses ofte som et mer overfladisk konsept enn sikkerhetskultur, som en overflatemanifestering av kulturen (Flin, 2007), mens kultur referer normalt til meninger og antagelser som er dypere rotfestet og ofte tatt for gitt (Antonsen, 2009). Til tross for at sikkerhetsklima og sikkerhetskultur kan benyttes for å referere til ulike nivåer av kultur, velger vi å benytte oss av begrepene sikkerhetskultur og sikringskultur konsekvent gjennom oppgaven. Begrepene omfatter dermed alle tre nivåer i Schein sin kulturmodell, fra de mer observerbare artefaktene til de underliggende antagelsene.

2.4.3 Ledelse og sikkerhetskultur

I dag er det få forskere som er under den oppfatning at kultur er noe som kan endres ut ifra ledelsens ønske (Antonsen, 2009). Likevel er det flere som påpeker at ledere har en viktig rolle i forhold til utvikling av en sikkerhetskultur (Reason 1997, Flin, 2007, Zohar, 2010 , Haukelid, 2001 & Dejoy, 2005). Reason (1997) vektlegger blant annet lederes makt til å endre kultur ved å introdusere nye tiltak og praksiser. Selv om det erkjennes at det er vanskelig å endre verdiene til mennesker, hevder han at kollektive praksiser kan påvirkes på mer eller mindre forutsigbare måter ved å endre på organisasjonens strukturer og systemer (Reason, 1997). Dette kan ses i

sammenheng med at kultur og struktur er sammenvevde og påvirker hverandre. Dermed hevdes det at en optimal sikkerhetskultur kan til en viss grad bli "socially engineered" ved å identifisere og skape de nødvendige komponentene, og deretter sette disse sammen til en helhet (Reason, 1997).

Reason (1997) er et eksempel på hvordan fokus ofte er rettet på det øverste nivået i Schein (2010) sin modell, på det som er synlig og tilgjengelig. Når man skal målrettet endre sikkerhetskulturen kan man "forskyve" dette øverste nivået ved å endre rutiner og innføre nye retningslinjer og prosedyrer (Nordby & Hansen, 2005). Det er derimot svært vanskelig å endre medlemmenes holdninger og grunnleggende verdier. På lik linje hevder Haukelid (2001) at endringer i manifeste uttrykk (observerbare artefakter) er ingen garanti for at normer, verdier og grunnleggende antakelser har endret seg i organisasjonen. Selv om man klarer å endre på rutiner og atferd vil de grunnleggende antagelsene motsette seg endringen og henge igjen. Disse vil kun endres når atferdsmønstrene blir tatt for gitt som riktig av organisasjonens medlemmer, noe som gjør at kulturendring er en tidkrevende og langvarig prosess (Nordby & Hansen, 2005). Det krever derfor kontinuerlig fokus og ledelsesengasjement for å oppnå en varig endring av sikkerhetskulturen.

Ifølge Schein (1987) er kultur og lederskap sammenvevde. Han argumenterer blant annet at ledere og spesielt gründere er de viktigste kulturskaperne i en organisasjon, samt at dersom elementer ved kulturen er dysfunksjonell, kan og *bør* ledelsen gjøre noe for å endre kulturen. Ledere har dermed en evne til å drive kulturendring, men dette krever en forståelse for den kulturen som skal endres. Organisasjonskulturen blir påvirket gjennom hva ledelsen retter oppmerksomhet mot, måler og kontrollerer i organisasjonen (Schein, 1987). Det er dermed viktig med klar og tydelig ledelse, hvor systematikk og konsekventhet vektlegges, slik at de ansatte følger etter. Ledere anses som rollemodeller og hvordan de opptrer vil kommunisere antagelser og verdier til resten av organisasjonen, noe som kan bevisst brukes for å utvikle en god sikkerhetskultur (Schein, 1987). Zohar (2003) vektlegger også hvordan ledelsen og overordnede sender signaler til ansatte, som videre påvirker de ansattes atferd og dermed sikkerhetsrelaterte utfall. Det påpekes at ledere ubevisst kan sende signaler som forsterker en produksjonskultur når de egentlig verdsetter sikkerhet, men ikke

evner å uttrykke dette (Flin, 2007). Dermed blir både oppfatninger av ledelsens og overordnedes forpliktelse til sikkerhet sentralt i forhold til sikkerhetskultur.

Dejoy (2005) skiller mellom en atferdsbasert og en kulturbasert tilnærming til kulturendring. Førstnevnte fokuserer på å identifisere og modifisere kritisk sikkerhetsatferd, noe som over tid kan føre til skift i sikkerhetskulturen. På lik linje hevder Rossnes (2001, i Nordby & Hansen, 2005) at en vedvarende endring av atferdsmønstre og interaksjonsmønstre kan føre til kulturendring. En kulturbasert tilnærming vektlegger derimot viktigheten av organisasjonens sikkerhetskultur og hvordan denne former sikkerhetsatferd som legger føringer for effektiviteten av forskjellige sikkerhetsprogrammer (Dejoy, 2005). I motsetning til en atferdsbasert tilnærming, er kultur tilnærmingen mer "top- down" styrt. Fokuset er å forstå og ofte endre fundamentale verdier og antakelser i virksomheten, noe som medfører at ledelsen har en sentral rolle (Dejoy, 2005). Tilnærmingen vektlegger viktigheten av synlig ledelse, samt ledelsens motivasjon og engasjement i forhold til å demonstrere viktigheten av sikkerhet. Her vil man gjøre endringer på ledelsesnivå med forventninger om at disse skal "sildre" ned i organisasjonen. Videre påpekes det at dersom man skal oppnå varige forbedringer må man forstå kulturen i organisasjonen, noe som krever kvalitative tilnærminger (Dejoy, 2005).

Haukelid (2001) advarer mot å ha en overdreven tro på hva ledere kan oppnå, og påpeker at til tross for at ledelse er viktig, betyr ikke ledelse *alt***.** Flere studier demonstrerer at kultur er ikke noe som kan styres eller kontrolleres, men at det til en viss grad kan påvirkes (Haukelid, 2001). Eksempelvis nevnes det at organisasjoner kan bestå av flere subkulturer, og at de i den skarpe enden kan bevisst motstride ledelsens mål og verdier. I forhold til utvikling av en god sikkerhetskultur, kan man derimot gå meget langt i forhold til påvirkning og ulike tiltak, men det er viktig å være klar over at det er en grense (Haukelid, 2001). Dersom ansatte ikke finner tiltakene meningsfulle kan de bevisst "sabotere" dem, noe sikkerhetseksperter ofte overser. Videre vektlegges det at endringsprosessen må skje gjennom samarbeid og dialog preget av gjensidig tillit mellom ledelsen og ansatte, heller enn forsøk på å presse verdier og mål over hodet til ansatte (Haukelid, 2001).

2.4.4 High-Reliability Teorien og sikkerhetskultur

Mye av litteraturen om sikkerhetskultur baserer seg på forskning om såkalte High Reliability Organisations (HRO). Disse kjennetegnes av høy interaktiv kompleksitet og tette koblinger, og hvor feil og svikt kan ha langtrekkende og potensielt katastrofale konsekvenser (Lekka, 2011). Til tross for dette opplever de få ulykker. Teorien argumenterer at gjennom riktig organisasjonsdesign kan man kompensere for menneskelige feilhandlinger og svakheter og på denne måten oppnå pålitelige systemer. De har dermed et optimistisk syn på styring av sikkerhet og hevder at ulykker i høyteknologiske systemer kan forebygges (Aven et al., 2004). HRO-teorien vektlegger at høyt pålitelige organisasjoner vil kontinuerlig forberede seg på fremtidige overraskelser og situasjoner som kan utfordre deres nåværende antagelser om risikoforhold (Dekker & Woods, 2010). HRO anser ikke tidligere suksess som en garanti for suksess i fremtiden. Det forventes at feil vil inntreffe, og dermed opplæres ansatte i å oppdage og korrigere disse (Reason, 2000). Summert har HRO en evne til å innsamle, analysere og sammenfatte informasjon om "the bigger picture" av nåværende operasjoner på en slik måte som gjør dem i stand til å begrense og forebygge potensielle fremtidige feil (Lekka, 2011).

En av faktorene som vektlegges for å skape en høyt pålitelig organisasjon er utviklingen av en sikkerhetskultur (Dekker & Woods, 2010). En måte å konseptualisere måten kultur kan påvirke sikkerheten på er Weick et al. (1999) sitt konsept om "collective mindfulness", som kan forstås som et kollektivt oppmerksomhetsfokus (Antonsen, 2009). HRO klarer å håndtere det uventede på en vellykket måte på grunn av deres målrettede innsats til å handle på en "mindful" måte, noe som innebærer en økt årvåkenhet i forhold til risiko på tvers av organisasjonen og dens medlemmer (Jeffcott et al., 2006). HRO kjennetegnes både av evnen til å forutse feil og svikt, samt gjenopprette normaltilstand etter feil har inntruffet (Weick et al., 1999). Her vises det til at medlemmer av HRO innehar en kombinasjon av stabile kognitive prosesser som muliggjør oppdagelse av uventede hendelser, samt variasjoner i aktivitetsmønstre som gjør en i stand til å håndtere disse. Det har blitt identifisert fem prosesser som til sammen skaper såkalt "collective mindfulness"; *preoccupation with failure*, *reluctance to simplify interpretations, sensitivity to operations, commitment to resilience*, og *deference to expertise* (Weick et al., 1999). Disse inngår i stor grad i elementer ved en optimal sikkerhetskultur beskrevet under.

2.4.5 Elementer ved en optimal sikkerhetskultur

Flere forskere benytter en funksjonell tilnærming til sikkerhetskultur, og har ut ifra et slikt ståsted forsøkt å definere ønskelige egenskaper som organisasjoner bør strebe etter for å utvikle og opprettholde en optimal sikkerhetskultur. I litteraturen fremkommer det variasjon i forhold til ordbruk, hvor noen omtaler en "positiv" sikkerhetskultur, mens andre snakker om en "effektiv" eller "god" sikkerhetskultur. Vi vil i avhandlingen konsekvent benytte oss av ordet "optimal."

Flere tar i bruk James Reason (1997) sin teori og begrepsapparat i arbeidet med sikkerhetskultur (Ptil, 2014). Reason (2000) hevder at en god sikkerhetskultur er en *velinformert kultur* som vet hvor grensen mellom sikkerhet og uakseptabel fare er, uten å nødvendigvis måtte krysse denne. Det er flere forhold som kjennetegner en slik organisasjonskultur, blant annet at den har gode rapporteringssystemer, den oppleves som rettferdig, den er omstillingsdyktig og fleksibel, samt den lærer av sine erfaringer (Reason, 1997). Videre kjennetegnes kulturen av en konstant bevissthet og årvåkenhet i forhold til farene man står ovenfor, noe som innebærer at man ikke glemmer å være redd. Ved fravær av ulykker, er den beste måten å opprettholde en slik "sunn skepsis" å samle inn de rette type data (Reason, 1997).

I likhet med Reason (1997) hevder Jeffcott et al. (2006) at sikkerhetskultur er basert rundt et sett med definerte praksiser som organisasjonen kan justere i en positiv eller negativ retning. De har identifisert fire komponenter som kjennetegner en optimal sikkerhetskultur som i stor grad inkorporerer litteraturen om sikkerhetskultur og HRO gjennomgått ovenfor. Vi velger derfor å ta utgangspunkt i disse da vi mener de er svært dekkende samt at det kan forventes at de også kan anvendes i en sikringskontekst. Disse som følger: *forpliktelse, fleksibilitet, læring* og *tillit.*

Forpliktelse

Konseptene fra litteraturen fremhever ledelsens forpliktelse til sikkerhet som et kjennetegn ved en optimal sikkerhetskultur (Jeffcott et al., 2006). Det påpekes at denne forpliktelsen må være synlig overfor de ansatte og balansert i forhold til andre organisatoriske forhold. Det er svært viktig at ledelsen samhandler med de i den skarpe enden for å utvikle en realistisk forståelse for, og sensitivitet overfor operasjoner, samt for å etablere åpne systemer for kommunikasjon og læring (Jeffcott

et al., 2006). Hale (2000) fremhever også viktigheten av at ansatte og spesielt toppledere anser sikkerhet som et viktig mål. Videre at alle medlemmene i organisasjonene føler at de er involvert i prosesser som definering, prioritering og håndtering av risiko og at sikkerhet anses som et felles formål.

En av prosessene som inngår i konseptet om "collective mindfulness" er *sensitivitet overfor operasjoner* (Weick et al., 1999). Dette refererer til organisasjonens evne til å oppnå og opprettholde en oversikt over operasjoner, for å være i stand til å forutse potensielle fremtidige feil. Dette er et viktig kjennetegn ved HRO (Lekka, 2011). Weick et al. (1999) referer her til "having the bubble", som kan forstås som det å strebe etter å oppnå en tilstrekkelig god situasjonsforståelse. Det handler om å ha en oversikt over operasjonene til enhver tid, noe som er videre vanskelig å oppnå. HRO kjennetegnes ved at de retter stor innsats mot å oppnå nettopp dette. Gjennom en situasjonsforståelse kan man forebygge katastrofale konsekvenser ved at man kontinuerlig gjør tilpasninger og hindrer at feil akkumulerer (Weick et al., 1999).

Fleksibilitet

Flere teoretikere vektlegger fleksibilitet som et kjennetegn ved en optimal sikkerhetskultur (Jefcott et a., 2006). For å sørge for at passende beslutninger blir tatt i møte med kriser eller unormale operasjoner er det nødvendig å erkjenne, verdsette og bruke kunnskap og erfaringer som de i den "skarpe enden" besitter (Jeffcott et al., 2006). Pidgeon (1998) vektlegger viktigheten av realistiske normer og regler som tillater en fleksibel håndtering av farer som kan være mer eller mindre godt definerte på forhånd. Reason (1997) omtaler en *fleksibel kultur* som evnen organisasjonen har til å imøtekomme raske endringer og uventede situasjoner. Ofte innebærer dette et skift fra en hierarkisk struktur til en flatere struktur hvor beslutningsmyndighet gis til dem som besitter relevant ekspertise for å løse problemet. Reason (1997) referer her til "High Reliability Organisations" og deres evne til rask re-konfigurering og tilpasning. Under normale tilstander er HRO kjennetegnet av en hierarkisk struktur som innebærer klart definerte roller, ansvar, og rapporteringslinjer. Derimot når en krise oppstår, oppløses denne strukturen, og beslutningsmyndighet overlates til individer som besitter ekspertkunnskap for å håndtere det spesifikke problemet (Lekka, 2011). Evnen til å skifte fra sentralisert til desentralisert beslutningstaking i møte med kriser innebærer at ethvert problem får den oppmerksomhet som kreves fra

alle nivåer av organisasjonen. Oppløsning av hierarkiske strukturer blir videre fasilitert av HRO sitt vedvarende fokus på feil og faresignaler. Det som trigger en oppløsning av den hierarkiske strukturen er den kollektive, kulturelle antagelsen om at de nødvendige evnene for å håndtere problemet ligger et sted i systemet (Weick et al., 1999). Dette avhenger videre av kontinuerlig trening for sikre at de ansatte har nødvendig ferdigheter samt for å etablere tillitt mellom ledelsen og de i den skarpe enden (Reason, 1997). I forhold til fleksibilitiet vil også evnen til å unngå å forenkle fortolkninger være sentralt, da dette kan redusere sensitivitet overfor faresignaler (Weick et al., 1999).

Læring

Organisatorisk læring anses som et sentralt kjennetegn ved en optimal sikkerhetskultur. Dette omfatter at organisasjonen kontinuerlig reflekterer over praksiser gjennom monitorering, analysering og feedback systemer (Pidgeon, 1998). Pålitelige organisasjoner retter stor innsats mot å innsamle, analysere og videreformidle informasjon som kan ha betydning for sikkerheten. HRO er konstant opptatt av potensielle feil og svikt som kan oppstå, dvs.at de er kjennetegnet av en "kronisk" bekymring (*Preoccupation with failure*) og har en evne til å være opptatt av noe de sjeldent ser eller opplever (Weick et al., 1999). Ettersom ulykker er sjeldne, forsøker HRO å samle inn mest mulig data om alle mulige faresignaler og benytter dette som læringsmuligheter. Reason (1997) referer til dette som en *lærende kultur*. Selv de minste feil og svikt blir ansett som indikatorer av systemets helse, og nesten-ulykker blir grundig analysert (Weick et al., 1999).

For å samle inn mest mulig data oppfordres og belønnes ansatte til å rapportere feil. Det vil si en arbeider for å skape det Reason (1997) kaller en *rapporterende kultur*. Dette er spesielt viktig ettersom de fleste organisasjoner vil oppleve et fravær av ulykker, og man er derfor avhengig av at menneskene i systemet rapporterer selv de minste feil som kunne potensielt ha forårsaket skade. For å oppfordre til rappotering blir det blant annet viktig med konfidensialitet og av-identifisering av rapportenene, samt å separere de som samler inn og analyserer rapportene fra de som administrerer sanksjoner (Reason, 1997). Videre er det viktig at rapporteringsprosessen er enkel, og at de som rapporterer får rask tilbakemelding. Det påpekes også viktigheten av å beskytte de som rapporterer mot disiplinære sanksjoner så langt dette er praktisk

mulig. Dette fordi HRO vektlegger verdien av å være velinformerte og bevisste i forhold til potensialet for svikt, heller enn å straffe og legge skyld på individer. Dette kan videre knyttes til viktigheten av å skape en *rettferdig kultur* som Reason (1997) argumenterer for.

I HRO kan en feil være et svakt signal på sårbarheter i andre deler av systemet, det vil si at feil generaliseres og blir ansett som systemiske heller enn lokale (Weick et al., 1999) Her vil nyttiggjørelse av data være en avgjørende faktor for å lære etter hendelser og korrigere eventuelle svakheter i systemet. Det er viktig at ledelsen har en vilje og kompetanse til å trekke riktige konklusjoner, samt en vilje til å handle basert på disse (Reason, 2000). En av de mest alvorligste effektene av en dårlig sikkerhetskultur er en uvilje til å håndtere farer proaktivt. Historien er full av kjente eksempler hvor ledelsen neglisjerer eller utsetter å korrigere identifiserte svakheter i systemets barrierer (Reason, 1998).

HRO er også bevisste i forhold til at suksess kan ha uønskede konsekvenser i form av redusert oppmerksomhet, selvtilfredshet og redusert søken etter faresignaler. Slike dysfunksjonelle responser på suksess representerer en annen type "feil" som HRO søker å fange opp og benytte som en læringsmulighet (Weick et al., 1999).

Tillit

Jeffcott et al., (2006) påpeker at tillit er et viktig kjennetegn ved en optimal sikkerhetskultur. Han påpeker likevel at dette i stor grad har blitt oversett i litteraturen om sikkerhetskultur. Tillit blir ansett som et sett med holdninger og forventninger man har i forhold til andre mennesker og organisasjonens systemer. Dette påvirker faktorer som kommunikasjon, samarbeid, informasjonsdeling, samt rapportering (Jeffcott et al., 2006). Dermed blir også tillit sentralt i forhold til at det kan påvirke sikkerhetskulturen på en positiv måte. For å skape en *rapporterende kultur* er det essensielt at de ansatte har tillitt til at ledelsen behandler rapportene og impliserte personer på en rettferdig måte. Dette innebærer også at man må skape en *rettferdig kultur* knyttet til hvordan organisasjonen håndterer skyld og straff, og dette må ligge til grunn for enhver sikkerhetskultur (Reason, 1997). Dette betyr at man må skape en atmosfære hvor ansatte er oppfordret til å rapportere sikkerhetsrelatert informasjon

ved at grensen mellom akseptabel og uakseptabel atferd er tydeliggjort. Noen handlinger som for eksempel sabotasje eller uforsvarlig atferd vil kreve sanksjoner. Dermed vil en "no blame" kultur hvor alle medlemmene er immune mot straff og skyld kunne føre til lavere troverdighet og ikke oppleves som rettferdig (Reason, 1997).

I tillegg til overnevnte elementene vektlegger litteraturen at sikkerhetskultur må være noe man kontinuerlig streber etter å forbedre. Reason (2000) advarer, *"If an organisation is convinced that it has achieved a safe culture, it almost certainly has not. Safety culture, like a state of grace, is a product of continual striving. There are no final victories in the struggle for safety." (Reason, 2000, s. 4).* Selvtilfredshet svekker evnen til å fange opp faresignaler, som fører til økt risiko for ulykker og uønskede hendelser. Dersom man sier seg fornøyd med sikkerhetskulturen kan dette være et faresignal i seg selv.

Reason (1998) hevder at en dårlig sikkerhetskultur vil innebære manglene evne til å forstå og frykte hele spekteret av operasjonelle farer man står ovenfor, noe som kan undergrave systemets sikkerhet ved å øke antall aktive feil. Slike feil gjort i den skarpe enden stammer fra utilstrekkelig trening, kommunikasjon, prosedyrer og problemer med design. En svak sikkerhetskultur vil videre oppfordre til en atmosfære av manglende etterlevelse av sikkerhetsoperasjonelle praksiser. Brudd av en slik art er trolig mest fremtredende i organisasjoner hvor produktivitet og økonomiske mål overgår sikkerhetsmål (Reason, 1998). Videre kan manglende evne til å forstå omfanget av operasjonelle farer føre til langstidsvirkende svakheter i systemets forsvar (Reason, 1998).

2.5 Sikringskultur

I motsetning til litteratur om sikkerhetskultur viser vår litteraturgjennomgang at det er begrenset forskning og tilgjengelig litteratur omkring sikringskultur både som begrep og fenomen. Dermed fremstår begrepet som relativt umodent.

På lik linje med sikkerhetskultur anser vi sikringskultur som et aspekt av organisasjonskulturen, som kan påvirke sikringsnivået i positiv eller negativ forstand. Dette medfører at man kan snakke om det å ha en mer eller mindre optimal sikringskultur, hvor en optimal sikringskultur er en kultur som antas å påvirke sikringsnivået positivt. Vi vil først presentere ulike definisjoner på sikringskultur, og deretter presentere tilgjengelig litteratur og forskning.

2.5.1 Hva er sikringskultur?

Det fremgår i litteraturen at det ikke finnes noen akseptert eller praktisk definisjon på sikringskultur, heller ei en akseptert måte å måle sikringskultur. Samtidig fremheves det at uavhengig av grad av teknologiske tiltak og systemer, vil de ansattes atferd og holdninger sammen med sikringsprosedyrer ha en innvirkning på sikringssystemet (Malcolmson, 2009). Innen enkelte sektorer, for eksempel kjernekraftindustrien, har det vært et pågående arbeid med å utvikle og finne en adekvat definisjon på sikringskultur. Reniers et al. (2011) har utarbeidet en definisjon av sikringskultur som rettes spesielt mot kjernekraftindustrien:

A security culture in a chemical plant is the extent to which workers within the organizational premises (e.g plant employees, contrators) regard security as important and the beliefs about how (physical, electronic, organizational, etc) security should be executed, bearing in mind that hazardous substances are being handled in large quanities in the plant. These values and beliefs will evolve into certain norms about how to handle chemical company security (Reniers et al., 2011, s. 1242).

Reniers et al. (2011) knytter sin definisjon til Schein og hevder at normene i organisasjonen blir videreformidlet og lært til nye medlemmer som den måten sikring blir håndtert og utført på innad i organisasjonen. Til tross for at definisjonen er rettet mot kjemikalieindustrien, mener vi at deler av den kan benyttes generelt sett

uavhengig av industri. Eksempelvis at sikringskultur dreier seg om i hvilken grad ansatte anser sikring som viktig, og antagelser om hvordan sikring bør utføres, som videreutvikles til normer om hvordan man skal håndtere sikring. Dette kan videre knyttes opp til Schein sin trenivås modell (Schein, 2010).

Talbot og Jakeman (2009) viser til en annen generell definisjon av sikringskultur i sin bok om Securiy Risk managment:

> *Security culture is the logical result of a well-driven security awareness program. Once people become aware of threats it is in their nature to react to it. Motivated people want to solve a problem if they feel concerned about it.* (Lafrancè, 2004 i Talbot & Jakeman, 2009, s. 37).

Definisjonen legger vekt på bevissthet og motivasjon blant ansatte som nødvendig for å utvikle en sikringskultur. Det fremgår ikke hva sikringskultur faktisk er, men heller hvordan en sikringskultur kan oppnås. Definisjonen synes å bygge på en forståelse om at sikringskultur er noe en organisasjon enten har eller ikke har. Dersom de ansatte er bevisste omkring sikringstrusler og motiverte til å løse problemer, hevder definisjonen at man har en sikringskultur. I vår forståelse av sikringskultur vil alle organisasjoner ha en sikringskultur, men denne kan være mer eller mindre optimal. Overnevnte definisjon vil da tilsvare en såkalt "optimal" sikringskultur.

Malcolmson (2009) argumenterer for at sikringskultur potensielt kan påvirke sikringsnivået i organisasjonen, ved at den kan påvirke hvordan ansatte samhandler med organisasjonens systemer og prosedyrer til enhver tid, som videre resulterer i akseptabel eller uakseptabel atferd. Det blir påpekt at organisasjoner som har sikring som en kritisk suksessfaktor, har større sannsynlighet for å oppnå sine fastsatte mål og opprettholde sitt omdømme dersom de forstår betydningen av sikringskultur samt vet hvordan organisasjonen kan forsterke denne kulturen (Malcolmson, 2009). Malcolmson (2009) viser et forskningsprosjekt, gjort av QinetiQ, et britisk forsvarsindustriselskap, hvor hensikten var å utforske og definere begrepet sikringskultur i en rekke organisasjoner innen luftfart. Deres forskningsarbeid resulterte i følgende definisjon av sikringskultur:

> *Security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organisation, and behaviours they perform, which could potentially impact on the security of that organisation, and that may, or may not, have an explicit, known, link to that impact* (Malcolmson, 2009, s. 361).

Forfatterne hevder at enkelte aspekter ved sikringskulturen utvikles i møte med organisasjonens sikringstrusler som derav blir forfektet av organisasjonens ledelse. Dette kommer til uttrykk gjennom organisasjonens sikringspraksiser og styrende retningslinjer, grad av etterlevelse og forståelse for disse, samt erkjennelse og bevissthet for sikringstruslene i organisasjonen (Malcolmson, 2009). Andre aspekter av organisasjonens sikringskultur blir uformelt lært gjennom en naturlig, ikke-kontrollert sosialiseringsprosess. Dermed kan dette føre til holdninger og atferd som ikke nødvendigvis er akseptert blant lederne (Malcolmson, 2009).

Definisjonen legger vekt på at sikringskultur springer ut fra antagelser, verdier, og holdninger som medlemmer i organisasjonen innehar. I tråd med Schein sine nivåer av organisasjonskultur, kommer disse til uttrykk gjennom medlemmenes handlinger og atferd, som igjen påvirker sikringsnivået i organisasjonen. Videre er denne i tråd med vår forståelse av at sikringskultur er noe alle organisasjoner har, men sikringskulturen kan være mer eller mindre optimal i forhold til om den påvirker sikringsnivået positivt eller negativt.

2.5.2 Tilgjengelig litteratur om sikringskultur

Talbot og Jakeman (2009) sikter på å etablere et rammeverk for hvordan sikringsrisiko bør håndteres i en organisasjon og fremhever at sikringskulturen er et viktig element i organisasjonens helhetlige risikostyring. Sikringskultur forstås her ikke som et mål i seg selv, men snarere som en sinnstilstand og "måten ting blir gjort på her hos oss," noe som støtter opp organisasjonens bredere målsetninger. På bakgrunn av dette hevdes det at implementering av en slik sikringskultur kan være vanskelig og den avhenger av en rekke elementer for å forme atferd, holdninger og tillitt (Talbot & Jakemann, 2009). Forfatterne knytter dette til teori om sikkerhetskultur som argumenterer for at en optimal sikkerhetskultur er en *velinformert kultur* (Reason, 1997). Gitt likheten mellom sikkerhet og sikring hevder

de at også en optimal sikringskultur kan anses som en *velinformert kultur*. I en slik kultur vil de som leder, drifter og benytter sikringssystemet inneha kunnskap om de menneskelige, tekniske, organisatoriske og miljømessige faktorene som avgjør effektiviteten til systemet som helhet (Talbot & Jakeman, 2009). Reason (1997) argumenterer for fire ulike subkulturer som tilsammen skaper en informert kultur; rapporterende, rettferdig, fleksibel og lærende. Disse inngår i Jeffcott et al. (2006) sine elementer som beskrevet tidligere i oppgaven, og kan dermed støtte opp at elementene kan også være anvendelige i en sikringskontekst. Selv om forfatterne viser til Reason (1997) sin ide om en *velinformert kultur*, går de ikke særlig inn på hvordan disse elementene kan anvendes i en sikringssammenheng.

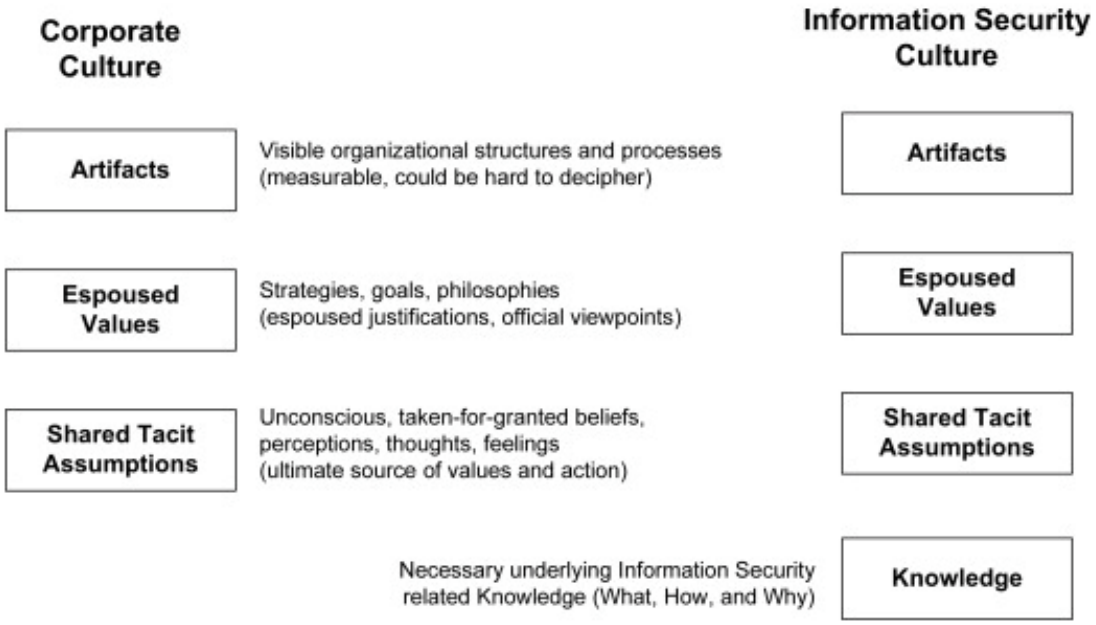
2.5.3 Information security culture

Til tross for at det er gjort lite forskning omkring sikringskultur, finnes det en del litteratur om en såkalt *Information Security Culture*, blant annet teorier om hva som er viktige aspekter ved en slik kultur. Forskningen bygger i stor grad på organisasjonskultur hvor information security culture anses som et aspekt av denne, og er dermed også i stor grad anvendelig i en bredere sikringskontekst. For å være i tråd med vår oversettelse av safety og security til henholdsvis sikkerhet og sikring, har vi valgt å oversette dette til informasjonssikringskultur.

For å kunne respondere på nye utfordringer og sikre overlevelse i et konkurransepreget marked argumenter AlHogail (2015) for at virksomheter må øke deres evne når gjelder informasjonssikring. Flere forskere fremhever at sikring både er et menneskeproblem og et teknisk problem, og at informasjonssikring er mye mer enn å anvende fysiske og tekniske tiltak (Thomson, Von Solms & Louw, 2006, AlHogail, 2015). Det påpekes videre at et av de største problemene når det gjelder beskyttelse av informasjon er mangel på kunnskap, ferdigheter og forpliktelse blant ansatte, samtidig som den menneskelige faktoren ofte blir oversett (Thomson et al., 2006). Van Nierkerk og Von Solms (2010) viser til en rekke studier som demonstrerer at utviklingen av en informasjonssikringskultur er helt essensielt for oppnå et høyt nivå av informasjonssikring i virksomheten. Ved å utvikle en slik kultur kan de ansatte bli en ressurs for sikringsnivået i virksomheten, i istedenfor en risiko.

Et kulturrammeverk for informasjonssikringskultur

Van Nierkerk og Von Solms (2010) hevder at innen informasjonssikring er det helt sentralt at de ansatte har tilstrekkelig med kunnskaper om hvordan de skal utføre sine normale arbeidsoppgaver på en sikker måte. De understreker at man ikke kan anta at de ansatte innehar kunnskaper om informasjonssikring. Forfatterne knytter dette til Schein sin trenivåsmodell, og legger til ett ekstra nivå i modellen; *kunnskap om informasjonssikring.* (Van Nierkerk & Von Solms, 2010). De argumenterer for at dette kan bli sett på som det fjerde nivået i en informasjonssikringskultur og at dette vil støtte opp samt påvirke hvert av de tre andre nivåene; artefakter, uttrykte verdier og underliggende antagelser. Uten tilstrekkelig kunnskaper kan ikke informasjonssikkerhet oppnås, og dermed må man inkludere kunnskapsnivået (Van Nierkerk & Von Solms, 2010).



Figur 4: Nivåer av kultur basert på Schein (Van Nierkerk & Von Solms, 2010).

Ved å modellere kunnskap som et individuelt nivå kan man enklere illustrere effekten som kunnskap, eller mangel på kunnskap, har på den samlede kulturen (Van Nierkerk & Von Solms, 2010).

Thomson et al. (2006) fremhever også at de ansatte må inneha nødvendig kunnskap for å være i stand til å sikre informasjon. De ansatte må forstå sine roller og ansvar,

samt motta opplæring i hvordan man skal beskytte informasjon i organisasjonen. Dermed må informasjonssikringspraksiser være en del av organisasjonskulturen, da denne legger begrensninger på aktivitetene og atferden til de ansatte (Thomson et al. 2006). Dette betyr at beskyttelse av informasjon må være en del av de daglige aktivitetene og en naturlig del av de ansattes atferd. Det er langt mer effektivt med en kultur som fremmer hensiktsmessig sikringsrelatert atferd gjennom kunnskap, artefakter, verdier og antagelser enn å pålegge de ansatte en viss atferd gjennom regler (AlHogail, 2015). Det påpekes at sikringen kun blir effektiv dersom ansatte har kjennskap til, forstår og aksepterer de nødvendige forhåndsreglene og tiltakene (AlHogail, 2015).

Thomson et al. (2006) påpeker at for å kunne endre kulturen, må de ansattes verdier, normer og holdninger endres. Dette innebærer at antagelser hos de ansatte må avlæres, noe som kan resultere i motstand til endring. Videre hevdes det at ettersom miljøet innad i organisasjonen har størst påvirkning på de ansattes holdninger og antagelser, vil makten til å endre kulturen hovedsakelig ligge hos toppledelsen. Ifølge Thomson et al. (2006) bør toppledelsen demonstrere sitt engasjement i forhold til informasjonssikring ved å vise støtte og forpliktelse til en formell og dokumentert *Corporate Information Security Policy.* Formålet med enhver policy er å påvirke beslutninger, handlinger og atferd hos ansatte ved å spesifisere hvilken type atferd som er akseptabel eller ikke (Thomson et al., 2006).

For å sikre et tilfredsstillende kunnskapsnivå i forhold til informasjonssikring, anbefales bruken av organisatoriske kampanjer for å øke security awareness, forstått som sikringsbevissthet (Van Nierkerk & Von Solms, 2010). Slike kampanjer fokuserer på ulike aspekter ved informasjonssikring slik at enhver ansatt vil anse informasjonssikring som en naturlig del av deres daglig arbeid. I tillegg har kampanjene til hensikt å belyse hvilke problemer mangel på kunnskap om informasjonssikring kan medføre, noe som igjen kan påvirke bevisstheten til de ansatte. På bakgrunn av dette anses bruken av awareness kampanjer som et nøkkelelement i arbeidet med å utvikle en informasjonssikringskultur (Van Nierkerk & Von Solms, 2010).

På lik linje vektlegger Relf og Stubblefield (2000) sikringsbevissthet og knytter dette opp til håndtering av sikringsrisiko i petroleumssektoren. Hovedfokus her er på

håndtering av terrortrusler i høyrisikoland hvor multinasjonale oljeselskaper er lokalisert. For å være i stand til å avskrekke og motvirke intenderte uønskede hendelser, understrekes betydningen av at virksomheten innehar et høyt nivå av sikringsbevissthet, i kombinasjon med avansert sikringstiltak og opplæring. Blant annet påpekes det viktigheten av proaktiv deltakelse på alle nivåer i virksomheten. For det første understrekes at de ansatte forstår viktigheten av sikringsbevissthet og setter seg inn de potensielle sikringsrisikoene virksomheten står ovenfor. Videre vektlegges korte og informative informasjonsorienteringer slik at de ansatte raskt kan identifisere kritiske situasjoner og reagere hensiktsmessig. Her er det også sentralt at personell er forberedt på en mulig beredskapssituasjon og vet hvordan og når en skal reagere. Avslutningsvis påpekes viktigheten av at informasjon om potensielle trusler kontinuerlig oppdateres, og at denne informasjonen videreformidles innad i virksomheten på en hensiktsmessig måte. Relevant informasjon om trusselbilde og sikringsrisikoer må dermed integreres inn i virksomhetens beredskapsplaner, noe som igjen legger føringer for både håndtering, akutt medisinhjelp, beskyttelse av verdier, samt normalisering (Relf & Stubblefield, 2000).

Aspekter ved en "optimal" informasjonssikringskultur

Ruighaver et al. (2006) har i sitt studie av informasjonssikringskultur anvendt et organisasjonskultur-rammeverk fra Detert, Schroeder & Maurriel (2000, i Ruighaver, 2006). Det argumenteres at sikringskultur ikke kan studeres separat fra den bredere organisasjonskulturen, noe som er i tråd med vår forståelse av sikringskultur som et aspekt av organisasjonskulturen. Ifølge forfatterne er informasjonssikring generelt sett et ledelsesproblem, og sikringskulturen reflekterer hvordan ledelsen håndterer dette problemet (Ruighaver et al., 2006). Forfatterne viser til åtte aspekter av det de anser som en "optimal" informasjonssikringskultur, og disse vil bli presentert i det følgende:

1) Grunnlaget for sannhet og rasjonalitet

Forfatterne hevder at kvaliteten av en sikringskultur vil både avhenge av antagelsene som organisasjonen har om viktigheten til sikring. I tillegg hvordan de evaluerer og håndterer rasjonaliteten til antagelser angående sikringen, både blant ledere og ansatte. Det fremkommer en tendens til at organisasjoner mener sikringsnivået er bra til tross for at de ikke evaluerer sikringens effektivitet. Det som utgjør en god

sikringskultur er ledernes og ansattes evne til å være kritiske til egne antagelser samt at organisasjonen har prosesser på plass som kan utfordre disse.

2) Tidsaspektet

Det argumenteres for at en sikringskultur av "høy kvalitet" vektlegger en langsiktig forpliktelse og strategi med den hensikt å bygge opp nødvendige ferdigheter relatert til sikring, eller for å innrette organisasjonens sikring med dens organisasjonskultur. Likevel påpekes det at ofte er sikringsfokuset rettet mot saker som krever umiddelbar oppmerksomhet, og ikke på saker som kan vise seg å være viktigere på lang sikt. Med et kortsiktig fokus vil sikring ofte blir glemt etter første opplæring, med mindre det oppstår et sikringsbrudd. Dermed argumenteres det for en mer langsiktig strategi hvor man jevnlig minner ansatte på deres ansvar i forbindelse med sikring gjennom ulike organisatoriske prosesser.

3) Motivasjon

Det fremkommer av case studiene at ansatte ikke har en iboende motivasjon til å adoptere sikringspraksiser. Organisasjoner med en "optimal" sikringskultur må derfor ha passende prosesser på plass som sikrer at ansatte er motiverte i forhold til sikring. Her nevnes eksempelvis belønning, erkjennelse og sosial deltakelse, som kan knyttes til motivasjon og videre fører til atferdsendring hos ansatte. Videre påpekes det viktigheten av at organisasjoner ikke motsier de verdiene de forsøker å "pålegge" de ansatte, ved eksempelvis å sette mål som motstrider sikringsmålene. I en ideell sikringskultur vil ansatte være motivert til å reflektere over sin atferd til alle tider, til å vurdere hvordan deres atferd påvirker sikringen, og hva de kan gjøre for å forbedre sikringsnivået. For å skape slike holdninger, er det viktig at en viss grad av tillit er tilstede, samt at alle ansatte har et individuelt ansvar for å handle på riktig måte. Dette betyr ikke at virksomheten ikke bør ha prosesser på plass som overvåker sikringsbrudd og som forsikrer at uakseptabel atferd korrigeres, samt at eksemplarisk atferd blir belønnet. Videre kan ansatte motiveres ved å ha et eierskap til sikring. Dersom ansvar delegeres fra ledelsen til alle ansatte i organisasjonen, kan dette skape en drivkraft som motiverer de ansatte til å etterleve sikringsprosedyrer. Videre påpekes at det er viktig å legge tilrette for sosial deltakelse på tvers av forretningsområder og/eller avdelinger.

4) Stabilitet versus endring/innovasjon/personlig utvikling

Ofte vil organisasjoner med et lavere sikringsbehov mangle en forståelse for at sikringsprosedyrer og praksiser må kontinuerlig forbedres, og at organisasjonen må konstant tilpasse dens sikringsarbeid i forhold til endringer i omgivelsene. Disse organisasjonene har også en tendens til å iverksette endringer uten å vurdere virkningene dette har for sikringen i organisasjonen. Organisasjoner med et høyt sikringsbehov har videre en tendens til å anse endring som uønsket ettersom det kan resultere i nye typer risikoer eller forbigåelse av eksisterende risikotiltak. Videre påpekes det at sikring aldri er 100% og derfor må man forsikre seg om at sikringsarbeidet ikke er statisk. I den forbindelse påpekes det at enhver organisasjon er unik og at nye utfordringer kan oppstå i omgivelsene som kan medføre et behov for nye og utradisjonelle tilnærminger.

5) Orientering til arbeid, oppgaver og medarbeidere

Et sentralt prinsipp innen informasjonssikring er at det alltid må foretas en avveining mellom bruk av organisasjonens eiendeler og eiendelens sikring. Ved å begrense tilgang på eiendelen kan man øke sikringsnivået til eiendelen, samtidig som dette kan sette begrensninger for de daglige operasjonene til de ansatte. I organisasjoner med et høyt sikringsbehov, har de ansatte en tendens til å akseptere disse begrensningene i større grad. Et viktig aspekt av sikringskultur er derfor å finne den riktige balansen mellom sikring og hvor begrenset de ansatte føler seg. Videre vil ansatte føle seg mindre begrenset dersom de er motiverte og føler et ansvar for sikringen. Dersom de ansatte føler at ledelsen ikke tar forbedringsforslag på alvor, kan dette svekke deres eierskapsfølelse. Videre er det viktig at ansatte blir opplært i deres roller og ansvar, og at slik trening forsterkes kontinuerlig og responderer på uakseptabel atferd. I mange organisasjoner får ansatte kun en rask gjennomgang ved oppstart, men det påpekes at opplæring også kan brukes som et verktøy for å øke ansvarsfølelsen og eierskap hos de ansatte som er involvert i sikringsrelaterte beslutninger eller implementering av disse beslutningene.

6) Isolasjon versus samarbeid

Case studiene avdekket at organisasjonens sikringsplanlegging og implementering ble kun håndtert av en mindre gruppe ledere og spesialister. Likevel var det tydelig at det var uakseptabelt å kun ha èn person med et slikt ansvar. Studien viste også at flere

erkjenner at utvikling av sikringspolicyer bør skje gjennom et samarbeid hvor en benytter input fra personer i ulike deler av organisasjonen for å sikre aksept. Til tross for dette blir prinsippet ofte oversett i daglige aktiviteter knyttet til styring av sikring og design av sikringsprosesser. Dette medfører at innsatsen til sikringsteamet ofte blir motvirket av beslutninger til ledere i andre enheter og på gulvet. Et slikt mangel på samarbeid kan påvirke både motivasjon og hvordan en forholder seg til arbeidsoppgaver på en negativ måte, samt kan føre til et for snevert fokus på sikring. I tillegg til sikringstiltakenes kvalitet, påpekes det viktigheten av å ta hensyn til alle sikringsområder. Å overse bestemte områder kan derfor være svært ødeleggende for den totale sikringen i organisasjonen.

7) Kontroll, koordinering og ansvar

Casestudiene viste at i de organisasjonene hvor sikringsmålene ikke var i tråd med de organisatoriske målene, var det også større grad av motvilje til å støtte sikringsinitiativene. Et viktig aspekt ved sikringskulturen er hvordan organisasjonen håndterer ansvarlighet for beslutninger i sikringsstyringen. Uavhengig om det er tett eller løs kontroll i organisasjonen er det viktig at det er klare retningslinjer for hvem som har beslutningsmyndighet i ulike områder knyttet til sikring. Dette kalles som regel ansvar, men her påpekes det at det å *ha* ansvar og det å *føle* et ansvar er to forskjellige ting, hvor delegering av ansvar gjennom organisasjonen blir sentralt. I tillegg til dette trengs det støtte fra toppledelsen, da deres støtte til informasjonssikring utgjør en betydelig indikator for hvilken retning organisasjonens sikringskultur utvikler seg i, og i hvilken grad sikringspolicyene blir håndhevet. Toppledelsen har et ansvar for å:

a. Synlig demonstrere prioritering av informasjonssikring
b. Ta hensyn til sikringssaker i planlegging av organisasjonens strategier
c. Gi sterk og konsistent støtte til det helhetlige sikringsprogrammet

8) Orientering og fokus - internt og eksternt

Studien viser at det ofte er fokus på å etterleve kravene, heller enn å forbedre sikringen. Dermed kan man si at organisasjonene ofte har et eksternt fokus, men mangel på internt fokus. Andre organisasjoner ser det både som viktig å etterleve eksterne krav, samtidig som de selv vurderer hva som er best for organisasjonen. Ettersom sikring i en organisasjon påvirkes både av eksterne og interne faktorer,

påpekes det at en optimal sikringskultur har en slik balanse mellom dem. Det eksterne fokuset bør inkludere en bevissthet omkring omgivelsene og hvordan dette endres over tid, slik at man proaktivt kan håndtere nye trusler som oppstår. I tillegg må en skape en bevissthet i forhold til det interne sikringsmiljøet, hvor man søker å identifisere sikringsbrudd og hvorfor disse inntreffer. Dette er nødvendig dersom man skal vurdere om sikringsstrategiene fungerer effektivt og hvordan man kan forbedre implementeringen av disse.

Til tross for den overnevnte teorien fokuserer på informasjonssikring og utvikling av en informasjonssikringskultur, mener vi dimensjonene er relativt generelle da de baseres på litteratur om organisasjonskultur. Dermed synes de også å være anvendelig i en bredere sikringskontekst som omfatter blant annet fysisk- og personellsikring.

Oppsummering av teori

Vi har i det foregående beskrevet en teoretisk bakgrunn som danner rammen for problemsstillingen og hva vi ønsker å undersøke i avhandlingen. Vårt teoretiske rammeverk er i stor grad basert på teori om sikkerhetskultur som bygger på teori om organisasjonskultur og HRO. Blant annet har vi valgt å benytte oss av fire fremtredende elementer ved en optimal sikkerhetskultur som beskrevet av Jeffcott et al. (2006): *forpliktelse, fleksibilitet*, *læring* og *tillit*. Det kan tenkes at disse også kan anvendes i en sikringskontekst, samtidig som vi ser at det er en mangel på lignende teorier innenfor sikringskultur-feltet. En optimal sikringskultur kjennetegnes dermed av følgende elementer; ledelsen demonstrerer en forpliktelse til sikring, åpen kommunikasjon basert på gjensidig tillit, høyt fokus på kontinuerlig læring og forbedring ved å samle inn, analysere og videreformidle informasjon som har betydning for sikringen, samt en fleksibel tilnærming til å håndtere sikringshendelser. Ved en slik tilnærming blir sikringskultur basert rundt et sett med definerte praksiser som organisasjonen kan justere i en positiv eller negativ retning.

Til tross for at forskning om sikringskultur er begrenset, fremkommer det en rekke definisjoner, hvor flere referer til Schein (2010) og hans tre nivåer av organisasjonskultur. På bakgrunn av begrenset forskning omkring sikringskultur, har vi også inkludert tilgjengelig litteratur om informasjonssikringskultur. Gitt ulikhetene

mellom sikkerhet og sikring som i knyttes til intensjonsbegrepet, kan denne litteraturen fungere som et supplement hvor sikkerhetskultur-teorien ikke nødvendigvis er tilstrekkelig dekkende i en sikringskontekst. Litteratur om sikringskultur, herunder *information security culture*, vektlegger sikringsbevissthet ("security awareness"), kunnskap, motivasjon og ansvarsfølelse for sikring som viktige aspekter ved en informasjonssikringskultur. Litteraturen fokuserer i større grad på de dypere nivåene av Schein sin trenivåsmodell. Teorien understreker at det er mer effektivt å fremme ønsket atferd gjennom kunnskap, verdier og antagelser enn å pålegge de ansatte en viss type atferd gjennom regler. Til tross for at teoriene fokuserer på informasjonssikring, bygger teoriene på teori om organisasjonskultur, hvor informasjonssikringskultur ses på som et aspekt av organisasjonskulturen. Litteraturen kan dermed tenkes å være anvendelig i en bredere sikringskontekst. På lik linje vil en sikringskultur også være et aspekt av virksomhetens organisasjonskultur, hvor sikring også omfatter andre områder som fysisk sikring og personell sikring, som kan påvirke sikringsnivået i positiv eller negativ forstand.

Det teoretiske rammeverket danner grunnlaget for vår forståelse av hva sikringskultur er og hva som forventes å være elementer ved en optimal sikringskultur. Med dette som bakteppe vil vi utforske operatørselskapenes syn på utvikling av en optimal sikringskultur og på bakgrunn av dette vurdere hvorvidt begrepet sikringskultur fremstår som hensiktsmessig i arbeidet med å utvikle en slik kultur.

Med utgangspunkt i problemstilling og teori har vi utarbeidet følgende forskningsspørsmål som vi ønsker å få svar på:

1. *Hva legger operatørselskapene i begrepet sikringskultur og hvorvidt benyttes begrepet i virksomhetens sikringsarbeid?*
2. *Hvilke elementer oppfattes som viktige i arbeidet med å utvikle en "optimal" sikringskultur?*
3. *Hvilke utfordringer opplever operatørselskapene i arbeidet med å utvikle en slik kultur?*

3.0 Metode

3.1 Begrunnelse for metodisk tilnærming

Avhandlingen tar sikte på å utforske meninger, fortolkninger, oppfatninger og synspunkter omkring sikringskultur både som begrep og som fenomen. Dette på bakgrunn av at kulturens betydning for sikringsnivået har blitt belyst i kjølvannet av en rekke sikringshendelser, samtidig som sikringskultur begrepet har blitt løftet frem. I lys at det endrede risikobildet i Norge, som preges av blant annet en økt terrortrussel og vedvarende etterretningstrussel (NSM, 2015), anses temaet som svært aktuelt både for petroleumssektoren, og samfunnet forøvrig. Basert på den erfaringen operatørselskaper i petroleumssektoren har med sikkerhetskulturbegrepet samt at sikring har fått et økt fokus i sektoren, forventes det at fagpersoner innen security/HMS feltet kan bidra med meninger og innehold omkring temaet. Som konsekvens tar avhandlingen for seg hvilket syn operatørselskapene har på utvikling av en optimal sikringskultur, for å så vurdere hvorvidt sikringskultur begrepet fremstår som hensiktsmessig i arbeidet med å utvikle en slik kultur.

Vår litteraturgjennomgang illustrerte at det er begrenset forskning omkring sikringskultur og det rådes ingen entydig definisjon av begrepet (Malcolmson, 2009). En kvalitativ tilnærming ble dermed ansett som egnet for å avdekke ulike forståelser, meninger og oppfatninger om fenomenet blant fagpersoner, hvor det krevdes en åpen og fleksibel tilnærming. Ved å benytte en slik tilnærming fikk vi mulighet til å oppnå en dybeforståelse for temaet og på den måten være i stand til å besvare problemsstillingen (Jacobsen, 2000). Vår problemsstilling er som nevnt innledningsvis følgende:

> "*Hva er operatørselskapene i petroleumssektoren sitt syn på utvikling av en optimal sikringskultur og hvorvidt fremstår begrepet sikringskultur som hensiktsmessig i arbeidet med å utvikle en slik kultur?*

3.2. Datainnsamling

3.2.1 Intervju

Vi besluttet å benyttet åpne individuelle intervjuer som datainnsamlingsmetode. En slik metode var egnet ettersom vi var ute etter meninger og fortolkninger omkring temaet sikringskultur og dette ga oss mulighet til å gå i dybden med hensyn til aktuelle tema (Jacobsen, 2000). Samtidig er sikring et sensitivt tema, slik at fokusgruppeintervju ble ansett som mindre egnet for vår problemstilling.

Dataene ble innsamlet ved bruk av semi-strukturerte intervju med hovedsakelig åpne spørsmål, som er i tråd med formålet med vår avhandling. Fordelen med å benytte semi-strukturert intervju var at det ga oss mulighet til å komme med oppfølgingsspørsmål og dermed få mer utfyllende svar når dette var ønskelig (Thagaard, 2009). En annen fordel er at det ga oss anledning til improvisasjon dersom informanten brakte opp nye svar eller temaer som vi ikke hadde forutsett.

Vårt teoretiske rammeverk besto av litteratur innen både sikkerhetskultur og sikringskultur-feltet som i stor grad bygger på teori om organisasjonskultur samt studier av HRO. Til sammen skaper dette vår forståelse for hva en "optimal" sikringskultur er og hva som kunne forventes av studiet. Valgt teori ble så operasjonalisert ved å utarbeide en intervjuguide. Denne besto av en rekke temaer med tilhørende spørsmål med den hensikt at det skulle bidra til å besvare forskningsspørsmålene. Her ønsket vi blant annet å avdekke hva informanten la i begrepet sikringskultur, om begrepet ble benyttet i virksomheten, hva som ble ansett som sentrale kjennetegn ved en "optimal" sikringskultur, samt hvilke elementer ble vektlagt i arbeidet med å utvikle en slik kultur og eventuelle utfordringer. Intervjuguiden hadde som funksjon å sørge for at vi dekket disse emnene. Likevel ble ikke intervjuguiden fulgt slavisk fordi vi ønsket å skape en setting hvor informanten fikk tale fritt, og dermed ble temaene tatt opp i en rekkefølge som falt naturlig for informanten (Jacobsen, 2000). Dette grunnet at vi var ute etter informantens forståelser og meninger om sikringskultur, noe som kunne tenkes å variere fra informant til informant. I tillegg var det lite forskningsbasert kunnskap om temaet, og dermed var det viktig at vi inntok en åpen tilnærming til fenomenet.

3.2.2 Utvalg

Ettersom formålet med avhandlingen var å gi økt innsikt og kunnskap rundt fenomenet sikringskultur, heller enn å generalisere, har vi ikke benyttet statistiske metoder for å velge ut operatørselskapene (Kvale & Brinkmann, 2009). I februar 2015 utarbeidet vi en liste over operatørselskaper som opererer på norsk sokkel. Det ble deretter forsøkt opprettet kontakt med flere av disse, hvor vi ønsket å inkludere operatørselskaper av ulike størrelser, driftstid, ressurser, nasjonaliteter og historikk. Dette var fordi vi hadde som formål å få frem ulike meninger og tolkninger om fenomenet og få frem et nyansert bilde av temaet. Dermed inkluderte vi både selskaper med og uten en egen avdeling for sikring. Flertallet av selskapene på listen hadde kontorer i Stavanger, noe vi anså som en fordel både tidsmessig og ressursmessig. Likevel ønsket vi ikke å avgrense utvalget basert på lokasjon, noe som innebar at ett av selskapene i utvalget holdt til i Oslo. Vårt endelige utvalg besto av 12 operatørselskaper innen petroleumssektoren som opererer på norsk sokkel, av en populasjon på ca. 20 operatørselskaper.

3.2.3 Valg av informanter

I følge Kvale & Brinkmann (2009) finnes det ingen standard metode for utvelgelse av informanter i kvalitative undersøkelser, likevel er det viktig å velge ut informanter som medfører at forskningens funn preges av høy grad av gyldighet. Vårt valg av informanter ble tatt på bakgrunn av følgende kriteriet: hvem i selskapet besatt mest kunnskap og kunne gi best mulig informasjon om fenomenet (Jacobsen, 2000). Dette kriteriet ble vektlagt slik at vi kunne oppnå en dybdeforståelse om temaet og dermed være i stand til å besvare vår problemsstilling.

Når vi kontaktet selskapene forklarte vi temaet for avhandlingen og spurte om å bli henvist til personer som kunne oppfylle vårt kriteriet. Vi foretok kontinuerlig en vurdering hvorvidt de gjennomførte intervju var tilstrekkelig eller om det var behov for flere informanter for å besvare problemsstilling. Totalt ble det gjennomført 14 intervjuer, hvorav to av selskapene ble intervjuet ved to anledninger med ulike informanter. Grunnen til dette var at selskapet hadde flere personer som kunne bidra med informasjon og relevant kunnskap om temaet. Etter å ha gjennomført 14 intervjuer opplevde vi et metningspunkt, og vi besluttet at dette var tilstrekkelig datagrunnlag for å kunne besvare problemstillingen. Vi mener at våre funn er

utfyllende og dekkende samt belyser ulike perspektiver og fortolkninger av fenomenet. Ettersom det er kvalitet som er formålet med vår tilnærming, og ikke kvantitet, anså vi dette som tilstrekkelig.

Informantene besto av fagpersoner med kompetanse innen sikring, beredskap og/eller helse, miljø og sikkerhet (HMS), noe som kan ses i sammenheng med hvordan sikring er organisert i virksomheten. I noen av virksomhetene er sikring underlagt HMS - avdelingen, mens i andre virksomheter er det etablert en egen enhet for sikring. Vi anså ikke dette som en ulempe, men heller som en mulighet til å få frem ulike perspektiver i forhold til temaet. Det var heller ikke gitt at informantene hadde samme kunnskapsnivå i forhold til emne, men vi anså at deres bakgrunn og erfaring likevel kunne være nyttig i forhold til å belyse problemstilling. I utgangspunktet var det kun en informant fra hver virksomhet som ble intervjuet, med unntak av to intervjuer hvor virksomheten ønsket å stille med flere informanter. Disse hadde ulike roller tilknyttet sikringsarbeidet i virksomheten, og kunne dermed utdype ulike aspekter av fenomenet. Vi anså derfor dette som en god mulighet til å innhente mer kunnskap og informasjon om virksomhetens sikringsarbeidet og syn omkring utvikling av sikringskultur. Vi erfarte at informantene var samkjørte i sine oppfatninger og svar, og disse intervjudataene ble benyttet på lik linje som de andre intervjuene. Nedenfor vises en oversikt over informantene.

Informant	Fagområde	Antall informanter	Varighet for intervju	Dato for intervju
A	Safety & Security	1	Ca 1 time	26.03.2015
B	Security	1	Ca 1 ½ time	07.04.2015
C	Security	3	Ca 1 ½ time	08.04.2015
D	Security	1	Ca 1 ½ time	10.04.2015
E	Security	1	Ca 1 time	13.04.2015
F	Security	1	Ca 1 ½ time	15.04.2015
G	Security	1	Ca 1 ½ time	16.04.2015
H	Security	2	Ca 1 ½ time	23.04.2015
I	Security	1	Ca 1 time	27.04.2015
J	Security	2	Ca 1 ½ time	27.04.2015
K	Security	1	Ca 1 ½ time	04.05.2015
L	Security	1	Ca 1 ½ time	06.05.2015
M	Safety & Security	1	Ca 1 ½ time	08.05.2015
N	Security	1	Ca 1 time	11.05.2015

Tabell 2: Oversikt over informanter

3.3 Etiske betraktninger

Gjennom hele studien var det viktig at vi opptrådde i tråd med forskningsetiske retningslinjer, samt opparbeidet tillit mellom oss og informantene. Ifølge Kvale & Brinkmann (2009) bør man i kvalitativ forskning arbeide ut ifra tre etiske regler:

1) Informert samtykke

For å opptre i tråd med forskningsetiske retningslinjer ble informant i forkant av intervjuet tilsendt informert samtykke (Vedlegg 1). Dette inneholdt informasjon om formål, bakgrunn for studien samt hva deltakelse ville innebære for virksomheten. I tillegg ble det tydeliggjort at deltakelse var frivillig. Her ble blant annet spørsmål om anonymitet og konfidensialitet behandlet. Ettersom noen av virksomhetene stilte ulike

betingelser til å delta, tilpasset vi innholdet i dokumentet for å ivareta disse betingelsene.

2) Konfidensialitet

En forskningsetisk utfordring vi måtte ta stilling til var spørsmålet om konfidensialitet, som dreier seg om at data som kan identifisere informantene ikke avsløres i avhandlingen (Kvale & Brinkmann, 2009). På bakgrunn av at enkelte av informantene og virksomhetene stilte krav om full anonymitet, besluttet vi lik beskyttelse av alle informantene. Ettersom hensikten var ikke å utpeke hver enkelt virksomhet, anså vi ikke dette som en ulempe, heller en styrke ved at det kan ha bidratt til mer ærlige svar med hensyn til at sikring er et sensitivt tema. Alle personopplysninger og informasjon som kunne identifisere virksomheten ble dermed anonymisert under transkribering av intervjuene. Informantene er gitt bokstavbetegnelsene A til N, og er uavhengig av kjønn gitt betegnelsen "han".

3) Konsekvenser

I studien vurderte vi mulige fordeler og ulemper som deltakelse i forskningsprosjektet kunne medføre for informantene. Vi opplevde at informantene var svært positive til å delta i forskningsprosjektet, og ettersom vi sikret full anonymitet av både virksomhet og informant, anså vi ulempene for den enkelte som svært lav. Videre kan informantene selv dra fordel av resultatene fra forskningsprosjektet ved å oppnå økt kunnskap om fenomenet.

3.4 Gjennomføring av intervju

Alle informantene ble tilbudt å få tilsendt intervjuguide (Vedlegg 2) på forhånd. Enkelte ønsket dette, mens andre anså ikke dette som nødvendig. Vi så ikke dette som et problem, da det kan være både fordeler og ulemper med å få intervjuguide på forhånd. På den ene siden kan det bidra til mer reflekterte og gjennomtenkte svar, samtidig kan det tenkes å bidra til passivisering og innskrenkning av svarene. Vi registrerte likevel ingen vesentlig forskjell på kvaliteten på de innsamlede data, med hensyn til hvem som fikk tilsendt intervjuguide på forhånd eller ikke.

Selve intervjuprosessen startet med et testintervju med en av de utvalgte virksomhetene. Her vurderte vi hvorvidt intervjuguiden var funksjonell i forhold til å

besvare problemsstillingen og forskningsspørsmålene. I tillegg for å sikre gyldige data (Jacobsen, 2000), anså vi det som viktig at informanten forsto intervjuspørsmålene slik som tiltenkt. I etterkant av intervjuet gjorde vi noen få endringer, deriblant omformulering av spørsmål som fremsto som noe uklare for den aktuelle informanten.

I hvert av intervjuene presiserte vi innledningsvis hva som var formålet med intervjuet, samt at vi foretok en begrepsavklaring slik at informantene var inneforstått med hva vi mente med begrepene sikring og sikkerhet. Dette ble gjort for unngå misforståelser og uklarheter omkring begrepene.

Alle intervjuer med unntak av to, fant sted hos den aktuelle virksomhet. De øvrige intervjuene foregikk over telefon og videokonferanse, grunnet ønske fra virksomheten eller av praktiske grunner. Noen informanter ønsket å benytte powerpoint presentasjoner for å illustrere og utdype sitt arbeid med sikringskultur, noe vi anså som en mulighet til å få økt forståelse og innsikt i virksomhetens syn omkring fenomenet.

Dersom godkjent ble det benyttet båndopptaker under selve intervjuet. Vi anså dette som hensiktsmessig for å ivareta detaljene i dataene samt at vi i større grad var i stand til å fokusere på intervjuobjektet (Jacobsen, 2000). Dette ga oss mulighet til å gjengi mer direkte informantenes utsagn, og dermed redusere mulighet for feiltolkning og feilangivelser. Bruk av båndopptaker ble godkjent av alle informantene med unntak av en, hvor det ble tatt notater under intervjuet. Alle intervjuene med unntak av ett ble gjennomført på norsk. Ett av intervjuene ble gjennomført på engelsk, noe som medførte at vi måtte oversette intervjuguiden og dataene til norsk.

Avslutningsvis i intervjuene ble det foretatt en oppsummering, samt ble informantene spurt om vi kunne kontakte dem i etterkant dersom uklarheter eller andre spørsmål dukket opp.

3.5 Dataanalyse

Etter intervjuene ble data transkribert fra muntlig til skriftlig form. Til tross for at dette er en tidkrevende oppgave, bidro dette til å strukturere intervjuene og på denne måten letteregjøre analysearbeidet (Kvale & Brinkmann, 2009). En utfordring med transkribering er at setninger til informantene kan ofte være ufullstendige, hvor det i noen tilfeller kan være vanskelig å tolke meningen. I noen tilfeller innebar det også at vi måtte oversette fra dialekt til bokmål. Vi er likevel av den oppfatning at dette ikke har vært noe problem for avhandlingens resultater.

Vi benyttet oss av en abduktiv forskningsstrategi basert på Danemark, Jacobsen og Karlsson (1997) sin tilnærming. I en slik tilnærming blir teori brukt som utgangspunkt, hvor vi har relatert sikringskultur som begrep og som fenomen til de teoretiske rammene beskrevet tidligere, for så å utarbeide en ny tolkning og beskrivelse av fenomenet. Det bør det påpekes at dataene blir analysert ut ifra valgt teori og dette kan ha hatt noe å si for resultatene av forskningen (Blaikie, 2010). Videre bør det påpekes at tolkning og reduksjon av kvalitative data er svært utfordrende, hvor de innsamlede data har måtte blitt avgrenset og strukturert for å kunne besvare problemstillingen. De kvalitative dataene som har blitt samlet inn under studien må forstås som et produkt av våre fortolkninger som forskere, hvor vår forforståelse spiller inn i prosessen (Blaikie, 2010).

3.6. Styrker og svakheter ved forskningsdesignet

Det er viktig at vi kritisk vurderer kvaliteten til dataene som er samlet inn ved å drøfte både validitet (gyldighet) og reliabilitet (pålitelighet) (Jacobsen, 2000). Vi har fra starten av forskningsprosjektet vårt vært bevisste og systematiske i forhold til de valgene vi har tatt for å sikre mest mulig gyldige og pålitelige data. Vi vil i det følgende gjennomgå styrker og svakheter ved forskningsdesignet vårt.

Validitet dreier seg om de dataene vi har samlet inn bidrar til å besvare vår problemstilling eller ikke (Jacobsen, 2000). For å sikre valide data besto utvalget av fagpersoner med relevant kompetanse og kunnskap innenfor sikkerhet- og sikringsfeltet. Noen informanter hadde sikring som sin hoved arbeidsoppgave, mens andre hadde sikring som del av sine bredere HMS - relaterte arbeidsoppgaver. Vi

anser ikke dette som en svakhet, heller en styrke ved å inkludere ulike perspektiver fra fagpersoner som er tilknyttet sikringsarbeidet.

I forhold til å sikre valide data har vi vært avhengig av informantenes kunnskap og bidrag omkring temaet sikringskultur samt antall informanter. En mulig svakhet ved studien kan være at noen av informantene hadde lite kunnskap eller kjennskap til kulturbegrepet og dette kan ha begrenset hvorvidt deres besvarelser bidro til å belyse problemstillingen. Samtidig mener vi at vi har fått svært interessante funn gjennom de innsamlede data ved å ha inkludert en rekke selskaper og informanter.

Intervjuguiden ble utarbeidet med det formål at det skulle gi intervjuene troverdighet og sikre at de aktuelle temaene ble dekket. Intervjuguiden ble benyttet i alle intervjuene, igjen for å sikre validitet (Jacobsen, 2000) og forsikre at hver informant besvarte de samme spørsmålene. Det må påpekes at intervjuene ble noe ustrukturert, hvor spørsmålene ble gjennomgått i ulik rekkefølge fordi informantene fikk anledning til å styre samtalen til en viss grad selv. Dette medførte at det oppsto variasjon i hvordan intervjuene foregikk og hvilke emner fikk mest fokus. Ved å kontinuerlig vurdere hvorvidt alle spørsmålene var besvart, sørget vi for at alle emnene ble dekket. I følge Jacobsen (2000) er det viktig å validere hvorvidt fagpersonene opplever konklusjonene vi tar som riktige. Dermed ble informantenes fortolkninger og uttalelser kvalitetsikret ved hjelp av oppfølgingsspørsmål, samt ble det foretatt oppsummering både underveis og i slutten av intervjuet, hvor eventuelle misforståelser kunne avdekkes.

Transkribering av dataene ga oss mulighet til å kvalitetssikre våre egne tolkninger og har dermed bidratt til å øke validiteten. I tillegg kunne vi gjengi sitater direkte i avhandlingen, noe som øker påliteligheten og dermed troverdigheten til resultatene (Kvale & Brinkmann, 2009). I ett av intervjuene tok vi begge notater i stedet for å benytte båndopptaker etter ønske fra informant. I etterkant ble notatene kvalitetssikret ved å sende de til informant for godkjenning og oppklaring av eventuelle misforståelser. Dette bidro til å øke validiteten til dataene. Ettersom ett av intervjuene ble gjennomført på engelsk var vi nødt til å foreta en oversettelse til norsk under transkribering. En utfordring her er muligheten for feiltolkninger, noe som kan påvirke validiteten til dataene.

I forhold til valg av teori, har vi i stor grad benyttet oss av teori fra sikkerhetskultur-feltet, grunnet mangel på litteratur om sikringskultur. Ved at sikkerhetskultur er et svært utforsket felt har vi vært nødt til å foreta noen avgrensinger, noe som innebærer at andre teorier blir utelukket. Dette vil ha betydning for forskningens resultater, da funnene har blitt analysert opp mot valgt teori. Likevel mener vi at ved benytte oss av Jeffcott et al. (2006) sine elementer har vi benyttet en teori som sammenfatter mye litteratur både fra sikkerhetskultur og HRO-feltet. Videre har vi supplert med tilgjengelig litteratur fra sikringskultur-feltet, blant annet "Information security culture." Ettersom formålet har vært å bidra til en økt innsikt og forståelse omkring sikringskultur, mener vi at ved å analysere våre funn opp mot det teoretiske rammeverket har vi utarbeidet en ny tolkning og beskrivelse av sikringskulturfenomenet, og vært i stand til å besvare problemstillingen.

Samtidig bør det påpekes at kultur er et svært omfattende område, hvor det finnes utallige definisjoner, forståelser og perspektiver på hva kultur er og hvordan det bør måles og studeres. Vår forståelse av kultur og valg av teorier vil også her spille inn på resultatene. Samtidig er kultur noe som er lite håndfast og målbart, noe som medfører at tolknings- og struktureringsarbeidet er svært krevende.

3.7 Noe vi ville gjort annerledes?

Det kan tenkes at det kunne ha styrket avhandlingen ved å også inkludere myndighetenes syn på sikringskultur og på denne måten fått fram flere perspektiver omkring fenomenet. Likevel på grunn av tidsmessig og ressursmessige grunner lot ikke dette seg gjøre, og dermed ble avhandlingen avgrenset til operatørselskapenes syn.

3.8 Oppsett av funn

Våre funn er presentert ved hjelp av avhandlingens tre forskningsspørsmål, som videre er inndelt i forhold til hovedtemaer. Dette ble gjort for å sikre at problemstilling ble besvart og at funnene ble avgrenset i forhold til hva som er formålet med avhandlingen.

1. *Hva legger operatørselskapene i begrepet sikringskultur og hvorvidt benyttes begrepet i virksomhetens sikringsarbeid?*
2. *Hvilke elementer oppfattes som viktige i arbeidet med å utvikle en "optimal" sikringskultur?*
3. *Hvilke utfordringer opplever operatørselskapene i arbeidet med å utvikle en slik kultur?*

4.0 Empiri

I det følgende vil vi presentere resultatene fra forskningsprosjektet vårt. Disse er presentert og strukturert i henhold til forskningsspørsmålene.

4.1 Hva legger operatørselskapene i begrepet sikringskultur og hvorvidt benyttes begrepet i virksomhetens sikringsarbeid?

I det følgende vil vi presentere hvorvidt sikringskulturbegrepet benyttes, samt de ulike forståelsene og tolkningene av kultur og sikringskulturbegrepet. Avslutningsvis vil vi presentere hva som anses av informantene som en optimal sikringskultur, hvor vi har delt empirien inn i følgende hovedtemaer: sikringsbevissthet og kompetanse, ansvarsfølelse og etterlevelse av prosedyrer.

4.1.1 Bruk og ikke bruk av begrepet sikringskultur

I resultatene fremgår det at en rekke av informantene benytter begrepet sikringskultur i ulik grad i sikringsarbeidet, mens andre ikke har et bevisst forhold til det. En del av informantene benytter i stedet begrepet sikkerhetskultur som et overordnet begrep, hvor sikring inngår. En av informantene viser derimot til at de hverken benytter begrepene sikkerhetskultur eller sikringskultur, men snakker heller om en organisasjonskultur. Generelt ser vi at det er ingen som har eksplisitt definert begrepet, til tross for at flere benytter det i sitt sikringsarbeid. I forhold til bruken av begrepet, er det enkelte av informantene som benytter dette aktivt og eksplisitt som del av sikringsarbeidet, hvor begrepet blant annet blir brukt i presentasjoner, brosjyrer, HMS program osv. Andre viser til begrepet security awareness som en del av sitt HMS program, hvor dette anses som sentralt i utvikling av en sikringskultur.

Organisering av sikring	Bruk av begrepet sikringskultur
Egen enhet for sikring	Ja
Egen enhet for sikring	Ja
Sikring underlagt HMS	Ja
Sikring underlagt HMS	Ja
Sikring underlagt HMS	Ja
Sikring underlagt HMS	Ja
Sikring underlagt HMS	Ja
Sikring underlagt HMS	Nei
Sikring underlagt HMS	Nei
Sikring underlagt HMS	Nei
Sikring underlagt HMS	Nei
HMS avdeling	Nei

Tabell 3: Bruk av begrepet sikringskultur

Som vist i tabell 3, benyttes sikringskulturbegrepet både av virksomheter som har opprettet en sikrings- og beredskaps-avdeling underlagt HMS, og virksomheter som har etablert en egen enhet for sikring. Alle av disse virksomhetene har ansatt minst én person til å arbeide med sikring på fulltid. De som ikke benytter begrepet er både virksomheter som enten har en egen sikrings- og beredskapsavdeling underlagt HMS, eller virksomheter som ikke har en egen sikringsavdeling, men hvor HMS avdelingen også omfatter sikring. Alle utenom en av disse virksomhetene hadde ansatt minst en person til å arbeide med sikring på fulltid. Dermed fremkommer det at organisering av sikkerhet- og sikringsarbeidet ikke er avgjørende for om sikringskultur begrepet benyttes i virksomheten eller ikke.

4.1.2 Kulturbegrepet

I spørsmålet om hva informantene legger i begrepet sikringskultur, er det flere som viser til en generell forståelse av kultur, hvor kultur blir ansett som "måten vi gjør ting på her hos oss". Informant C meddeler at:

> *"Kultur er den måten du lærer det videre til nyansatte på, (...) det er en måte å gjøre ting på her hos oss (...) Sånn ser vi det. Også selvfølgelig og i denne store sammenheng, hvordan vi tilpasser den rette måten å gjøre ting på, i forhold til de rammene som omgivelsene gir oss.*

Videre meddeler flere av informantene at kultur kan ses på som noe felles, noe som definerer virksomheten, "hvem er vi?" Informant I hevder at kultur er en måte å leve etter, og være enig om, som igjen er basert på verdier og holdninger. Enkelte av informantene viser til at virksomheten ikke har et tydelig forhold til kulturbegrepet. Informant H viser til en forvirring omkring begrepet sikringskultur og sier i det følgende: *"Men vi har ikke hatt noe kultur. Vi har hatt sikring, men vi har ikke hatt noe begrepskultur, vi har hatt mer en begrepsforvirring, for den er aldri blitt beskrevet for å si det sånn da."* Informant J knytter sikringskultur begrepet til Sun Zi sitt verk "kunsten å krige", som går ut på at krigen skal vinnes lenge før slaget har begynt.

4.1.3 Sikringskultur som en del av HMS kulturen

I empirien fremkommer det at 5 av 12 av virksomhetene ikke benytter begrepet sikringskultur i sikringsarbeidet. Til tross for dette har flere en oppfatning av begrepet. Informant A påpeker at han oppfatter begrepet som en "spinn-off" av sikkerhetskultur, der han ser en beslektning mellom begrepene. Han forklarer det slik:

> *Det har jo med hva som er innenfor HMS kultur eller sikkerhetskultur, altså at det har noe med å følge regler, å ha et aktivt forhold når du gjør avvik i forhold til regler, det har med holdninger, det har med, du er også inne på verdier, og atferd. Og dette blir jo da kollektivt, det er et samlebegrep, som da tilhører bedriften.*

Informanten knytter dermed sikringskulturbegrepet til HMS kultur, hvor fokus er på kollektive verdier, holdninger og atferd. Videre meddeler informant A at virksomheten benytter kun begrepet "sikkerhetskultur", men hvor det påpekes at "S" i "HMS" har tre betydninger; *sikkerhet, sikring* og *samfunnsansvar.* Også informant E skiller ikke spesifikt mellom sikkerhetskultur og sikringskultur. Han forklarer det slik*:*

> *Kultur for sikringsarbeidet er som kultur for resten av det HMS arbeidet som vi egentlig driver med. Hos oss er HMS, det er SSHE (...) Hos oss, spør du meg, så er kultur med på alt det her, og det betyr at når du kommer med koppen din og en veske, (...) så skal vi ha en kultur for at jeg sier ifra, også skal vi ha en kultur der du tenker at "så bra at han sa ifra for det tenkte ikke jeg på.*

Begrepene blir dermed ikke ansett som adskilte, og begge informantene viser til at sikring ses på som en del av det totale HMS arbeidet. Informant E påpeker: *"Altså, security for oss, sikring, er en del av hele HMS faget. Så sånn sett kan du si at da blir ikke security spesielt"*.

4.1.4 Bevisst bruk av begrepet sikringskultur

Resultatene viser at 7 av 12 av virksomhetene bruker begrepet sikringskultur, der flere er av den oppfatning at det er hensiktsmessig å skille mellom sikringskultur og sikkerhetskultur. Det fremkommer i empirien at de som bruker begrepet vektlegger i stor grad holdninger, verdier og atferd, og hvilken betydning kultur har for sikringsarbeidet. Informant I meddeler at selskapet benytter begrepet og tolker det slik: "*Så sikringskultur vil jeg si er en sånn felles tankegang (...) at en enes om en felles forståelse og en holdning til hvordan ivareta personell og informasjon og bygg og sånt, og sikre oss mot uønskede hendelser."* Her vektlegges en felles forståelse for sikringsarbeidet i organisasjonen som skal bidra til å øke sikringsnivået. Informant G vektlegger også dette og påpeker:

> *Det er holdninger og atferd, innen et fagfelt som security, som skaper kulturen. Atferden, hva du faktisk gjør. De holdninger du har med deg, den atferden du utviser, og det kommer gjerne som er resultat av den kunnskapen du har.*

Her inkluderes også kunnskap som et viktig element. I forbindelse med begrepet nevner et flertall at innenfor sikkerhetskultur har man kommet langt, i motsetning til utvikling av en sikringskultur, noe som igjen viser at informantene skiller mellom begrepene. Informant B forklarer det slik:

Som oljeselskap er vi veldig gode på sikkerhetskultur, og har en lang tradisjon med denne den klassiske HMS greia, men sikring der er vi ung. Der ble vi "konfirmert" ved In Amenas ulykka. (...) For det første kultur bygger ikke du over natten, du vedtar det heller ikke. Det handler om eksponering for security terminologi, og forståelse for hva det handler om over tid. Så på samme måte som safety, altså sikkerhetskultur, og det er veldig solid i selskapet nå. Og det har tatt, ja 40 år.

Videre hevder informanten at det skilles mellom sikkerhetskultur og sikringskultur i høyeste grad og forklarer dette som følgende: *"Rett og slett fordi det er villede, ondsinnede handlinger, ikke sant? Som prinsipielt skiller oss fra safety issues."*

4.1.5 Ett begrep - organisasjonskultur

Informant M fremhever at virksomheten hverken bruker begrepene sikkerhetskultur eller sikringskultur, men snakker heller om èn organisasjonskultur. Han sier det slik:

Vi har jo en kultur i vår bedrift, kall det gjerne organisasjonskultur da, og den dekker på en måte alle fagfelt, så vi har faktisk ikke et eget begrep som vi kaller for sikringskultur, for det er inkludert i vår kultur. (...) altså vi har en kultur, og den skal dekke alt. Men det vi liker å snakke om i den sammenheng er likevel security awareness, bevisstgjøring.

Fokuset er dermed ikke rettet mot å utvikle en såkalt sikringskultur, heller å bygge sikringsbevissthet inn i selskapets organisasjonskultur.

4.1.6 Oppfatninger om hva som anses som en optimal sikringskultur

Sikringsbevissthet og kompetanse

I forhold til begrepet sikringskultur blir bevissthet eller "awareness"og kompetanse ansett som sentralt. En av informantene kaller det en "security awareness kultur*",* mens en annen informant påpeker at "security awareness" må bygges inn i organisasjonskulturen. Informant B vektlegger også security awareness og forklarer det slik:

(...) i ordet awareness tror jeg det ligger ganske mye av nøkkelen til kultur. Folk må ta det inn og dem må tenke security når dem ser en pakke som står i resepsjonen eller en person en ikke har sett før, eller nå var det var det et avvik fra normalen her. Ikke sant? Altså, når folk begynner å se sånt og tenker gjennom sånne briller da har vi nok oppnådd litt sikringskultur.

Også informant F vektlegger security awareness og sier i det følgende: *"Security awareness – den setter jeg veldig høyt opp på den lista. En har kommet svært langt når en opplever at de ansatte sier ifra hvis du ser "noe som skjer", eller er uvanlig, og har dette litt i bakhodet i arbeidsdagen sin."* Videre påpekes det at awareness henger sammen med kompetanse, hvorav disse er gjensidig forsterkende. Informant B forklarer det slik: "*Fordi du lærer noe også blir du aware. Eller hvis du blir aware på noe, så kan du lære det mer."* Informant K vektlegger også kompetanse, samt forståelse og en viss mental kapasitet og at dette kan føre til at de ansatte reagerer dersom det oppstår avvik fra normalen. Dermed blir mindset og tankegangen til hele organisasjonen satt i fokus i forhold til sikring. Videre vektlegges det at denne tankegangen bør komme innenfra ved at man innehar en forståelse for hvorfor sikring er viktig. Informant K fremhever "(...) *alle ansatte har en rolle å spille i sikringskultur i større eller mindre grad (...) Det som er viktig er at sikringstankegangen, at den kommer naturlig."*

Det fremkommer i empirien at de som benytter sikringskulturbegrepet synes å vektlegge sikringsbevissthet i større grad en de øvrige informantene, med unntak av informanten som fremhever at fokuset deres er å bygge sikringsbevissthet inn i organisasjonskulturen.

Ansvarsfølelse

Ansvarsfølelse og forståelse blir også trukket frem i forhold til hva som legges i begrepet sikringskultur. Informant C forteller om hvordan virksomheten arbeider ut ifra selskapets verdier der fokus er på å bygge en kultur hvor alle skal få et felles ståsted. Flere av informantene fremhever hvor viktig det er at folk bryr seg om sikring og tar ansvar for sikringen, både i forhold til selskapets beste, men også for de ansatte. Informant D forklarer det slik: "*Jeg vil si det er optimalt hvis du får folk til å bry seg, og lære seg å bry seg om. Ikke bare bry deg om kollegaene dine, at du faktisk har et*

ansvar, ikke bare deg selv." Informant I enes i dette og anser det som optimalt når folk tar ansvar og bryr seg og virkelig ønsker å beskytte selskapets verdier og sine kollegaer. Informant L snakker om ansvarsbevissthet som sentralt i forhold til sikringskulturbegrepet og forklarer det slik:

> *Det som jeg mener er mest viktig å få gjennom til de ansatte at de ansatte har et ansvar her, at de er ansvarsbevisst. Og da mener jeg at hvis vi som bedrift klarer å få det gjennom, alle ansatte, at de har en forståelse for den ansvarsbevissthet, da mener jeg at det er en, at det er vellykket.*

Flere av informantene fremhever dermed at de ansatte må ta sikring på alvor, og at sikringskultur handler om å bry seg. Det fremkommer i resultatene at de som bruker begrepet synes å vektlegge dette. Enkelte av informantene som ikke benytter begrepet nevner holdninger som viktig, men utdyper ikke i særlig grad hvilke type holdninger som anes som ønskelige i en sikringskontekst.

Etterlevelse av prosedyrer

Flere av informantene fremhever at en optimal sikringskultur kjennetegnes av at de ansatte følger gjeldende regler og prosedyrer og ikke tar snarveier. Spesielt èn av virksomhetene vektlegger i stor grad atferd i forhold til begrepet sikringskultur, hvor de ansattes etterlevelse av krav og regler er i fokus. Informant E sier det slik: *"Den ansatte generelt bidrar ved å følge reglene (...) Alt vi gjør er risikobasert. Og vi har regler og systemer for alt. Følger du reglene, så i utgangspunktet så skal det gå bra."*. Informant A fremhever også dette i forhold til hva som er optimalt: *"Ja da ville jeg sagt at folk følger reglene, at det er få avvik fra reglene, og at dersom det er avvik blir disse behandlet."* Informant K anser også viktigheten av å etterleve fastsatte krav, men påpeker at kultur er mer enn dette. Han forklarer det slik: "*Kultur og compliance henger veldig tett sammen egentlig. Men kultur løfter det et steg videre, en tenker selv."* Til tross for at etterlevelse anses som viktig, fremhever flertallet av informantene at kultur er mer enn kun å følge regler.

4.1.7 Relevante trusler

I empirien fremheves viktigheten av å ha en risikobasert tilnærming til styring av sikringsrisiko, hvor tiltak må være tilpasset det gjeldende trusselnivået. Dette kobles av flere til sikringskulturbegrepet. Det fremkommer variasjon i forhold til hvilke trusler informantene fokuserer på, samtidig som resultatene viser at virksomhetene generelt står ovenfor et bredt spekter av trusler. Flere av informantene påpeker at de baserer seg i stor grad på informasjon de får av PST og NSM. Generelt har virksomhetene delt sikring inn i tre områder; informasjonssikkerhet, personell sikring og fysisk sikring, som videre er ofte knyttet til ulike avdelinger. Informant B hevder at de har trusler innenfor hvert av de tre domenene, og at disse kan operere på tvers. I forhold til hva som anses som relevante trusler for virksomhetene nevnes blant annet innside trusler, sabotasje og skade på utstyr, IT trusler, tyveri, aktivister, herunder Non governmental organizations, samt terrorisme. Hovedsakelig fremkommer det at flertallet av informantene ser på informasjonssikkerhet, herunder IT trusler som en av de største truslene. Informant E omtaler trusselbildet i Norge på følgende måte:

> *Vi ser et stabilt demokratisk system, det er ingen plan om å legge ned her, så dette her med, kan du si, illojale ansatte eller den type ting, er ikke så aktuelt som når du er i en omstilling, nedleggelsesfase. Så for vår del, kan du si at den største trusselen, for vår del, det er cyber. Det er den største. Det er en på en måte utsatt for hele tiden. Men det er klart at, altså, etterretningsvirksomhet er alltid en utfordring.*

Informant B vektlegger også informasjonssikkerhet og forklarer at informasjonstyveri kan få svært alvorlige konsekvenser, han forklarer: "*(...) cyber domenet, selvfølgelig veldig viktig domene for både å miste informasjon, men også for potensielt sabotasje, ødelegge utstyret vårt, komme inn i prosess-systemene våres."* Han sier videre: "(...) *terrorisme selvfølgelig, som resten av den vestlige verden er vi også eksponert. Ikke nødvendigvis direkte i det daglige, men ja det er ingen av disse truslene her som er irrelevante."* Det fremkommer variasjon i forhold til hvorvidt informantene ser på terrorisme som en relevant trussel, hvor noen av informantene vektlegger at Norge er et lavrisiko land.

4.1.8 Betydning av sikringskultur for sikringsnivået

Det synes at kultur anses av de fleste som et viktig verktøy for å sikre seg mot intenderte uønskede hendelser. Likevel har informantene ulikt fokus på hvordan kulturen er med på å støtte opp sikringen i selskapet, samt hvilket behov virksomheten har for å videreutvikle kulturen. Informant I påpeker hvor viktig det er å inkludere menneskefaktoren, ut over de tekniske og fysiske barrierene:

> *Kultur betyr, det er nå viktig at en, det har en viktig betydning for en er nødt til å bry seg da. Og en kan bygge mange barrierer, en kan sette opp mange gjerder og låste dører osv. og systemer i forhold til IT da, men det hjelper nå lite hvis ikke personell da på en måte bruker og forstår hvordan de skal bruke det og hvorfor de skal følge en felles standard. Så det er på en måte vårt verktøy for å få folk til å gjøre sånn som vi vil at de skal gjøre for selskapet da, for å sikre selskapet.*

Flere fremhever kultur som grunnleggende for sikringsarbeidet. Informant A meddeler:

> *Det er viktig, og det henger også litt sammen med sikkerhet. Jeg ser de ikke som adskilt. For det har jo med HMS og HMS holdninger å gjøre. Og da er det viktig at holdningene er bra for du kan ikke kontrollere alt. Så må du stole på at folk gjør det riktige og at de har det riktige nivået.*

Informant D anser også viktigheten av kultur :

> *(...) for meg så er det basis i sikring (...) Mangler du kultur, har du heller ingen sikring. (...) Vi kan aldri sikre oss 100%, det er ikke fysisk mulig. Vi har med mennesker å gjøre, mennesker er vår sterkeste og svakeste ressurs, det er vår styrke, det er vår svakhet.*

Flere av informantene fremhever dermed at kultur er helt avgjørende for sikringen i virksomheten.

Oppsummering

Som det fremgår i empirien, ser vi en variasjon både i forhold til innehold, betydning og hvorvidt sikringskulturbegrepet benyttes. Enkelte av selskapene ser på sikring som en del av selskapets HMS kultur og benytter dermed ikke begrepet sikringskultur eksplisitt i sitt sikringsarbeid. Andre har derimot et mer bevisst forhold til begrepet, hvorav noen bruker begrepet mer aktivt enn andre. Ingen av informantene eller virksomhetene kunne vise til en eksplisitt definisjon av begrepet, til tross for at begrepet blir av noen brukt i sikringsarbeidet. Likevel har flere gjort seg opp noen oppfatninger og meninger om begrepet, der noen av fellestrekkene er at kultur i stor grad omfatter kollektive holdninger, verdier og atferd, samt at det er "måten vi gjør ting på her hos oss". Dette blir av noen koblet opp til sikringsarbeidet, eller til det bredere HMS arbeidet. Det fremkommer uklar terminologi i forhold til begrepene sikkerhet og sikring, hvor noen synes å bruke dem som to adskilte begreper for safety og security. Andre ser på sikkerhet som et overordnet begrep, der både safety og security inngår. Resultatene viser videre at informantenes fokus varierer; noen fokuserer på atferd og handlinger til ansatte, mens andre vektlegger i større grad verdier og holdninger. Essensen i sikringskulturbegrepet synes å være sikringsbevissthet ("awareness") og forståelse, hvor sikringskultur handler om at ansatte bryr seg og tar ansvar for sikring, samt at denne tankegangen kommer naturlig.

4.2 Hvilke elementer oppfattes som viktige i arbeidet med å utvikle en "optimal" sikringskultur?

I resultatene fremgår det at få av selskapene har en klar og tydelig strategi eller tilnærming for å utvikle en såkalt sikringskultur. Likevel kommer det generelt frem at selskapene gjennomfører ulike tiltak og initiativer som kan bidra til å utvikle en kultur som støtter opp det totale sikringsarbeidet og sikringsnivået til virksomheten. I det følgende vil vi presentere hvilke elementer som vektlegges som viktig for å kunne utvikle en slik kultur, som det fokuseres på i ulik grad. Empirien struktureres ved hjelp av vårt teoretiske rammeverk, herunder de forhåndsdefinerte elementene; *forpliktelse, fleksibilitet, læring* og *tillit.*

4.2.1 Forpliktelse

Alle informantene fremhever ledelsens forpliktelse som helt nødvendig dersom man skal utvikle en optimal sikringskultur. Informant G forklarer det slik: *"Ledelsesforpliktelse er alfa omega. Det er de som styrer retningen på skuta."* Informant A understreker også viktigheten av å få sikring forankret hos ledelsen, hvor ledere blir ansett som rollemodeller for resten av organisasjonen. Informant B beskriver lederen som en "katalysator" for utvikling av en sikringskultur og sier i det følgende:

> *Det er derfor det er så viktig at vi har toppledelsen om bord, og det er vi heldige med som vi har i Selskapet. Toppledelsen tar dette med rammeste alvor. Så folk blir fulgt opp på security nedover i linja. For alle ledere på alle nivåer er accountable for sin egen security.*

Informant E enes også i dette og meddeler at:*"Får du med deg sjefen og de andre underanbudene ser at han er opptatt av dette, blir også de opptatt av dette, og da kan du begynne å klarte ned til du kommer til gulvet."* Her påpekes at dersom ledelsen er forpliktet til sikring vil dette forplante seg nedover i organisasjonen.

Flere av informantene påpeker at ledere er viktige kulturbærere i virksomheten, hvor deres handlinger, holdninger og verdier gjenspeiles i resten av organisasjonen. Informant E meddeler:

> *Men når det gjelder sikring igjen, dette med verdier og dette med at du får folk med deg, opplæring, trening, kultur inn i selskapet er. Beste å se kulturen i selskapet er å gå å se på de øverste ledernivåene, så vil du få svaret egentlig.*

Informant I fremhever at ledelsens må ta ansvar og eierskap til sikring, hvor dette anses som et "middel" for å få alle ansatte til å "skjerpe seg" og være bevisst omkring sikring. Flere av informantene forteller at de bruker dermed mye tid på å få sikring forankret hos ledelsen, ved å blant annet holde sikringsbriefer for dem. Informant B forteller:

> *(...) og den som har rolle som security professional rundt i omkring i selskapet, de er engasjert i sitt eget forretningsområde og holder briefings,*

(...) og tar opp security tematikk jevnlig, for å få inn ledelsen, fordi ingenting av det vi har snakket om idag fungerer hvis ikke ledelsen har buy-in. (...) sant så ledelsedelen og interaksjonen med dem er nøkkelen tror vi da. Og få security budskapet ut til alle.

Her kommer det frem at samhandlingen mellom ledelsen og dem med sikringsrelaterte arbeidsoppgaver spiller en viktig rolle til å øke forpliktelse til sikring hos ledelsen. Det blir blant annet påpekt viktigheten av at ledelsen er informerte i forhold til trusselbildet, da det er de som tar sikringsrelaterte beslutninger. Informant E forklarer: *"De som trenger å vite noe, det er ledelsen. For ledelsen tar til enhver tid informerte beslutninger. Noen ganger lar de være å beslutte, som er å beslutte, og det betyr at de må vite hva som foregår."*

En av informantene meddeler også betydningen av at ledere tar temaet sikring opp på lik linje som sikkerhet på allmøter. Han mener dermed at ledere må demonstrere tydelig sitt engasjement og forpliktelse til sikring, ikke kun når det gjelder sikkerhetsrelaterte temaer. Videre påpekes det viktigheten av at ledere ikke bare uttrykker deres forpliktelse gjennom ord, men også gjennom deres handlinger. Informant B forklarer:

Men ledelsens direkte påvirkning og håndtering av i det daglige, er å vise at man tenker security. At man gjør de rette tingene, ikke bare sier det, men at en gjør, er helt avgjørende for å få folk til å tro på at det er viktig.

I resultatene fremgår det også at linjeledelsen spiller en stor rolle i forhold til utvikling av en optimal sikringskultur. Informant K sier i det følgende:

Det som er veldig viktig er at linjeledelsen er tydelig på dette området. Men ikke sant, først må jo linjeledelsen forstå hvorfor de må være tydelige og de må velge å ta dette alvorlig. Dette er en del av kulturklatring ikke sant? Når det er da, at de er trygge på dette her, de skjønner hvorfor, de kan ordlegge seg så vil ledelsen ta eget initiativ på alle måter der det er naturlig til å følge de kravene og forventningene vi har, også ta det lengre enn det og på en måte tenke selv.

Her fremheves betydningen av at linjeledere må inneha en forståelse for sikring slik at de selv tar initativ, noe som flere anses som sentralt i forhold til sikringskulturbegrepet.

Flere av informantene meddeler at ledelsens prioritering av sikring har endret seg over tid, der ledere vektlegger dette i større grad enn tidligere. Noen av årsakene til dette knyttes til hendelser som har gjort store inntrykk, blant annet hendelsene 22.juli og terrorangrepet ved In Amenas anlegget, samt mediafokus og regulering fra myndighetenes side. Likevel uttrykker Informant D at arbeidet med å skape en kultur har vært en tung reise. Han meddeler:

> *(...) det med kultur for å si det rett ut, det tar årevis og uten støtte fra ledelsene kommer du ingen vei. Du må har ledelsen med deg på dette. Og alt som har med sikring er jo en utgift og det er ingen inntekter forbundet med sikring.*

Flere av informantente påpeker dette og at det til tider har vært krevende å overtale ledelse for å få gjennomslag for sine tiltak. Resultatene viser at flertallet synes å ha en top-down tilnærming til sikringskultur, hvor en er nødt til å få sikring forankret hos ledelsen for deretter å spre dette nedover i organisasjonen og ut i avdelingene. Informant K forklarer det slik:

> *Ledelsen er forferdelig viktig. Du får ikke gjort noe hvis ikke ledelsen skjønner hvorfor det er nødvendig å gjøre en del sikringsgrep i henhold til risiko, verdier, sårbarheter og trussel. (...) Det er en slags top-down approach, men på ett eller annet tidspunkt får du hele organisasjonen med deg da, når kulturen modnes på en måte slik at folk tar kontakt fordi de ser noe. (...) Og det er ikke fordi de har fått beskjed (...) De skjønner det selv, det er det som er kulturen. At det på en måte er selvgående, de vet hvorfor det er viktig også må de vite hvordan de skal reagere og hvordan de skal forholde seg.*

Her fremheves det at målet er at hele organisasjonen skal være pådrivere for sikring, og at alle ansatte selv tar initiativ og forstår viktigheten av sikring. Ansattes forpliktelse til sikring blir dermed trukket frem som sentralt.

Ledelsens forpliktelse anses av alle informantene som en forutsetning for å utvikle en optimal sikringskultur, der det understrekes at dersom ledere ikke tar sikring på alvor, vil heller ikke resten av organisasjonen ta det alvorlig. Til tross for at informantene vektlegger ledelsens forpliktelse i arbeidet med å utvikle en sikringskultur, er det få som har formulert en eksplisitt security policy. Informant L forteller at det manglet en security policy når han startet i sin stilling som sikringsansvarlig, men at dette er noe han har klart å skape forståelse for hos toppledelsen. Videre påpeker han at alle oljeselskap som arbeider internasjonalt bør ha en security policy, på lik linje som HMS og kvalitetspolicy. Til tross for manglende security policy, viser enkelte av informantene til sikringsprinsipper og prosedyrer.

4.2.2 Fleksibilitet

Flere av informantene vektlegger viktigheten av det å kunne håndtere eventuelle sikringshendelser og ser på dette som et viktig kjennetegn ved en optimal sikringskultur. I den forbindelse anses øvelser som en viktig del av å utvikle og opprettholde kompetansen til ansatte og gjøre dem i stand til å håndtere uventede hendelser. De fleste har inkorporert sikring i beredskapsplanene sine samt gjennomfører øvelser på ulike sikringsscenarioer. Informantene forteller at dette er viktig i forhold til å øke bevisstheten omkring sikring. Blant annet meddeler informant K følgende: *"Det hjelper oss ikke bare mentalt, men også praktisk på en måte være forberedt på at ting virkelig kan gå galt."* Informant F påpeker at man kan ikke beskytte seg mot alle typer angrep, og dermed er selskapets normaliseringsevne helt avgjørende. Han forklarer det slik:

> *En må ha like gode planer for normalisering som for bekjempelse. De senere tids angrep på f.eks. IT siden tilsier at det å stoppe en aktør som har både intensjon og kapabilitet er vanskelig. Av de ca 50 selskapene som da ble rammet i forbindelse med fjorårets store " cyberangrep" er det kanskje kun et fåtall som har sjanse til å stoppe et slikt angrep, hvor forskjell på suksess og fiasko kan da være hva du faktisk klarer å gjøre i etterkant.*

Flere av selskapene har utarbeidet sikringsplaner hvor de har definert en rekke hendelser og kommet opp med ulike tiltak for hvordan disse hendelsene skal håndteres.

Øvelser anses som viktig for å sikre at planverket er tilstrekkelig og fungerer i praksis, og det fremheves at dette kan bidra til kontinuerlig forbedring. De fleste informantene forteller at de har årlige øvelser offshore, eksempelvis på bombetrussel, samt at de har øvelser i regi av forsvaret. Noen deltar også på nasjonale øvelser slik som Gemini. Videre meddeles det at det er et krav om ukentlige beredskapsøvelser offshore. Flere av informantene forteller om table-top øvelser, hvor de gjennomgår ulike scenarioer, også inkludert sikringshendelser. Informant K har stor sans for table-top øvelser hvor konsernledelsen får brynt seg på krevende situasjoner der de må ta viktige beslutninger med hensyn til sikring. Generelt anser informantene erfaringer fra slike øvelser som nyttig lærdom, med muligheter for forbedring og kompetanseheving, samt at det bidrar til kulturbygging i selskapet. Informant F påpeker at work shops har hatt stor betydning for deres sikringsarbeid. Han meddeler at de gjennomførte en workshop hvor en sikringscase ble presentert uten planverk og sjekklister. Erfaringer fra denne ble så benyttet som input i selskapets beredskapsplan. Informant F meddeler: "(...) *første gang vi prøvde oss på sikring, så øvde beredskapsorganisasjonen uten noe sikringsplan. Under mottoet: hvis du kan håndtere en tung oljevernaksjon, så kan du også håndtere en sikringshendelse."* Dette arbeidet anså han som svært positivt for å teste ut selskapets evne til å håndtere en sikringshendelse, samt at dette medførte til økt mestringsfølelse og sikringsbevissthet.

Det fremgår i empirien at håndtering av sikringshendelser krever en annerledes tankegang sammenlignet med for eksempel brannøvelser. Informant B meddeler at man må tenke annerledes i en sikringskontekst og dette er noe som man også må trene på. Han forklarer det slik:

> *Det er ingen standard reaksjonsmønster som en skal følge, snarere tvert imot. Man må tenke, man må forholde seg til trusselen og agere deretter. Går terroralarmen eksempelvis, så er det snarere tvert imot at vi ønsker at alle samles på samme sted. Man må redde seg selv, og sine ansatte. Så det er et helt annet mindset, så ja vi trener på det.*

Videre påpekes det at security scenarioer trenes i alle linjer. Informant D mener også at håndtering av sikringshendelser krever et annet tankesett. Han ser dette i lys av det

endrede trusselbilde og hva selskapet anser som relevante trusler, noe som igjen påvirker hvordan de arbeider for å være i stand til å håndtere sikringshendelser. Han forteller det slik: "*Men du må være klar over at trusselen kan endre seg i morgen, og da må du har gjort jobben din med at du faktisk kan øke sikringen din. Og det er her jeg tror mange feiler."* Videre meddeler han: "*Tenker sånn som det var før med bomber og granater og den type ting. Du må tenke på at det kommer en, mye mer en person som kommer inn i resepsjonen og skyter vilt rundt seg. (...) Så du må jobbe helt annerledes. Tenke annerledes, og det er noe som også tar tid i en organisasjon."* Videre meddeler han at selskapet opererer med flere nivåer av sikring og har dermed mulighet til å eskalere mengden tiltak i forhold til trusselnivået. Han forklarer at her spiller kulturen også en viktig rolle, som gjør at de ansatte aksepterer tiltakene. I denne sammenheng vektlegges informasjonsutveksling til de ansatte. Informant E knytter mengden tiltak til at virksomheten har en risikobasert tilnærming. Han påpeker at dersom trusselnivået øker, iverksetter de en rekke ressurser. Han forklarer det slik:

> *Og når det er, hvis vi tror at vi er utsatt for en trussel, så setter vi på enorme ressurser. (...) Jeg hadde aldri drømt om at det var sånne ressurser som vi setter ned. Det er helt enorme ressurser vi setter inn, hvis vi er utsatt for noe. Og derfor tror vi og at vi er utsatt for lite. Det er en, en del av vår kultur, det er at vi er søkke robust. Vi tar ikke, vi tar ikke lett på ting.*

Til tross for at øvelser anses som viktig for å kunne respondere på trusler, fremkommer det i resultatene at hovedvekten av øvelser legges på sikkerhetsrelaterte øvelser. Likevel påpekes det at der mye likt mellom håndtering av en beredskapshendelse og en sikringshendelse. Informant I forklarer: "*Om ikke det er den som blir vektet mest i forhold til trening og øvelse, så vil den reaksjonen eller de prosessene der være likt med det som hadde skjedd hvis det hadde skjedd en vanlig beredskapshendelse."* Det er videre få av virksomhetene som har øvelser som involverer alle ansatte. Hovedfokus synes å være på ledelsen, linjeledere, beredskapsorganisasjon samt de som har en funksjon innen sikring. Eksempelvis meddeler informant G at de involverer de som har et ansvar i forhold til sikring. Han påpeker videre: *"Det du ønsker å oppnå med en øvelse er at det blir håndtert riktig av de som skal håndtere det. I tillegg vil det bidra til mer kompetanse ned i linjen"*.

Informant I forteller at de skiller mellom ulike grupper i selskapet; mellom vanlig kontoransatte, vanlig offshore ansatte, og de som har har en beredskapsfunksjon. I forhold til øvelser meddeler han: *"Og de som er en del av beredskapsorganisasjonen har vært gjennom et trening og kompetanse program, og der er security, er også en del av den pakken da."* Når det gjelder øvrige ansatte er opplæringen vanligvis begrenset til en HMS introduksjon hvor de ansatte får en grunnleggende innføring, hvor blant annet sikring inngår.

4.2.3 Læring

Det fremgår i empirien at få av virksomhetene har erfart alvorlige sikringshendelser i Norge. Informantene fremhever ulike elementer som vektlegges slik at virksomhetene skal være i stand til å lære i fravær av intenderte uønskede hendelser. Deriblant; åpenhet, rapportering, og samarbeid med eksterne aktører, som er i stor grad gjensidig avhengig av hverandre.

Åpenhet

Åpenhet anes som helt sentralt for utvikling av en sikringskultur og knyttes både til kunnskapsdeling, tillit og bevisstgjøring i organisasjonen. En rekke av informantene fremhever at en form for åpenhet er viktig slik at menneskene i organisasjonen forstår truslene. Til tross for at informantene vektlegger åpenhet fremkommer det at denne åpenheten må begrenses på en slik måte at det ikke avslører virksomhetenes sårbarheter.

I forbindelse med åpenhet, påpekes det at sikring skiller seg fra sikkerhet og HMS på dette området. Informant A påpeker at innenfor HMS faget stiller selskapet seg positivt i forhold til åpenhet, der det anses som ønskelig at andre adopterer HMS metodikk og beste praksiser. Likevel påpekes det at i en sikringskontekst kan man ikke dele alt, eksempelvis selskapets sikringsrutiner og barrierer som potensielle trusselaktører kan få kjennskap til og dermed utnytte. Informant I forklarer:

> *For på sikkerhet da, så er poenget å ha full åpenhet. En skal på en måte lære av hverandre. Hvis vi har gjort en feil, hatt en hendelse, så ønsker vi på en måte å granske den også dele den med industrien og leverandørene, for vi ønsker ikke at dette skal skje igjen (...) Innenfor sikring så er det også viktig å*

dele ting med hverandre (...) men da er vi inne igjen på det med åpenhet og at en kan dele det i et felleskap i all hemmelighet, men når det fellesskapet har fått den informasjonen så kan de ikke nødvendigvis gå tilbake til sine selskap og fortelle om den historien.

Her snakker informanten om åpenhet mellom selskapene i petroleumssektoren som viktig i forhold til læring. Dette er noe flere informanter trekker frem som viktig. Informant F meddeler:

En risikerer og sitte på "hver sin holme" og finne opp kruttet på nytt. (...) *Vi kunne hatt en større grad av åpenhet uten å gå på akkord med sikkerheten. Selvfølgelig skal du ikke gå inn på de barrierene du har satt og de svakhetene du har, det er ikke ting du leverer fra deg. Men innen metodikk, arbeidsformer, systemer og sikringskultur er jeg sikker på at mye kan deles. Dette er nokså vanlig innenfor fagfeltet beredskap; her deles det erfaringer, planer overalt, men med en gang noe får et sikringsstempel så kan det ikke deles lenger.*

Åpenhet og erfaringsoverføring mellom selskapene anses av flere som viktig i forhold til læring. Videre påpekes det at det også er viktig med åpenhet fra myndighetenes side. Informant I forklarer:

Det er vanskelig for oss som industri og gjøre så veldig mye hvis myndighetene på en måte ikke vil dele med industrien da, om at det er et økt trusselbilde mot deres industri (...) så vil det være vanskelig for industrien å forstå det da.

Samarbeid med myndighetene blir dermed fremhevet som viktig for at selskapene skal kunne forstå trusselbildet de står ovenfor. Også informant D fremhever at de er åpne om veldig mye, men igjen understreker at man kan ikke dele informasjon om alle tiltak som er på plass. Videre meddeler informanten at de er veldig lukket når det kommer til saker som omhandler personell og personopplysninger. Han sier videre: *"Ellers prøver vi å være åpne og fortelle. Fortelle hva trusselnivået er, forteller ikke hva tiltakene er, men jeg er for at vi skal være åpne og folk skal vite. Det gjør jo at folk er mer bevisste på det som skjer."* Informant B legger vekt på at det å være åpen

er ikke det samme som å være naiv, og understreker at man må unngå å være naiv. Åpenhet anses dermed som viktig i forhold til å skape bevissthet og forståelse for sikringen i organisasjonen. Informant E forklarer det slik:

> *Så åpenhet er kjempe bra i forhold til at vi skal si at det finnes trusler, vi skal ikke overdrive trusler, vi skal være realistiske på det. Og vi skal fortelle folk at vi jobber med å beskytte oss. Så det er kjempe bra. Samtidig så er det en balansegang i forhold til å beskytte oss som selskap, og for å lykkes med det vi holder på med. Og det er ikke alt vi er åpne om.*

Han forteller blant annet at han ikke er åpen om hvordan selskapet driver etterretning eller alt som er taktisk og operasjonelt rettet. Dette er informasjon som kun ledelse og relevante personer har tilgang til, og informasjonsdeling er basert på en "need to know" basis.

Informant K knytter åpenhet til ærlighet og forteller hvordan dette har endret seg over tid. Tidligere var det en tendens til at IT angrep ble hysjet ned og han forteller:

> *Og det har det også gjort i vår virksomhet tidligere, men nå er vi veldig tydelig på det at ja nå har vi blitt angrepet av, ja, targeted målrettet epost angrep, ikke sant? Og dette kommuniserer vi i dag, relativt åpent. Men selvfølgelig forsiktige med å avsløre sårbarheter.*

Han meddeler at innen sikring er det fortsatt mye som må være begrenset, og referer til såkalte "chatam rules". Eksempelvis ved informasjonsinnhenting om trusler utveksles det en gjensidig forståelse for at man ikke skal røpe kilden til denne informasjonen. Slike regler gjelder eksempelvis i fellesmøter mellom selskapene.

Rapportering

Rapportering og avvikshåndtering blir i ulik grad fremhevet som viktig for å sikre kontinuerlig læring. Flere anser en optimal sikringskultur som en kultur der de ansatte sier ifra dersom de ser mistenkeligheter eller noe som kan skade organisasjonens verdier. Informant B sier følgende:

> *Med en optimal sikringskultur så tror jeg der man tørr og sier ifra, dersom enser noe som en tror er feil eller en trussel. Altså det å rapportere eksempelvis da, er veldig viktig. Og folk rapporter kun hvis dem er "aware" hvis dem ikke er "aware", er de ikke i stand til å rapportere. Så awareness, bare for å understreke det, det å være klar over, være informert på, bevisst, er kjempe viktig.*

Informant F knytter også rapportering til "security awareness", og han forteller at dette går ut på at folk sier ifra dersom de ser noe og at de har det litt "i bakhodet" i hverdagen sin. Alle informantene forteller at de har et rapporteringssystem for avvik, hvor også sikringshendelser blir registrert. Flere har også en egen modul for sikringsrelaterte hendelser. Informant L ser på rapporteringssystemet som et "erfaringsoverføringssystem", hvor hendelser rapporteres inn slik at andre kan lære av det. Informant B meddeler at systemet benyttes til å monitorere og analysere hva som skjer i selskapet. Videre sier informant E at selskapet vektlegger informasjonsutveksling og erfaringsoverføring på tvers av selskapets lokasjoner. Han påpeker at man er nødt til å spre informasjon om hendelsene rundt slik at man kan lære fra dem, og dette gjelder både safety og security. Likevel påpeker han at det er mye som er skjult innenfor security feltet. Informant B påpeker at det også er viktig å ta lærdom fra andre selskaper. Dette ses på som viktig i forhold til å ligge i forkant av truslene som er aktuelle for selskapet.

Det fremkommer videre at de fleste selskapene oppfordrer de ansatte til å rapportere avvik, herunder sikringsrelaterte hendelser. Informant K meddeler:

> *Men vi er veldig tydelige på at en skal rapportere sikringsbrudd. Og det er viktig. Jeg mener at det er ikke bare viktig for å få statistikk der noen mener noe om noe, men det er viktig at det skjer noe. At man tar fatt i det som er verdt å ta fatt i. Men rapportering, sikringsrapportering spesielt, er en vanskelig sak fordi det er mye sensitivt.*

Rapportering oppfattes dermed som viktig for å sikre kontinuerlig læring og forbedring. Likevel er det utfordringer forbundet med at mye av opplysningene er sensitive. I resultatene fremkommer det at enkelte av selskapene har dermed både en

åpen og en lukket del i rapporteringssystemet sitt. Med utgangspunkt i begrenset åpenhet, forklarer informant K det slik: *"Det som er spesielt med sikringshendelser er at tiltakene er som regel gradert, altså de kan du ikke legge i et åpent system, og heller ikke det som skjedde fordi det kan avsløre sårbarheter."* Dette medfører også at de som rapporterer ikke nødvendigvis får tilbakemelding på det som blir rapportert inn. Samtidig påpeker informant I at ikke alle sikringshendelser nødvendigvis blir registrert, da noen hendelser anses å være av en begrenset art. Informant G meddeler at det er størst fokus på rapportering av hendelser i det operative miljøet, sammenlignet med blant annet kontormedarbeidere.

Samarbeid med eksterne aktører

Flere av informantene beskriver at de forsøker å dra lærdom fra andre i bransjen, eksempelvis Statoil og deres erfaringer fra angrepet ved In Amenas anlegget. Informant I forteller:

> *Det er klart det er erfaringer der som en tar med seg inn da, av det som har kommet ut som er åpent ,om hvordan en kan ja mentalt tenke på situasjonen, hva utfordringer har selskapet vært i, og prøve å sette det inn i vår kontekst, og se hva vi kan gjøre, eller må vi gjøre noe?*

Flere av informantene medeler at de utveksler erfaringer og lærdommer med andre selskaper og ser på dette som nyttig i sikringsarbeidet. Informant C meddeler: *"Vi skal ikke finne opp kruttet alene"* mens informant B forteller: *"Og alle da, eksempelvis oljeselskaper, som vi samarbeider med, i den samme trusselsituasjonen, og derfor prater vi mye med dem, og utveksler informasjon og samarbeider på hvordan vi best mulig skal håndtere security risks."* Informant I viser til at det er viktig at selskapene har en dialog slik at de drar i samme retning. Han påpeker at til tross for at de besitter en type informasjon så er det fortsatt mye usikkerhet knyttet til den som skaper utfordringer. Informant C forteller: *"Så vi deler kunnskap. Vi skal ikke sitte på vår egen tue og tro vi kan alt. Vi har mye å lære av hverandre."* Samarbeid, både nasjonalt og internasjonalt, anses som nyttig for å få en bedre forståelse for de ulike truslene selskapene står overfor. Eksempelvis nevnes ulike sikringsnettverk og forum. Likevel er det noen av informantene som ikke anser

hendelser som terrorangrepet ved In Amenas som like relevant. Informant E meddeler:

> *In Amenas er ikke så veldig relevant for oss egentlig. Med all respekt. (...) Er det noe å lære? Ja kanskje, men hvor mye skal du egentlig implementere? (...) Men vi har systemer for å lære, men vi er nok veldig fokusert på at det skal være tilpasset det teateret vi er i.*

Også samarbeid med myndigheter og etater fremstår som svært nyttig i utvikling av en sikringskultur. Her nevnes blant annet et tett samarbeid med Petroleumstilsynet (Ptil), Politiet og Forsvaret, der råd og anbefalinger fra disse verdsettes av selskapene. Videre vektlegges samarbeid i forhold til utvikling av beredskapsplaner og beredskapsøvelser, der enkelte av informantene viser til store beredskapsøvelser hvor alle etatene deltar. Informant G understreker dette på følgende måte:

> *Når du arbeider med security kan du ikke stå alene, du er nødt til å samarbeide med myndigheter og ha et nettverk med andre selskaper som står ovenfor de samme utfordringene. Du er nødt til å samarbeide med dem og være avstemt med dem, vi spiller mye på hverandre og samarbeider på security.*

Etterretning spiller en viktig rolle i virksomhetenes sikringsarbeid og har som funksjon å kontinuerlig innhente og analysere informasjon for å fange opp faresignaler og trusler mot bransjen. I denne sammenheng nevner et flertall av informantene at de har et tett samarbeid med Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) da dette er viktig for å kontinuerlig holde seg oppdatert på dagens trusselbilde, og dermed være i stand til å agere i henhold til trusselnivået. Videre nevnes det at selskapet gjennomfører analyser og prosesser uavhengig om det har skjedd en hendelse eller ikke, som oppdateres ved jevne mellomrom. Det påpekes at disse prosessene må kjøres på nytt dersom der skjer store endringer i trusselbildet.

4.2.4 Tillit

Flere av informantene fremhever tillit som essensielt i arbeidet med å utvikle en optimal sikringskultur. Informant B meddeler at tillit er nøkkelen til å lykkes i enhver organisasjon. Han forklarer det slik:

> *Det handler om hvordan en leder får med sine ansatte til å gjøre et eller annet, da må det være tillit. Og det må også være en tillit til organisasjonen, til alle ansatte, at det vi gjør på sikring er bra, og at de har lyst å ta det til seg og gjør som vi har sagt fordi de forstår. Der er det også en tillit som vi må sørge for å stable på bena. Så det er kjempe viktig.*

Også Informant K vektlegger at de ansatte har tillit til at både fagfolk og systemet tar tak i problemene. Informant I fremhever også viktigheten av at selskapet har tillit til nøkkelpersoner som arbeider med sikring i organisasjonen fordi de kan besitte informasjon som ikke kan deles med resten av selskapet. Dette gjelder også beslutningstakere som ikke er sikkerhetsklarerte og som gjerne må fatte beslutninger uten fullstendig bakgrunnsinformasjon. Det fremheves også at organisasjonen må ha tillit til sine ansatte, til tross for at trusler kan oppstå internt. Her er det andre prosesser og systemer som må være på plass for å fange opp potensielle innsidetrusler, eksempelvis bakgrunnssjekker i forbindelse med rekruttering. Noen fremhever også at avdelingslederne har et ansvar for å følge med og ha en såpass god dialog med ansatte at faresignaler blir fanget opp. En av informantene påpeker også viktigheten av tillit mellom virksomhet og samarbeidspartnere. I forhold til dette samarbeidet meddeler han: "*Og vi tror at den tilliten som er mellom oss, det er utrolig viktig for en god sikringskultur."* Dette er derfor noe han forsøker å beskytte i høyeste grad.

Også Informant G ser på tillit som nødvendig i arbeidet med å utvikle en sikringskultur. Han sier som følgende:

> *Tillit må være til stede for å oppnå en god sikringskultur. Du har lover og systemer, men det er du som security ansvarlig som skal sørge for å drive frem denne kulturen, og du blir da kulturbærer, og som kulturbærer må du ha tillit*

fra organisasjonen. Åpenhet er derfor viktig. Empowerment forsvinner uten tillit.

Informant G understreker at man må ha tillit oppad og nedad i organisasjonen og i denne sammenheng vektlegger han integritet. Han eksemplifiserer at når han startet i selskapet var det viktig at de ansatte og ledelsen visste hvilke verdier og holdninger han sto for. Han påpeker at dersom de ansatte har et negativt inntrykk av ham, vil man heller ikke få til noe endring i sikringskulturen. Samtidig som åpenhet blir vektlagt som viktig i forhold til å bygge tillit og påpeker informant G at han har et ansvar for å skape forståelse for at det er ikke alt som kan deles. Han understreker at med åpenhet menes at man må være transparent i forhold de prosessene som benyttes, for eksempel hvordan man kom fram til at risikoen var høy. Det påpekes at man må få til en balansegang i forhold til hvordan man håndterer informasjon som er begrenset og klassifisert. Informant I forklarer at innen security må man vurdere informasjonen, vurdere hva man skal gå ut med, når man skal gå ut med det, samt hvordan man skal gå ut med det.

Resultatene viser at åpenhet og tillit anses som nødvendig for å sikre læring i organisasjonen, blant annet gjennom rapportering og tilbakemeldinger fra ansatte. Informant E påpeker at tillit er viktig slik at ansatte føler de kan henvende seg til ham angående sikringsrelaterte saker og problemer. Ettersom det kan dreie seg om personellrelaterte saker, er det viktig at de ansatte stoler på at informasjonen vil bli holdt konfidensielt, og kun deles etter behov. Flere enes om dette. Informant L meddeler:

Åpenhet og tillit er nok ganske viktig, for hvis jeg ikke får tilbakemeldinger eller hvis selskapet ikke får tilbakemelding fra sine ansatte på hva som har skjedd, da kan vi ikke lære, og da kan vi ikke ha en erfaringsoverføring.

Resultatene viser også at en del av informantene vektlegger muntlig rapportering, og det blir dermed viktig å skape et miljø hvor terskelen er lav for å si ifra. Videre fremkommer det i resultatene at ettersom innrapporterte hendelser kan være sensitive av natur, er det ikke alltid at de som rapporterer får tilbakemelding på dette. Informant K meddeler: *"Der synder vi nokså mye tror jeg. Men folk forventer at det blir tatt tak*

i, ikke sant?" Igjen blir det lagt vekt på at ansatte har tillit til at systemet er i stand til å håndtere problemet.

I forhold til håndtering av brudd på sikringsprosedyrer, fremhever informant B viktigheten av at de ansatte rapporterer sikringsrelaterte hendelser slik at virksomheten er i stand til å fange dette opp. Han understreker at straff er ikke den riktige tilnærmingen for å stimulere til rapportering. Han forklarer det slik: *"Det er liksom trening og opplæring som er tanken, ikke straff. Vi må bli flinkere, og for at vi skal bli flinkere må folk rapportere, tørre å rapportere, lyst til å rapportere, så vi ønsker å stimulere det."* Rapportering blir dermed sett på som viktig i forhold til å sørge for kontinuerlig forbedring. Likevel viser mange av informantene til at det er viktig å være tydelig på hva som er akseptabel eller uakseptabel atferd. Informant E sier det på følgende måte: "*Så vi følger reglene. Og når du ikke følger reglene, så får det konsekvenser." (...) vi har klare regler, klare forventninger, og hvis du bryter de, så må du ha et godt svar. Det gjelder også security biten.*" Informanten ser dermed ikke annerledes på brudd på sikringsregler enn andre typer brudd forøvrig. I forhold til hvordan det reageres på brudd på sikringsprosedyrer forteller de fleste informantene at det avhenger av frekvens samt alvorligheten av sikringsbruddet. Flere viser til at dette kan i noen tilfeller medføre til stillingsmessige konsekvenser og oppsigelse. Blant annet sier informant K: "*Det kommer an på hvor alvorlig det er. Hvis det er, og hvor gjentatte de er. De vanlige reglene gjelder her. Man kan få skriftlige advarsel, og man kan også bli avskjediget hvis det er en grov tjeneste forsømmelse."* Flere skiller mellom brudd som er gjort med "vilje og viten", eller som er gjort ved en feilhandling eller glipp.

Generelt fremgår det i resultatene at informantene mener det er viktig å reagere, men det foregår på ulike måter avhengig av alvorligheten på sikringsbruddet. Informant E meddeler: "*Tror også at, for at vi skal ha en sikringskultur i selskapet, så må det være slik at folk må se at vi mener alvor. Og det betyr at når du bryter reglene så mener vi alvor."* Informant L påpeker at det kan være en utfordring å få folk til å rapportere sine feil da de vet at det kan få konsekvenser og vil unngå problemer. Likevel mener han at dette er en større utfordring i andre land hvor de ansatte ikke er like godt beskyttet som i Norge.

4.3 Hvilke utfordringer opplever operatørselskapene i arbeidet med å utvikle en slik kultur?

Det fremgår av empirien at utvikling av en sikringskultur anses av mange som en tung og krevende prosess der man møter en rekke utfordringer. Vi har strukturert utfordringene ut ifra de hovedtemaene som går igjen i empirien og som har relevans for arbeidet med å utvikle en sikringskultur.

Etterlevelse av prosedyrer

En av utfordringene som informantene belyser er å få menneskene i organisasjonen til å følge prosedyrer og regler. Informant G meddeler: *"Den største utfordringen er menneskene. De tenker selv og velger de letteste løsningene."* Han påpeker at man må sørge for at menneskene i organisasjonen har kulturen, verdier, holdninger og atferd som gjør at de opererer sikkert. Informant H forklarer det slik:

> (*...) bedriften har lagt til grunn at du har et skap med en dedikert nøkkel, du legger verdisaker inn også låser du og tar nøkkelen i lommen. Det gidder ikke folk å gjøre nødvendigvis. Så de legger lommeboken sin på pulten og så syns de at det er helt kjekt, også vil de ikke ha så veldig mye med adgangskontroll og den type ting fordi det er en ulempe for "meg". Alltid "jeg-et". Men så forsvinner den lommeboken, og da kommer de.*

Her påpeker han at mennesker velger løsninger som gagner "jeg-et" og argumenterer for at dette kan føre til snarveier med hensyn til sikring. Informant D enes også om dette og forklarer det slik: "*Vi har med mennesker å gjøre, mennesket er vår sterkeste og svakeste ressurs, mennesker velger de enkleste løsninger, det er vår styrke det er vår svakhet."* Informant D knytter videre problematikk med etterleves av sikringsprosedyrer til norsk kultur og sier i det følgende:

> *Og folk får begrensninger. Det er liksom egentlig veldig unorsk tankegang. Vi har jo lyst til å gå hvor vi vil henne. Ser vi et gjerde på fjellet så blir vi sure. Altså det er den tankegangen vi drar med oss hjem også.*

Sikringstiltak vil ofte oppleves som begrensende for ansatte og det kan dermed være vanskelig å få aksept og forståelse for disse, som igjen henger sammen med

etterlevelse. Også informant L forklarer at de ansatte føler at han legger begrensninger på dem ved å innføre regler og prosedyrer som de må følge når de er på reise.

Hvorvidt norsk kultur er en ulempe eller fordel for å utvikle en sikringskultur oppfattes ulikt av informantene. Noen ser på norsk kultur som en fordel ved at Norge ses på som et tillitssamfunn. Noen påpeker også at nordmenn generelt sett er lovlydige mennesker, noe som gjør at vi ønsker å følge regler og prosedyrer. Flere hevder at folk er i utgangspunktet veldig positive og ønsker å gjøre ting riktig, noe som anses som positivt for sikringskulturen. Informant C forteller likevel at det er en utfordring å få folk til å ta sikring på alvor og få de til å se på sikring som en del av det totale HMS bildet. Dette gjelder spesielt det operative miljøet. Informant L meddeler at for at de ansatte skal ta sikring på alvor er det viktig at de forstår risikoen, noe som igjen fører til høyere grad av aksept til de implementerte sikringstiltakene. Dette ser han som en utfordring i og med at opplevelsen av risiko varierer. Informant K påpeker også vanskelighetene med å skape forståelse for sikringstiltakene, og han meddeler at han ofte merker en "nå kommer de for å sjekke meg" holdning blant de ansatte. Også informant H forteller at mange ansatte oppfatter tiltak knyttet til adgangskontroll som "storebror ser deg", og påpeker samtidig at det er ikke det som er hensikten. Videre hevder han at det vil alltid være mye støy i begynnelsen når man implementerer nye tiltak. Også informant E påpeker at man kan møte på litt motstand i en overgangsfase, men at folk lærer seg å leve med det, slik at det oppleves ikke som en stor utfordring for informanten.

Prioritering av sikring

I empirien fremgår det at informantene har bevilget mye tid og energi på å overtale ledelsen og at det til tider har vært utfordrende å få ledelsen til å forstå viktigheten av sikring. Blant annet meddeler informant L at når han ble ansatt i selskapet måtte han overtale ledelsen til å innføre en security policy. Videre påpeker han at det fortsatt er noen ledere som ikke tar sikring alvorlig, og at dette er en utfordring i arbeidet med å utvikle en sikringskultur. Han forklarer det slik, *"Dette må gå top-down (...) og hvis de har den holdning at sikring ikke er viktig, og det går ikke nedover i avdelingen, så hjelper det ikke."* Dette er noe mange av informantene beskriver som utfordrende.

Resultatene viser at kun et fåtall av selskapene har utarbeidet en egen sikringspolicy, samt utarbeidet eksplisitte sikringsmål. Informant D anser utarbeidelse av sikringsmål som en utfordring og forklarer det slik: *"Og liksom, vi sliter. Setter du deg mål og skal bli målt opp mot mål, innenfor sikring er det forferdelig vanskelig. Ja, det der er politikk på høyt plan."* Flere viser til et overordnet mål som sier at man ikke skal bli skadet på jobb uavhengig om det er en sikringshendelse eller sikkerhetshendelse.

Både informant D og G forteller at når de begynte som sikringsansvarlig i selskapet var det lite fokus på sikring blant lederene og de måtte bruke mye tid på å forklare hvilke konsekvenser et lavt sikringsnivå i selskapet kunne medføre. Informant D understreker at både kulturen og tiden har endret seg, og sier i det følgende:

> *Vi har ikke hatt en direkte trussel mot oljenæringen i Norge. (...) Men der vi merker at den kulturen vi har fått implementert fra ledelsen og sånne ting, at de aksepterer det. De begynner ikke å tenke i kroner og øre. I begynnelsen var det sånn, ok hva koster en ekstra vekter? Nå er det ikke lenger diskusjonstema en gang. De ser nytten av det og de ser at det er sånn vi gjør det.*

Dette er noe et flertall av informantene enes i. Likevel påpeker Informant C at kost-nytte problematikken kan forekomme i forbindelse med utvikling av en sikringskultur. Han sier i det følgende: *"Det er ofte når du kommer til kost, det koster penger, da kan du jo møte hindringer."*

Balanse mellom sikringstiltak og risikonivå

Resultatene viser at enkelte av informantene mener at det er en utfordring å finne den riktige balansen mellom sikringstiltak og risikonivå. Blant annet understreker informant H viktigheten av å tilpasse sikringstiltakene på en fornuftig måte. Han sier i det følgende:

> *Så sikkerhet er jo egentlig noe som skal spille på lag med sikre verdier og sikre interesser, samtidig som det også er en faktor som skal være minst mulig synlig, minst mulig til hinder, men samtidig gjør jobben, sikre verdier og kunnskap, og mennesker.*

Her påpekes blant annet at sikringstiltakene skal være minst mulig synlig slik at folk føler seg minst mulig begrenset. Informant K påpeker også viktigheten av å finne den riktige balansen og meddeler følgende:

> *Det jeg hadde tenkt å si da, det er at når du starter med ikke helt blanke ark, men relativt tyntskrevne ark så, og når du setter store ressurser på å bygge en kultur så renner det over av gode ting. Da er det slik at organisasjonen, både ledere og ansatte generelt, men kanskje ikke sikringsfagfolk, de vil jo føle at det blir veldig mye. Veldig veldig mye. Og vi er jo redd for security overload som jeg kaller det.*

Flere av informantene påpeker at man må ikke overdrive sikringstiltakene. Informant C sier, *"Det skal ikke være sånn over-kill heller altså. Det skal være på et ganske, hva skal du si, et godt nivå som ivaretar verdiene våre på en god måte."* Noen av informantene fremhever at dersom man har for høyt sikringsnivå kan dette medføre til paranoia og skape en uønsket angstfølelse blant de ansatte. Informant G forteller at dersom man eksempelvis øver på kidnapping eller terror kan dette skape frykt blant ansatte som begynner å tvile på om det er trygt å komme på jobb. Informant K forteller:

> *Også er det de ansatte som du sier, som ikke må føle at de bor i festning fordi det kan oppleves traumatisk av mange. Sant, de som jobber i NOKAS, pengehuset, de har jo ekstraordinære sikringstiltak. Om de føler seg komfortable eller ikke komfortale med å ha sånne ekstreme sikringstiltak vet jeg ikke.*

For å ikke skape uønskede reaksjoner blant ansatte påpeker informant I at det også er viktig å gjøre en nøye vurdering av hvilke type informasjon man velger å gå ut med, samt hvordan man kommuniserer ut et økt trusselnivå til de ansatte. Videre påpeker informant D: "*Du må legge sikring på et nivå, som gjør at du kan leve med det. Som gjør at du kan forsvare det både kostnadsmessig og hensiktsmessig og at du legger det på et som tilsvarer den trusselen her og nå."* Flere fremhever dermed viktigheten av at man skal ha en risikobasert tilnærming hvor tiltakene er tilpasset trusselnivået.

Begrenset åpenhet

I resultatene kommer det frem at begrenset åpenhet omkring sensitiv informasjon fra myndighet kan by på utfordringer for sikringsansvarlig i virksomheten. Informant I forklarer det slik:

> *Så det er balansegangen på en måte på hvordan en evner å håndtere informasjonen som er begrenset og klassifisert da, og det kan være utfordringer innenfor selskapet. At jeg går til, eller får informasjon da fra myndighetene på situasjoner hvor jeg ikke har lovt til å går videre med denne informasjonen, men det er en situasjon. Og det er nok en utfordring i alle oljeselskaper eller alle selskaper, å kunne få en type informasjon fra nasjonale myndigheter, og hvor en da må gjøre tiltak og hvor da oppover i systemet da ikke har personell som sitter og er godkjent, sikkerhetsklarert da, og hvordan skal en da kunne gi informasjon til de, og en skal fatte beslutninger på selskapet hvor da de kanskje nødvendigvis vet ikke helt hva som er bakgrunnen."*

Informantene belyser flere utfordringer knyttet til åpenhet i en sikringskontekst, både i forhold til informasjonsdeling og rapportering.

Sikring versus HMS

Informant D påpeker at det ofte oppstår en organisatorisk konflikt mellom selskapets HMS og sikring, noe han videre knytter til HMS kultur og sikringskultur. Han forklarer at i mange tilfeller der sikringstiltak og HMS tiltak blir satt opp mot hverandre, vinner HMS. Han sier det slik:

> (...) *hvis du setter HMS veldig høyt og sikring veldig lavt så er det klart da vinner HMS. HMS skal vinne i de fleste tilfeller i store konflikter, det som går på brann, det som går på sikkerhet til de ansatte.*

Videre meddeler han at i flere år gikk HMS foran sikring og det gikk 4- 5 år før sikringstiltaket fikk gjennomslag hos ledelsen. Han påpeker at dette trolig skjer i andre selskaper også. Videre viser han til et eksempel der et sikringstiltak ble implementert og ble svært dårlig mottatt av de ansatte. Likevel påpeker han at etter en

stund opplevdes sikringstiltaket som nyttig fordi den hadde en positiv effekt på selskapets totale HMS. Dermed mener han selv at han klarte å snu det negative fokuset som sikringstiltaket hadde fått, og knytter dette til endringer i kulturen i selskapet.

Det fremkommer i empirien at sikring ikke nødvendigvis får ønsket fokus blant ansatte på grunn av målkonflikter. Blant annet nevner informant I at en boreingeniør vil fokusere på å utføre sine arbeidsoppgaver, og ønsker minst mulig stopp og forsinkelser. På grunn av dette hevder informanten at det kan være lett å glemme sikringselementet. Informant D påpeker at dette utgjør en av forskjellene mellom sikringskultur og sikkerhetskultur, og sier i det følgende:

> *Der en god HMS kultur vil være at du, der skal du passere der du egentlig ikke skaper forsinkelser, du skal egentlig ikke ha stopp, altså. Men god sikringskultur det kan være at du vil ha mer kontroller og der du får mer opphold i arbeid. (...) Altså den type ting som kan være litt motstridende kan du si.*

Samtidig påpeker han at dersom du har en god sikkerhetskultur, er det lettere å få en god sikringskultur, noe flere enes om. Informant B påpeker også fordelen ved å ha en god sikkerhetskultur og meddeler:

> *Fordi det er veldig mange ting der som vi kan bruke, altså tilnærming og begreper for så vidt. Selv om vi har vårt eget unike begrepsapparat, som vi må ha. Er man vant til å være compliant, som vi sier, altså å følge lovene og reglene. (...) er man vant til å tenke litt sånn, kan man også lære å tenke, se etter trusler, og se avvik fra normalen.*

Samtidig påpeker Informant G at ikke alt en gjør på sikkerhetsområdet kan overføres til sikring, slik som mange tror.

Kontinuerlig arbeid

Flere av informantene påpeker at kulturbygging er en tidkrevende prosess som krever kontinuerlig arbeid. Informant B forklarer blant annet at innenfor sikkerhetskultur har selskapet blitt veldig gode, og har en lang tradisjon med å utvikle en slik kultur. Det

påpekes at innenfor sikring er selskapet "ung", og at dette er noe som har fått økt fokus som følge av In Amenas hendelsen. Det understrekes at utviklingen av en sikringskultur vil ta lang tid og er vanskelig å oppnå, og viser til at det tok omtrent 40 år å få en solid sikkerhetskultur i selskapet. Informant J påpeker også at bransjen har en lang vei å gå når det gjelder sikring i Norge og sier i det følgende:

> *Flere ganger kommer dette sikkert tilbake, men jeg mener at i Norge har vi blitt veldig flinke på HMS kultur, og folk passer for fallende gjenstander over seg, holde seg i rekkverket osv. Men dessverre er vi fremdeles ganske naiv når det gjelder security, altså når det gjelder sikring.*

Likevel fremgår det empirien at et fåtall av informantene er fornøyde med den sikringskulturen de har og ser ikke behov for kontinuerlig arbeid. Deriblant hevder informant E:

> *Vi har ikke noen store initiativ på securitykultur biten. Og det tror jeg er fordi vi egentlig ikke opplever noe behov. (..) "Og jeg jobber lite med mine offshore folk i forhold til security kultur, vil jeg si. Delvis fordi det at jeg tror vi har en ganske god sikringskultur. Delvis og fordi våre installasjoner ligger 20 mil fra land.*

Informant M meddeler også at det ikke foregår noe kontinuerlig arbeid og forklarer det slik:

> *Vi gjorde det når vi holdt på med det, men nå har det vært stille det siste året, siden vi fikk dette på plass, så har vi ikke motivert noe mer, fordi at vi har mye annet å holde på med, kan du si. Og min tid er også begrenset. Jeg gjorde en innsats da, også hadde vi en motivasjonsrunde også håper jeg det sitter litt i folka da. Men det er ikke noe kontinuerlig oppfølging.*

Norsk kultur

Flere av informantene fremhever at norsk kultur har betydning for sikringsarbeidet. Blant annet fremkommer det at naivitet kan skape utfordringer med å skape de ønskede holdninger og atferd blant ansatte. Blant annet informant L påpeker at naiviteten til nordmenn og en manglende risikoforståelse kan være en utfordring for utvikling av en sikringskultur. Han påpeker at sikringsbevisstheten i Norge er generelt sett ikke god nok, og viser til at det ikke er uvanlig at man overhører forretningspersoner snakke om konfidensiell informasjon i offentligheten. Han forklarer at spesielt nordmenn som ikke har vært i utlandet før har en liten forståelse for risiko og sikring og tror at alt er likt i utlandet. Informant D ser derimot litt annerledes på naivitet og sier det slik: *"Nei, det er ikke en hindring, det er en utfordring. Og ja vi er nordmenn, vi har langt å gå. (...) men vi må ha lov til å være naive, men samtidig bry oss om andre*." Informant A påpeker at vi er ikke naive, men derimot: *"Norge er tillitssamfunn, det er basert på tillit. Og vi vil gjerne følge den til det motsatte er bevist liksom."* Han forklarer videre at han anser nordmenn som lovlydige og at nordmenn i stor grad etterlever fastsatte regler og prosedyrer som virksomheten har, noe som anses som positivt. Informant M knytter norsk kultur til at nordmenn har en type "skjer ikke oss" holdning, noe han mener kan være en utfordring. Han forklarer det slik:

> *Det er litt med holdningen med storulykker; det skjer ikke meg, det skjer de andre. Også nå har jeg en statistikk på storulykker fra de siste tjue årene, og så ser jeg der og der skjedde det der. Neste år skjer det et annet sted, da må det ikke være her. Men det kan skje. Macondo, Kielland og Piper Alpha, det skjer ting ikke sant. Og In Amenas, var jo nære oss.*

Det fremkommer uenigheter om hvorvidt norsk kultur kan påvirke sikringskulturen i positiv eller negativ forstand, da informantene fremhever ulike aspekter ved norsk kultur som kan ha betydning for sikringskulturen.

Kunnskap

I empiren fremgår det at kunnskapsnivået omkring sikring er skjevfordelt. Informant G påpeker at kunnskapsnivået nivået er høyt på strategisk nivå, altså de som har funksjoner innen sikring, men lavt på operativt nivå. Dette knytter han opp til håndtering av sikringsscenarioer hvor de i linjen ikke vet hvordan de skal håndtere situasjoner når de først oppstår, og må dermed bed om råd fra strategisk nivå. Dette påstår han er en av forskjellene mellom safety og security, samt en av de største utfordringene med å utvikle en sikringskultur. Han forklarer det slik: *"Utfordringen med å utvikle en sikringskultur contra safety culture, er at linjen håndterer safety til daglig, mens securityhendelser er et fenomen som opptrer sjeldent."*

Organisering av sikring

I resultatene belyser informantene både fordeler og ulemper med hvordan selskapene organiserer sitt sikringsarbeid i forhold til arbeidet med å utvikle sikringskultur. Informant G meddeler at tidligere var sikring underlagt HSE, noe han anså som en ulempe fordi det medførte til at sikringsarbeidet bar preg av mangel på sikringskompetanse. Han hevder at det er behov for en funksjonell ledelse innen sikringsfagfeltet ettersom det er lite kunnskap både hos toppledelsen og i linjen, og dermed ser det som en fordel at selskapet har etablert en egen enhet for sikring. Dette mener han fører til større synlighet, noe han mener er positivt grunnet til at HSE ofte får mest oppmerksomhet. Også informant K påpeker at det er både fordeler og ulemper med å ha sikring underlagt HMS. Fordelen er at dersom sikring er underlagt HSE kan det være lettere å få dette inn som tema på møtene på lik linje med sikkerhet. Videre påpeker han at da må sikring bli en del av HSE begrepet, der sikring blir en ekstra S, altså HSSE. En annen fordel er at man allerede har en etablert organisasjon som er velkjent med HMS. Informanten påpeker at en ulempe derimot er at HMS ofte ses på som "mas", slik at ved å skille sikring fra HMS kan man lettere fokusere på den positive delen av sikring.

Fravær av intenderte uønskede hendelser

Læring fremstår som utfordrende i fravær av intenderte uønskede hendelser i bransjen generelt, og spesielt rettet mot virksomhetene. Flere påpeker at det er ikke så mange hendelser å lære fra. Blant annet hevder Informant E:

> *Når du ikke har hendelser, så er det vanskelig å lære kan du si. (...) Hvis du skal basere trusselen fremover basert på det du ser bakover, sant? Så har Norge vært i krig en gang. Så hvis du har en hendelse, skal du da… hvor mye skal du da bruke i beskyttelse? Og det er jo det som er utfordringen med sikringsfaget.*

Videre er det flere av informantene som fremhever at de skal ha en risikobasert tilnærming og at sikringstiltak må være tilpasset det trusselbildet de står ovenfor. En utfordring er dermed å finne denne balansen, og vite hvor mye tiltak man bør egentlig implementere. Flere av informantene påpeker at ofte så må en hendelse inntreffe for at sikring skal få et økt fokus i organisasjonen. Informant I meddeler, *"Så dessverre er det sånn at hendelser er ofte det som skal til for at vi er påvirket."* Dette er noe flere enes om. En av informantene viser til at de som gjør det best på sikring er de som har opplevd hendelser. Han forklarer det slik: *"Det er en sannhet at de selskapene som gjør det best på sikring, de har gått på en smell. Det er dessverre sånn. Hvis du ser på de selskapene som har ganske omfattende planverk."* Her refererer informanten til utenlandske aktører som gjerne har en annen risikoforståelse grunnet at de opererer i andre omgivelser, og dermed har sikring høyere på agendaen.

Mangelfull rapportering

I forhold til rapportering meddeler enkelte av informantene noen utfordringer knyttet til dette. Deriblant meddeler informant L at rapporteringsstatistikken kan ikke benyttes til å vurdere målet om "null sikringshendelser" ettersom han mener at man kan ikke stole på at tallene stemmer overens med virkeligheten. Han forklarer det slik:

> *Fordi rapportering er ikke alltid, en del rapporterer ikke for å unngå kjeft, unngå problemer (...) her i Norge er vi veldig beskyttet, men hvis vi tenker i Brasil eller UK eller andre, er det mye lettere å sparke personen dersom vi mener de har opptrådd på en helt feil måte, og dermed kan det være at folk ikke ønsker å rapportere for å beskytte seg selv.*

En utfordring er dermed å få oversikt over hvorvidt organisasjonen oppnår sine fastsatte mål samt å avdekke problemområder. Selskapet har et ønske og forventer at alle rapporterer sikringsrelaterte hendelser, samtidig kan frykten for konsekvenser

gjøre at de ansatte unnlater å rapportere sine feil. Dette gjør at statistikken kan være misvisende og gir begrenset mulighet for læring og forbedring. Videre fremgår det i empirien at det også kan oppstå sikringssituasjoner der ansatte kan unnlate å gripe inn. Informant K forklarer det slik:

> (...) *terskelen er kanskje ganske høy, men hvis det er noen som er i ferd med å gjøre noe galt i en sikringssammenheng, det kan være stjeling etter eller annet ikke sant. Så skal man da gripe inn? prøve å stanse dem? Det kommer an på hvor risikabelt det fremstår der og dra, å gripe inne og hvem er det man står ovenfor osv.*

Han understreker dermed viktigheten at de ansatte vet hvem de skal ringe slik at de kan få profesjonell hjelp til å håndtere situasjonen. Det fremkommer likevel ut ifra empirien at generelt opplever informantene en økning i både antall rapporterte hendelser i rapporteringssystemet og muntlige beskjeder og henvendelser fra de ansatte. Dette er noe de anser som et resultat av en økt bevisstgjøring og forbedring generelt i kulturen.

5.0 Drøft

I det følgende vil vi drøfte våre funn opp mot vårt teoretiske rammeverk for å kunne besvare vår problemsstilling. Drøftingen vil hovedsakelig bestå av tre deler, hvor den første tar for seg begrepet sikringskultur knyttet opp mot ulik terminologi, mens den andre delen tar for seg hva som inngår i sikringskulturbegrepet. Den tredje delen tar for seg elementer ved en optimal sikringskultur.

5.1 Ulik terminologi

Hvorvidt virksomhetene benytter begrepet sikringskultur eller kun sikkerhetskultur kan ses i lys av uenigheter og tvetydigheter knyttet til terminologi. Våre funn viser at noen oppfatter det som hensiktsmessig å skille mellom begrepene sikringskultur og sikkerhetskultur. Her vektlegges skillet mellom sikkerhet og sikring på samme måte som de engelske begrepene safety og security, hvorav sikkerhetskultur referer til safety culture og sikringskultur referer til security culture. Andre ser derimot på sikkerhet som et overordnet begrep, på lik linje som Aven et al. (2004) og benytter kun begrepet sikkerhetskultur, hvor sikringselementet inngår.

Pietre-Cambacedes og Chaudet (2010) viser til forskjeller mellom safety og security og påpeker viktigheten av en tydelig begrepsavklaring. Dette vektlegges for å unngå misforståelser og uklarheter når personer fra ulike fagmiljøer samhandler. Vi ser en tendens til at informantene bruker de norske og engelske begrepene om hverandre, noe som tyder på at de mangler en konsekvent begrepsbruk. Flertallet synes å foretrekke de engelske begrepene, hvor det blant annet påpekes at folk forstår bedre innholdet og forskjellene mellom safety og security, sammenlignet med de norske begrepene. Eksempelvis kommer det frem at når man skal samhandle med andre i bransjen, brukes de engelske begrepene for å skape klarhet. Videre fremkommer det at HMS blir ofte oversatt til HSSE på engelsk, noe som viser at begrepet sikkerhet benyttes på norsk for å dekke både safety og security. Det synes å være enighet om at sikring er det samme som security og dreier seg om beskyttelse mot intenderte uønskede hendelser. Likevel fremgår det uenighet og uklarheter om dette inngår i det bredere sikkerhetsbegrepet eller om det bør være adskilt slik som safety og security. Ved at ulike fagpersoner benytter seg av ulike begreper, kan dette medføre til uklarhet og misforståelser når de samhandler. Dersom sikkerhetskulturbegrepet benyttes for å

både omtale safety culture og security culture, er det ikke tydelig hvilket av disse begrepene som er i fokus. Dermed kan det tyde på at de som benytter sikringskulturbegrepet gjør dette bevisst for å unngå misforståelser, samtidig som det fremkommer at eksponering for security terminologi over tid er viktig i utvikling av en sikringskultur. De som benytter begrepet vektlegger også at det er forskjeller mellom sikkerhet og sikring, på lik linje som safety og security, som knytter seg til intensjonsbegrepet. Dermed blir det i deres syn viktig å ha to begreper.

I resultatene fremgår det at de som benytter begrepet sikringskultur understreker at virksomheten har en lang vei å gå i utvikling av en slik kultur. Flere av informantene påpeker derimot at sikkerhetskulturen i selskapet er svært velutviklet da dette arbeidet har pågått over mange år, hvor fokuset har tradisjonelt vært rettet mot uintenderte uønskede hendelser. Dersom virksomheten benytter begrepet sikkerhetskultur som et overordnet begrep kan det tenkes at denne "suksessen" kan overskygge sikringselementet, da dette kun ses som en del av det totale HMS arbeidet. Det kan dermed synes å være problematisk å kun benytte ett begrep som skal dekke både safety culture og security culture, hvor det ikke tydelig fremkommer hvilket aspekt man snakker om.

Selv om de fleste av virksomhetene har sikringsavdelingen underlagt HMS avdelingen, er det flere av disse som har tatt sikringskulturbegrepet i bruk og ser det som hensiktsmessig med et slikt begrep. Igjen knyttes dette ofte til at man oversetter begrepene safety og security til sikkerhet og sikring, selv om dette kan synes å motsi hvordan sikringsarbeidet er organisert. Ved å ha sikring underlagt HMS tyder det på at sikring forstås som en del av sikkerhetsbegrepet, likevel benytter flere av informantene sikkerhet for safety og sikring for security. Igjen viser det tvetydigheter og forvirringer omkring begrepene, og mangel på konsekvent begrepsbruk. Et spørsmål som reiser seg i den forbindelse er om det er mer hensiktsmessig å benytte de engelske begrepene safety culture og security culture, da det synes å gjøre det tydeligere hva fagpersoner egentlig snakker om. Resultatene viser at det oppstår en forvirring omkring de norske begrepene og dermed ulike oppfatninger omkring sikkerhetskultur- og sikringskulturbegrepet. Variasjon i oppfatninger av terminologi i bransjen kan videre representere en utfordring i forhold til sikkerhets- og sikringsarbeidet. Det blir i denne sammenheng også viktig å poengtere at til tross for

at noen ikke har tatt sikringskulturbegrepet i bruk betyr ikke dette nødvendigvis at de har noe imot begrepet. Det kan heller synes at for enkelte av informantene fremstår begrepet generelt som nytt og at de har dermed ikke et forhold til begrepet per dags dato.

Uavhengig om begrepet sikringskultur benyttes eller om virksomhetene kun benytter sikkerhetskultur som et overordnet begrep, fremkommer det at virksomhetene på generell basis anser en god kultur som en forutsetning for å oppnå et tilstrekkelig sikringsnivå, hvor fysiske og tekniske barrierer ikke alene er tilstrekkelige. Dette kan ses i tråd med at både myke og harde sikringshjelpemidler er nødvendige og må ses i en sammenheng for å oppnå et godt sikringsarbeid, på lik måte som i sikkerhetsarbeidet (Nordby & Hansen, 2005). Også litteratur om informasjonssikringskultur fremhever at informasjonssikring er mye mer enn å anvende fysiske og tekniske tiltak, hvor utvikling av en kultur er helt essensielt for å kunne beskytte informasjonen til virksomheten (Thomson et al., 2006). Et viktig spørsmål er hvorvidt det å ha et bevisst forhold til sikringskulturbegrepet har noe å si for kulturbyggingen i virksomheten.

5.2 Forståelse av sikringskulturbegrepet

5.2.1 Nivåer av kultur

Til tross for at ikke alle virksomhetene benytter seg av begrepet sikringskultur, har flere en oppfatning og tolkning av begrepet. I våre resultater fremgår at de som ikke benytter sikringskultur begrepet synes i stor grad å vektlegge etterlevelse av regler og prosedyrer hvor fokus synes å være på atferd. Dette kan ses i lys av Schein sin trenivås modell der fokuset er på det øverste og synlige nivået (Schein, 2010). Til tross for at holdninger nevnes, eksempelvis "HMS holdninger," blir det i liten grad utdypet hvilke typer holdninger som er ønskelig i en sikringskontekst. De som benytter seg av begrepet derimot synes i større grad å vektlegge de dypere nivåene av kultur og dermed ser ut til å ha et mer reflektert forhold til hva som legges i sikringskulturbegrepet. Her vektlegges i stor grad kompetanse, bevissthet og ansvarsfølelse, hvor det understrekes at kultur er mer enn kun etterlevelse av regler og prosedyrer. På lik linje fremhever litteraturen at det er langt mer hensiktsmessig å fremme en kultur som stimulerer til sikringsrelatert atferd gjennom kunnskap,

artefakter, verdier og antagelser, heller enn å pålegge de ansatte en viss atferd gjennom regler og prosedyrer (Thomson et al., 2006). Det kan tenkes at dersom fokuset er kun på regler og prosedyrer vil ikke disse nødvendigvis oppleves som meningsfulle og de ansatte kan dermed bevisst velge å motarbeide tiltakene. Informantene synes å vektlegge at de ansatte skal tenke selv og at denne sikringstankegangen skal komme naturlig. Med dette fremheves at kulturen skal være selvgående og at ansatte selv skal ta initiativ til sikring. På lik linje hevder Thomson et al. (2006) at sikringspraksiser må være en naturlig del av de ansattes atferd. Dette kan videre ses i tråd med det tredje nivået i Scheins kulturmodell som består av underliggende antagelser som ofte er ubevisst og "tatt for gitt" av organisasjonens medlemmer. En optimal sikringskultur vil dermed oppnås når man har fått til en endring i de underliggende antagelsene til medlemmene i organisasjonen. Dette utgjør kjernen i kulturen som videre er avgjørende for de ansattes atferd, holdninger og oppfatninger (Schein, 2010). En slik forståelse av kultur innebærer at kulturendring er en tidkrevende prosess som krever vedvarende fokus og en forståelse for kulturen som skal endres.

Sikringskultur blir med dette forstått som et mer omfattende begrep, hvor underliggende antagelser, verdier, holdninger og atferd inngår og må ses i en sammenheng. Å ta hensyn til de dypere nivåene av kultur er viktig ettersom endringer i observerbare artefakter er ingen garanti for at normer, verdier og grunnleggende antagelser har endret seg (Haukelid, 2001). Dette betyr at atferden i organisasjonen ikke nødvendigvis gjenspeiler holdninger og verdier blant de ansatte, og at det dermed ikke er gitt at man har en "optimal" sikringskultur. Dette fordi våre funn tyder på at sikringskultur dreier seg om at ansatte bryr seg om sikring og tar det på alvor, hvor målet er at dette skal være selvgående. Samtidig vil slike underliggende antagelser, holdninger og verdier blant ansatte kunne påvirke grad av etterlevelse og sikringsrelatert atferd, slik at dersom man får til en endring på disse nivåene kan man i større grad oppnå ønsket atferd i organisasjonen. Det fremheves blant annet i våre funn at man ikke kan kontrollere alle ansatte gjennom regler og prosedyrer, og dermed må man stole på at de ansatte har de riktige holdningene og verdiene slik at de handler som ønsket. Likevel kan det stilles spørsmål til hvorvidt det er mulig å påvirke disse nivåene av kultur og dermed utvikle en optimal sikringskultur. Blant annet er det viktig å understreke at en organisasjon kan bestå av flere subkulturer som

kan gå på tvers av strukturer, yrker, avdeling og som påvirkes av både interne og eksterne faktorer (Richter & Koch, 2004). Dette kan anses som problematisk ved utvikling av en sikringskultur, som oppfattes som noe felles og kollektivt. Likevel er det snakk om et aspekt av organisasjonskulturen, hvor man ønsker å påvirke de ulike nivåene av kulturen som har betydning for sikringsnivået i organisasjonen. På lik linje som Haukelid (2001) som fokuserer på sikkerhetskultur, mener vi at man kan gå svært langt i forhold til påvirkning og ulike tiltak når det gjelder utvikling av en sikringskultur. Samtidig er det viktig at ansatte finner tiltakene meningsfulle, og kunnskap og forståelse for sikring vil da spille en viktig rolle. Til tross for at kultur anses som noe mer enn atferd, påpekes det i litteraturen at endringer i atferdsmønstre over tid kan føre til kulturendring når disse blir tatt for gitt som riktig av organisasjonens medlemmer (Nordby & Hansen, 2005). Å inneha en forståelse for at kultur "eksisterer" på ulike nivåer hvor man også tar hensyn til de dypere nivåene er, ifølge teorien, nødvendig for å få til en varig kulturendring, og her vil forståelse av kultur spille inn. Hvilket nivå informantene fokuserer på kan tyde på ulikt kunnskapsnivå, oppfatninger og forståelser for kulturbegrepet, noe som kan tenkes å ha betydning for kulturbyggingen tilknyttet til sikringsarbeidet.

5.2.2 Kunnskapsdimensjonen

I våre funn fremkommer det at forståelse og kompetanse vektlegges i utvikling av en kultur som støtter opp sikringsarbeidet. Dette er noe virksomhetene vektlegger gjennom opplæringsprogrammer, informasjonsdeling og ulike bevisstgjøringskampanjer. Det synes dermed at kunnskapsdimensjonen vektlegges med den antagelsen at dette vil påvirke atferd, verdier og holdninger knyttet til sikring. Videre kan dette ses i tråd med teori om *information security culture*, hvor kunnskapsdimensjonen anses som helt sentralt for å støtte opp de tre nivåene av organisasjonskultur, fra underliggende antagelser, verdier og holdninger til atferd (Van Nierkerk & Von Solms, 2010). Teorien vektlegger at ansatte må ha kunnskaper om hvordan de skal utføre sine arbeidsoppgaver på en sikker måte, samt inneha en forståelse for sine roller og ansvarsområder (Thomson et al., 2006). Samtidig fremhever litteraturen at mangel på kunnskap er et av de største problemene når det gjelder beskyttelse av informasjon i virksomhetene. Selv om Thomson et al., (2006) fokuserer på informasjonssikring, ser vi at kunnskapsdimensjonen er også viktig i en bredere sikringskontekst. Ansatte må vite hvordan de skal opptre på en sikker måte,

men også vite hvorfor sikring er viktig. Dette innebærer at man må vite hvilke verdier virksomheten ønsker å beskytte, samt hvilke trusler virksomheten står ovenfor. Det fremgår dermed at sikringskultur er noe som omfatter alle i organisasjonen, da alle ansatte kan bidra både positivt og negativt til virksomhetens sikringsnivå. Dette kan ses i sammenheng med at sikring er forbundet med en høy grad av usikkerhet (Albrechtsen, 2003) hvor risikoen er i større grad ukjent for organisasjonen og kan oppstå både internt og eksternt (Pietre-Cambacedes & Claudet, 2010). Ved at en trusselaktør vil søke de beste strategier for å skade virksomheten (Reniers et al., 2006), representerer alle ansatte en mulig risiko. Slik som informantene forklarer er mennesker både selskapets sterkeste og svakeste ressurs. På den ene siden kan alle ansatte være viktige bidragsytere ved å "fange" opp faresignaler og mistenksomheter. På den andre siden kan de også begå sikringsbrudd eller andre feilhandlinger, og på denne måten utgjøre en risiko for virksomheten. Alle ansatte må ha derfor ha kunnskap om hvordan de som enkeltpersoner kan bidra til å øke sikringsnivået og hvordan deres feilhandlinger kan få konsekvenser for sikring av virksomhetens verdier og omdømme. Sikringskultur er dermed ikke noe som er forbeholdt sikringsfagfolkene og ledelse, selv om disse anses som viktige kulturbærere. Dette betyr ikke at alle har en like stor rolle i sikringsarbeidet, men at ansatte må ha den kunnskapen som er nødvendig for at de skal bidra positivt til sikringen.

Våre funn tyder på at kunnskap vil også være viktig for å skape forståelse for nødvendigheten av sikringstiltakene, noe som kan føre til en høyere grad av aksept for dem. Dette kan ses i tråd med behovet for at ansatte har kjennskap til, forståelse for, samt aksepterer tiltakene som virksomheten implementerer (AlHogail, 2015). Her spiller informasjonsdeling og kommunikasjon ut til de ansatte en viktig rolle, blant annet i forhold til å holde ansatte oppdatert på de aktuelle truslene virksomheten står ovenfor. Van Nierkerk og Von Solms (2010) anbefaler bruken av security awareness kampanjer for å sikre et tilfredstillende kunnskapsnivå blant ansatte. På lik linje fremkommer det i empirien at kunnskap og security awareness, her forstått som sikringsbevissthet, er nært beslektet og gjensidig avhengig av hverandre. Både funn og teori omtaler sikringsbevissthet som et nøkkelelement i utvikling av en sikringskultur (Talbot & Jakeman, 2009, Van Nierkerk & Von Solms, 2010) og informantene synes å bruke begrepene om hverandre. Det fremstår likevel tvetydigheter omkring hva som legges i begrepet sikringsbevissthet, men flere synes å

enes om at det handler om å ha sikring i "bakhodet" og at man sier ifra dersom man ser noe som avviker fra normalen. Sikringsbevissthet kan dermed forstås som en slags overvåkenhet og oppmerksomhet til fange opp slike avvik, samt en vilje til å handle basert på dette.

5.2.3 Ansvarsfølelse

I tillegg til sikringsbevissthet og kunnskap fremgår det i resultatene viktigheten av at ansatte bryr seg om og tar sikring på alvor, noe som kan tolkes som at ansatte føler et ansvar og en forpliktelse til sikringen. Litteratur om informasjonssikringskultur understreker at i tillegg til mangel på kunnskap, er mangel på forpliktelse blant ansatte et av de største problemene virksomheter opplever i forbindelse med beskyttelse av informasjon (Ruighaver et al., 2006). En utfordring som fremkommer i våre funn er at ansatte ikke tar sikring på alvor samt mangler en forståelse for sikringstiltak. I den forbindelse vektlegger både teori og funn viktigheten av at ansatte har et eierskap til sikring, noe som kan oppnås gjennom å delegere ansvar nedover i organisasjonen (Ruighaver et al., 2006). Virksomhetene legger dermed vekt på at sikring er "everybody's responsibility" hvor det vektlegges at sikring er noe man skal oppnå i et felleskap. Igjen understrekes viktigheten av at alle har en rolle og må bidra dersom man skal lykkes med sikringsarbeidet, og her kulturen spiller inn. I resultatene knyttes manglende ansvarsfølelse til mangelfull aksept og etterlevelse av prosedyrer, noe som kan tenkes å gjøre virksomheten mer sårbar. Dermed ser man et behov for at menneskene har de riktige holdningene ettersom dette kan være styrende for atferd. En rekke av informantene anser dette som en av de største utfordringene i sikringsarbeidet, da mennesker ofte velger de letteste løsninger som gagner "jeg-et". Ettersom sikringstiltak til tider oppleves som begrensende for ansatte, kan dette ha betydning for hvorvidt de velger snarveier eller ikke (Ruighaver et al., 2006). Igjen blir det sentralt å ta hensyn til de dypere nivåene av kultur, da ansvarsfølelse og forståelse for tiltak vil spille en viktig rolle for om ansatte etterlever prosedyrene eller ikke. Hvorvidt ansatte føler et ansvar for sikring kan videre knyttes til motivasjon, hvor teorien tyder på at de ikke har en iboende motivasjon til å adoptere sikringspraksiser (Ruighaver et al., 2006). Dette kan gjøre arbeidet med å utvikle en sikringskultur spesielt utfordrende, noe som også støttes av våre funn. Desto viktigere blir det at ansatte har et eierskap til sikring, noe som kan oppnås gjennom at ledelsen delegerer ansvar ut i organisasjonen (Ruighaver et al., 2006), og slik sett blir

ansvarsfølelse et viktig kjennetegn ved en optimal sikringskultur. Til tross for at teorien vektlegger motivasjon gjennom belønning og erkjennelse, fremgår ikke dette tydelig ut ifra våre funn.

5.2.4 Sikringsbevissthet

Sikringskulturbegrepet synes å omfatte kunnskap, forståelse og ansvarsfølelse som antas å påvirke atferden i organisasjonen. En interessant bemerkelse er at sikringsbevissthet synes å anses som et nøkkelelement til utvikling av en sikringskultur, noe som fremgår både i teori og funn. Som nevnt ovenfor blir sikringskultur og sikringsbevissthet brukt om hverandre, og i denne sammenheng blir det viktig å stille spørsmål om sikringskultur er det samme som sikringsbevissthet? Det vil si dersom alle ansatte innehar en tilstrekkelig sikringsbevissthet kan man da si at man har en optimal sikringskultur? Ettersom både funn og teori vektlegger at de ansatte innehar en forståelse, at de er motiverte og føler et ansvars- og eierforhold til sikringen i virksomheten, kan det argumenteres at sikringsbevissthet blir et for snevert begrep. Dermed anser vi ikke at sikringskultur begrepet kan "reduseres" til sikringsbevissthet eller "security awareness." Til tross for at sikringsbevissthet er viktig, er det ikke dermed gitt at bevissthet fører til aksept for tiltakene, altså at man etterlever regler og prosedyrer. Samtidig fremhever både funn og teori at aksept er en forutsetning for oppnå et høyt nivå av sikring i virksomheten (AlHogail, 2015). Det fremstår dermed som en forenkling å si at sikringskultur er det samme som "security awareness", men at dette likevel er en av forutsetningene for å utvikle en optimal sikringskultur.

5.2.5 Sikringskultur - en felles kultur

Resultatene viser at virksomhetene står overfor et bredt spekter av trusler, hvor sikringsbegrepet brukes for å dekke de tre nevnte sikringsområdene; informasjonssikring, personell sikring og fysisk sikring. På denne måten vil også sikringskulturbegrepet omfatte de tre domenene og eventuelt andre områder som er relevante for virksomheten. Et spørsmål i denne sammenheng er hvorvidt man bør snakke om en felles sikringskultur eller for eksempel en kultur for informasjonssikring og en for beskyttelse mot terroranslag? I denne forbindelse bør det understrekes at vi bruker sikringskulturbegrepet konseptuelt for å omhandle aspekter av organisasjonskulturen som påvirker sikringsnivået i en eller annen

retning. Ved en slik tankegang vil en informasjonssikringskultur bare være et aspekt av sikringskulturen, og det er derfor ikke snakk om "separate" kulturer. Om det er hensiktsmessig eller ikke å snakke om eksempelvis en "informasjonssikringskultur" kan ses i forhold til viktigheten av å ha en helhetlig tilnærming til sikring, hvor man bør se de tre domenene i en sammenheng. Både teori og funn synes å vektlegge en slik tilnærming til sikring, hvor informantene fremhever at det er viktig å bygge en sikringskultur som tar hensyn til alle aspekter ved sikring. Dette kan også ses i sammenheng med viktigheten av å unngå en slags "silotenkning" hvor hver avdeling fokuserer utelukkende på sitt eget domene. Trusler kan oppstå i alle domenene samt gå på tvers eller bevege seg fra ett domene til ett annet. Dette kan knyttes til at man står ovenfor et bredt spekter av trusler, samtidig som det er svært vanskelig å forutse og kontrollere eksterne trusler (Albrechtsen, 2003). Dette får støtte fra litteraturen som påpeker at ved å overse bestemte områder, kan dette være svært ødeleggende for den totale sikringen i virksomheten (Ruighaver et al., 2006). Dermed blir en helhetlig tilnærming og samarbeid på tvers av avdelinger sentralt i utvikling av en optimal sikringskultur som støtter opp det totale sikringsnivået i virksomheten.

Basert på diskusjonen ovenfor omhandler sikringskultur i stor grad underliggende antagelser, holdninger, verdier, oppfatninger, og atferd som har betydning for sikringsnivået i virksomheten. Dermed synes våre funn å gi støtte til Malcolmson (2009) sin definisjon av sikringskultur, som fanger opp de ulike nivåene i Schein sin modell:

> *Security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organisation, and behaviours they perform, which could potentially impact on the security of that organisation, and that may, or may not, have an explicit, known, link to that impact* (Malcolmson, 2009, s. 361).

I tillegg til dette ser vi at kunnskapsdimensjonen er svært sentral i forhold til å påvirke og støtte opp disse nivåene, hvor kunnskap og sikringsbevissthet er nært beslektet. Kunnskap anses som spesielt viktig i en sikringskontekst da det kan tenkes at sikringstankegangen ikke er intuitiv sammenlignet med sikkerhetstankegangen, hvor, ifølge Albrechtsen (2003) farer er i større grad kjente, forutsigbare og observerbare.

Kunnskap og sikringsbevissthet synes å være nødvendig for å skape forståelse og ansvarsfølelse for sikringen, samt til å utvikle et tankesett som innebærer at menneskene reflekterer over sin egen atferd og hvordan de selv kan bidra til å styrke sikringsnivået. Dette antas videre å ha betydning for atferden i organisasjonen, herunder aksept for sikringstiltak. Ved å rette fokus mot de ulike nivåene av kultur, kan det antas at over tid vil atferd, holdninger og verdier kunne bevege seg nedover til det mer ubevisste, og dermed bli "tatt for gitt" som riktige av organisasjonens medlemmer. En slik forståelse av sikringskultur innebærer at det vil i praksis være vanskelig å oppnå, noe som krever kontinuerlig fokus og tålmodighet samt gjennomtenkte tilnærminger hvor det tas hensyn til at organisasjonen består av ulike subkulturer hvor medlemmene kan ha ulike fortolkninger og meninger om sikring.

Slik som organisasjonskultur, må sikringskultur ses i sammenheng med organisasjonens strukturer, systemer og prosesser, da det er samspillet mellom disse som påvirker hvordan organisasjonen presterer (Guldenmund, 2000). Det fremgår i empirien at det er viktig å finne en balansegang mellom gjeldende risikonivå og implementerte sikringstiltak. Blant annet vektlegges at man må unngå "security overload" og at sikring er noe som skal være minst mulig synlig og til hinder, men samtidig gjøre jobben med å sikre verdier. Dermed fremheves det at strukturelle prosesser og systemer kan ha betydning for sikringskulturen og slik sett blir det viktig å se disse i en sammenheng da dette vil til sammen påvirke det total sikringsnivået i virksomheten.

5.2.6 Oppsummering

Resultatene viser tvetydigheten knyttet til kulturbegrepet, samt at sikringskultur begrepet fremstår som et relativt nytt og umodent begrep for en rekke av selskapene. Det fremkommer også et varierende oppfatninger og forståelser knyttet til kulturbegrepet, hvor enkelte synes å fokusere i større grad på atferd og etterlevelse av regler, mens andre har i tillegg fokus på holdninger, verdier og antagelser. Vi ser at det fremkommer en begrepsforvirring og uenighet i forhold til oppfatning av begrepene sikring og sikkerhet, noe som kan synes å ha betydning for om sikringskulturbegrepet er tatt i bruk i virksomheten eller ikke. Ulike forståelser av sikkerhetskultur og sikringskultur kan videre føre til misforståelser og uklarheter i forhold til om man mener safety eller security når fagpersoner samhandler. Samtidig

er det viktig å skille mellom disse ettersom det er flere ulikheter mellom dem, blant annet knyttet til intensjonsbegrepet. Det kan stilles spørsmål om bruk av sikkerhetskultur som overordnet begrep kan medføre at sikringskultur-elementet blir glemt.

Uavhengig om virksomhetene skiller mellom sikringskultur og sikkerhetskultur, arbeider alle i ulik grad med kulturbygging som kan støtte opp sikringsarbeidet. Noe som henger sammen med at sikringskultur er ikke noe som eksisterer separat fra organisasjonskulturen, men er heller en integrert del av den. Likevel tyder resultatene på at de som benytter begrepet synes å ha et mer reflektert forhold til skille mellom safety og security, samt hva som legges i begrepet sikringskultur. Her vektlegges blant forståelse, ansvar og bevissthet knyttet til sikring, hvor kunnskapsdimensjonen synes å være sentral i forhold til utvikling av en optimal sikringskultur. Videre synes de som benytter begrepet også å ha et mer bevisst forhold til å stimulere til en kultur som støtter opp sikringsarbeidet i virksomheten, hvor initiativ og tiltak er rettet mot de overnevnte kvalitetene. Resultatene viser at sikringskultur er ikke noe som kan reduseres til et enkeltbegrep som "sikringsbevissthet," til tross for at dette anses som helt sentralt ved en optimal sikringskultur. Kultur består av flere nivåer, og dermed vil sikringskultur omfatte alt fra atferd, holdninger, til de mer underliggende antagelsene som tilsammen påvirker sikringsnivået til virksomhetene på kjente eller ukjente måter. Man må derfor ta hensyn til alle nivåene, med et mål om å påvirke de underliggende antagelser som medfører at sikringstankegangen kommer naturlig. Dette er ikke noe som oppnås "over natten" eller ved å forsøke å "pålegge" ansatte verdier og atferd uten at de forstår viktigheten av sikring.

5.3 Elementer ved en optimal sikringskultur

I det foregående har vi fokusert på hva som legges i begrepet sikringskultur hvor fokus har vært på atferd, holdninger, verdier og underliggende antagelser. Samtidig påpekte vi at de kulturelle aspektene må ses i sammenheng med de strukturelle aspektene da disse påvirker hverandre og vil tilsammen utgjøre sikringsnivået. I det følgende vil vi drøfte våre funn opp mot de forhåndsdefinerte elementene om hva som kan forventes å være elementer ved en optimal sikringskultur, basert på vår teoretiske rammeverk. Her er fokus i større grad rettet mot kollektive praksiser og hvordan dette

henger sammen med strukturer og prosesser i organisasjonen. Disse elementene er som nevnt tidligere *forpliktelse, fleksibilitet, læring* og *tillit*.

5.3.1 Forpliktelse

I resultatene fremkommer det at alle informantene vektlegger i stor grad ledelsens forpliktelse til sikring som en forutsetning for å kunne utvikle en optimal sikringskultur. Her blir ledere blant annet omtalt som rollemodeller og kulturbærere i organisasjonen. Deres syn kan ses i tråd med en mengde teori innenfor både organisasjonskultur, sikkerhetskultur og informasjonssikringskultur feltet. Blant annet hevder Schein (1987) at ledere er noen av de viktigste kulturskaperne i en organisasjon, og at de kan påvirke kulturen gjennom hva de retter oppmerksomhet mot, samt hva de måler og kontrollerer i organisasjonen. Ifølge Schein (1987) vil dette kommunisere verdier og holdninger til de ansatte, noe som kan tenkes å brukes bevisst for å utvikle en god sikkerhetskultur. På lik linje viser resultatene at dette også vektlegges i en sikringskontekst. Det kommer frem i empiren at flere oppfatter det slik at dersom ledelsen ikke bryr seg om sikring og tar dette på alvor, vil de ansatte heller ikke bry seg. Videre fremheves det at ledere må uttrykke deres forpliktelse både gjennom ord og handling. Dermed blir signalene som ledelsen sender, samt hvordan de ansatte oppfatter dette sentralt, noe også Zohar (2003) påpeker som viktig i utvikling av en sikkerhetskultur. I den forbindelse blir det sentralt at ledelsen ikke sender motstridende signaler i forhold til prioriteringer som gjøres.

Flertallet av informantene synes å se på utvikling av en sikringskultur som en top-down styrt prosess. Dette kan ses i tråd med Dejoy (2005) som vektlegger at endring av verdier, holdninger og atferd på ledelsesnivå kan "sildre" ned i organisasjonen og føre til kulturendring. I empiren understrekes det viktigheten av at ledere tar ansvar og eierskap til sikringen da dette vil forplantes nedover i organisasjon over tid. Videre vektlegges linjeledelsen sin rolle, der de har et ansvar å formidle budskapet ut i avdelingene, og på den måten kan også ses som kulturbærere. Basert på empirien synes ledelsesengasjementet å bli oppfattet som et "middel" eller "verktøy" for å utvikle en optimal sikringskultur, noe som kan tyde på en til dels funksjonell tilnærming til sikringskultur. Samtidig vektlegger teori om sikkerhetskultur at ledelse er ikke *alt*, og at det er viktig at endringsprosessen skjer gjennom samarbeid og dialog

mellom ledelsen og ansatte (Haukelid, 2001). Det advares videre mot forsøk på å presse verdier og mål over hodet til ansatte, hvor det påpekes at de på gulvet kan bevisst sabotere tiltak dersom de ikke oppleves som meningsfulle. Litteraturen påpeker at det er vanskelig å endre holdninger og verdier til ansatte, og at dette krever et vedvarende engasjement fra ledelsens side (Nordby & Hansen, 2005), noe informantene synes også å enes om. Flere fremhever at kultur skapes ikke over natten, og er heller ikke noe som vedtas. Med tanke på manglende forståelse for sikringstiltak blant ansatte, blir det desto viktigere med et kontinuerlig engasjement og ledelsesforpliktelse til sikring. I denne forbindelse kan det stilles spørsmål til hvorvidt ledelsen evner å demonstrere et slikt engasjement over tid.

Flere av informantene forklarer at det har til tider vært en kamp å overtale ledelsen om å prioritere sikring. Dette kan ses i sammenheng med at ledere vil ofte stå overfor ulike målsetninger, blant annet produktivitet (Reason, 1997). Ettersom informantene forklarer at sikring ofte ses på som en utgiftspost, samtidig som alvorlige sikringshendelser er et sjeldent fenomen (Pettersen & Bjørnskau, 2014), kan dette tenkes å føre til en nedprioritering av sikringstiltak. Fravær av hendelser kan føre til at risikoen oppleves som så lav at sikringstiltakene ikke kan forsvares kostnadsmessig. Reason (1997) referer til "unrocked boat", som viser til at tiltak vil ofte iverksettes som følge av en ulykke, og etterhvert nedprioriteres når virksomheten opplever et fravær av ulykker. Mye tyder på at dette også kan være tilfelle i forhold til sikringsarbeidet blant operatørselskaper. Flere av informantene oppfatter at de som gjør det best på sikring er ofte de som har opplevd alvorlige hendelser. Samtidig påpeker informantene viktigheten av at organisasjonen har en risikobasert tilnærming og at sikringstiltak er tilpasset det gjeldende trusselnivået. I hvilken grad trusler oppfattes som reelle av ledelsen, kan dermed ha noe å si for hvorvidt sikringstiltak anses som nødvendige, og i hvilke grad sikring prioriteres i virksomheten.

Et sentralt kjennetegn ved HRO er at sikkerhet settes som høyeste mål i organisasjonen (Aven et al., 2004). Empiri viser at en utfordring i forbindelse med sikringsarbeidet er at det kan oppstå målkonflikter mellom HMS og sikring, hvor det fremkommer at HMS som regel vil vinne. Også Reniers et al. (2011) påpeker at sikkerhetstiltak kan i enkelte tilfeller påvirke sikringsnivået negativt. Det fremkommer i empiri at det kan forekomme tilfeller hvor man må kjempe for å få

gjennomslag for sikringstiltak fordi det oppfattes å kunne påvirke sikkerheten negativt. I tilfeller hvor ledelsen velger å prioritere sikkerhet, kan dette sende ut signaler om at sikkerhet er hovedfokuset, og at sikring kommer i andre rekke. Det kan tenkes at slike signaler kan videre påvirke de ansattes forpliktelse til sikring da de vil oppfatte sikkerhet som viktigere. En slik målkonflikt representerer et mulig dilemma for ledelsen, spesielt når informantene viser til at både sikkerhet og sikring har som overordnet mål å forhindre skade på menneske, materielle verdier og miljø. Videre fremgår i funn viktigheten av at sikring tas opp på lik linje som sikkerhet på allmøter og lignende, og er en av måtene ledelsen kan tydeliggjøre sin forpliktelse til sikring.

Til tross for at resultatene indikerer at ledelsesforpliktelse til sikring er en forutsetning for å utvikle en optimal sikringskultur, fremkommer det at et fåtall av virksomhetene har utarbeidet en eksplisitt security policy. Dette kan være problematisk ettersom konseptene fra litteraturen fremhever at ledelsens forpliktelse må være synlig overfor de ansatte og balansert med andre organisatoriske mål (Jeffcott et al., 2006). En av informantene uttrykker at alle oljeselskaper som opererer internasjonalt bør ha en security policy på lik linje som HMS og kvalitetspolicy. Dette blir videre støttet av teori om *information security culture,* som hevder at ledelsen må demonstrere sitt engasjement ved å vise støtte og forpliktelse til en "Information Security Policy" (Thomson et al., 2006). Dette kan også ses på som viktig i forhold til å vise at sikring er høyt på agenda på lik linje som andre organisatoriske mål i selskapet. Videre kan det bidra til å gjøre ansatte mer kjent med sikringsterminologi, noe som understrekes i våre funn som viktig i utviklingen av en sikringskultur. Om selskapet har en security policy eller ikke kan signalisere overfor ansatte hvorvidt ledelsen prioriterer sikring og opplever trusler som reelle, noe som kan ha betydning for sikringskulturen. Blant annet forklarer Malcolmson (2009) at enkelte aspekter av sikringskulturen utvikles i møte med organisasjonens trusler som blir forfektet av ledelsen, noe som blant annet kommer til uttrykk gjennom organisasjonens sikringspraksiser og styrende retningslinjer. Ledelsens opplevelse av trusler blir dermed sentralt. Samtidig som flere mangler en security policy, viser likevel et flertall av informantene til sikringsprinsipper og at sikring inngår i deres HMS program, noe som også kan være en indikasjon på ledelsens forpliktelse. Det fremkommer likevel variasjon i hvorvidt dette kommuniseres ut til de ansatte.

Teori om sikkerhetskultur vektlegger viktigheten av at ledelsen samhandler med de i den skarpe enden for å utvikle en realistisk forståelse for, og sensitivitet overfor operasjoner (Jeffcott et al., 2006). Dette kan ses i lys av at risiko i en sikkerhetssammenheng oppstår som regel i forbindelse med operasjoner og håndteres dermed i stor grad på operasjonelt nivå. Slik sett blir samhandling sentralt for at ledelsen skal ha en tilstrekkelig situasjonsforståelse og oversikt over operasjonene. Dette anses som viktig for å kunne fange opp mulige fremtidige feil og er noe HRO retter stor innsats mot (Weick et al., 1999). Det fremkommer i resultatene at informantene legger vekt på det å kunne forstå trusselbildet som et sentralt kjennetegn ved en optimal sikringskultur, noe som videre kan tolkes som en situasjonsforståelse. Her er det derimot andre mekanismer som må være til stede, utover samhandling mellom ledelse og de i linjen, noe som skiller seg fra en sikkerhetskontekst. Ettersom sikringsrisiko kan både oppstå eksternt og internt (Reniers et al., 2011), er det ikke nødvendigvis at informasjon om faresignaler og trusler er knyttet til operasjoner og kommer fra de i den skarpe enden. Derimot synes samhandling mellom ledelse og virksomhetens sikringsansvarlig som avgjørende i forhold til at ledelsen skal oppnå en tilstrekkelig situasjonsforståelse og ta nødvendige sikringsrelaterte beslutninger. Sikringsansvarlig vil besitte viktig informasjon som kan ha betydning for sikringen, eksempelvis gjennom samarbeid med myndigheter, som må videreformidles til ledelsen slik at de er informert til enhver tid. En utfordring i den forbindelse kan være at informasjon i noen tilfeller er begrenset, eksempelvis på grunn av manglende sikkerhetsklarering blant ledelsen. I slike tilfeller må lederen stole på sikringsansvarlig og være villig til å handle basert på informasjonen som er tilgjengelig. Ettersom informasjonen er forbundet med høy grad av usikkerhet og trusselbildet kan endre seg raskt (Albrechtsen, 2003), kan det være spesielt utfordrende å oppnå en tilstrekkelig situasjonsforståelse i en sikringskontekst. HRO kjennetegnes ved at de retter stor innsats mot å oppnå nettopp dette (Weick et al., 1999), noe som krever forpliktelse hos ledelsen.

Oppsummering av forpliktelse

Både våre funn og teori støtter opp at ledelses engasjement og forpliktelse er en forutsetning for utvikling av en optimal sikringskultur. Ledelsen må demonstrere overfor de ansatte at de prioriterer sikring, noe som videre må balanseres med andre organisatoriske mål. Funn viser at i enkelte tilfeller kan sikring kollidere med HMS,

hvor HMS ofte vinner i en eventuell målkonflikt. Dette kan ses i sammenheng med at det er et fravær av intenderte uønskede hendelser, samt at det er vanskelig å måle effektiviteten av sikringstiltak (Pettersen & Bjørnskau, 2014). Signalene som ledelsen sender til de ansatte vil videre ha betydning for hvorvidt de ansatte tar sikring på alvor, noe som igjen kan påvirke grad av aksept og etterlevelse. Videre synes samhandling mellom ledelsen og sikringsansvarlig å være helt sentralt for å kunne oppnå en realistisk situasjonsforståelse for truslene virksomhetene står ovenfor. Dette er helt essensielt ettersom en optimal sikringskultur kjennetegnes av at organisasjonen er i stand til å forstå truslene og agere deretter.

5.3.2 Fleksibilitet

I tråd med teori om sikkerhetskultur synes informantene å vektlegge håndtering av hendelser som et viktig kjennetegn ved en optimal sikringskultur. Relf og Stubblefield (2000) vektlegger at relevant informasjon om trusselbilde og sikringsrisikoer må dermed integreres i virksomhetens beredskapsplaner, noe som igjen legger føringer for både håndtering, beskyttelse av verdier, samt normalisering.

Flere av informantene meddeler at en sikringshendelse skjer i regi av en aktør, internt eller eksternt, som har en intensjon om å skade virksomheten. Det påpekes at en slik aktør vil på en eller annen måte klare å penetrere selskapets systemer, eksempelvis adgangskontroll systemet, og dermed er det viktig å ha en plan for normalisering. På lik linje vektlegger teori om HRO evnen til håndtere feil når de oppstår (Weick et al., 1999). I en sikringskontekst er usikkerheten høy grunnet trusselens natur (Reniers et al., 2011) og dermed blir det desto viktigere at virksomheten har en normaliseringsplan og at ansatte har nødvendig kompetanse og innehar et tankesett til å reagere. Flere av informantene har derfor inkorporert sikring i virksomhetens beredskapsplan.

På lik linje som litteraturen om HRO vektlegger informantene trening og øvelser som en viktig del av å utvikle og opprettholde kompetansen til ansatte slik at de er i stand til å håndtere en eventuell sikringshendelse. I tillegg påpekes det at trening anes som et viktig element i utviklingen av en sikringskultur ved å blant annet øke sikringsbevisstheten til de ansatte. Generelt sett kommer det frem at det er i stor grad ledelse, personer med sikringsfunksjoner og beredskapsorganisasjonen som mottar

spesifikk trening på sikring, samt offshorearbeidere (skarpe enden). Dette kan tyde på at dersom en sikringshendelse oppstår er det de som besitter mest kunnskap og kompetanse som skal håndtere hendelsen. Dette kan ses i lys av teori om fleksibel kultur, hvor det ofte skjer et skift fra en hierarkisk struktur til en flatere struktur, hvor beslutningsmyndighet gis til dem som besitter relevant ekspertise for å løse problemet (Reason, 1997). Likevel kan det synes at virksomhetene har i større grad forhåndsdefinerte roller og ansvar for håndtering av en sikringshendelse, hvor det synes å være en mer sentralisert beslutningsmyndighet. Dette kan ses i sammenheng med at en sikringshendelse kan oppstå "hvor som helst" i virksomheten, i motsetning til sikkerhetshendelser som oppstår hovedsakelig på operativt nivå, og hvor man da vektlegger å trene de i den skarpe enden. Samtidig fremkommer det av empirien at poenget med øvelser er at det blir håndtert riktig av de som skal håndtere det. Dermed omfatter ikke trening og øvelser alle ansatte i organisasjonen, men heller de som har en rolle i forhold til håndtering av sikringshendelser. Det fremkommer også at det ikke er hensiktsmessig å involvere vanlige ansatte i eksempelvis terror og kidnappingsscenarier, da dette kan skape uønsket frykt og angst blant de ansatte. Det å ha forhåndsdefinerte roller og ansvar for håndtering kan også henge sammen med at mye av informasjonen i en sikringskontekst er ofte gradert og deles kun med utvalgte grupper. Eksempelvis nevnes det at dersom det oppstår en kidnappingssituasjon, blir kun et begrenset antall personer involvert.

Det fremgår at øvelser kan variere fra involvering av alle nivåer til kun ett nivå, eksempelvis at tredje linje involveres i en table-top øvelse. Flere av informantene understreker at slike øvelser anses som en måte å øke håndteringsevnen. Øvelsen innebærer at en sikringscase blir gjennomgått, hvor ledernes beslutningsevne testes, samt organisasjonens evne til å improvisere og håndtere en sikringshendelse. Igjen er dette viktig grunnet at risikoen er ofte forbundet med en større grad av usikkerhet sammenlignet med sikkerhetshendelser (Pettersen og Bjørnskau, 2014) og hvor det kan tenkes at det stilles høyere krav til improvisasjon. Teorien vektlegger også at øvelser og trening kan bidra til å skape tillitt mellom ledelse og de i den skarpe enden (Reason, 1997), noe som i en sikringskontekst vil også omfatte de som har sikrings- og beredskapsfunksjoner.

Det fremgår i empirien at håndtering av sikringsrelaterte hendelser krever et annet tankesett sammenlignet med sikkerhetshendelser, eksempelvis brann. Det understrekes at det er ingen standard reaksjonsmønstre og at de ansatte må i større grad tenke selv og forholde seg til trusselen. Dermed ses øvelser og trening på sikringsscenarioer som en viktig forutsetning for at de skal være i stand til å respondere på en fleksibel måte. Dette kan kobles til konseptet om "mindfulness", der organisasjonens medlemmer innehar evnen til å være årvåken og respondere til risikonivået (Weick et.al., 1999). Likevel påpeker Reniers et al. (2011) at håndtering av konsekvenser av en hendelse, eksempelvis en brannhendelse, behandles likt innen safety og security uavhengig av om denne er tilfeldig eller intendert. Samtidig påpekes det at trusselaktører vil søke etter de beste løsninger og planer for å utføre sitt mål om å forårsake skade (Reniers et al., 2011). Likheten mellom sikkerhet og sikring kommer også frem i empirien, hvor det forklares at mange av reaksjonene og prosessene vil være like for håndtering av beredskapshendelser og sikringshendelser. Til tross for dette viser funn at det kan oppstå sikringsscenarioer som krever enn annen type håndtering, eksempelvis kidnapping og terroranslag, hvor beredskapsplanen må ta hensyn til usikkerheten og gi rom for improvisasjon og fleksibel håndtering. Her påpekes det som eksempel at i motsetning til en brannhendelse, ønsker man ikke at alle skal samles på et forhåndsdefinert møtepunkt, men heller forholde seg til trusselen og i større grad tenke selv hvordan en kan redde ens eget liv. I lys av dette kan det stilles spørsmål til hvorvidt det er mulig å trene på å håndtere ulike typer sikringshendelser og utarbeide detaljerte beredskapsplaner, grunnet uforutsigbarheten knyttet til sikringshendelser. Til tross for at man ikke kan forutse alle mulige scenarioer, kan trening ha som formål å bidra til at man er i en viss grad mer mentalt forberedt på en sikringshendelse, noe som kan ha betydning for håndteringsevnen. Det fremkommer i empiri at det å være forberedt mentalt er vel så viktig i håndtering av slike hendelser. Øvelser kan også tenkes å bidra til at man opprettholder det Reason (1997) kaller en "sunn skepsis", som kan tolkes som en slags årvåkenhet og bevissthet omkring sikring.

Som nevnt tidligere er operativt nivå (offshore) en av gruppene som mottar trening og øvelser på sikringshendelser. En av utfordringene som kommer frem i resultatene er at kunnskapsnivået omkring sikring er ofte skjevfordelt i organisasjonen, noe som kan tenkes å påvirke den totale håndteringsevnen. Blant annet påpekes det at det er et lavt

kunnskapsnivå på operativt nivå, noe som henger sammen med at sikringshendelser opptrer sjeldent. I sikkerhetsfeltet vil de i den skarpe enden håndtere sikkerhet til daglig og dermed opparbeide seg mer erfaringsbasert læring og kunnskap, i motsetning til i en sikringskontekst hvor dette er begrenset. En av informantene anser lavt kunnskapsnivå som en av de største utfordringene med å utvikle en optimal sikringskultur. I fravær av intenderte uønskede hendelser blir øvelser og trening desto viktigere for å øke kunnskapsnivået og håndteringsevnen, som omfatter blant annet operativt nivå.

Oppsummering av fleksibilitet

Ut ifra teori og funn ser vi at fleksibilitet er vel så viktig i en sikringskontekst som i en sikkerhetskontekst ved at risikoen er forbundet med stor grad av usikkerhet og organisasjonen har mindre mulighet til å forutse intenderte uønskede hendelser. Dermed kreves det en håndtering som gir rom for improvisasjon, samtidig som det synes å vektlegges forhåndsdefinerte roller og ansvar. Ettersom organisasjonen har lite eller ingen erfaring med håndtering av alvorlige sikringshendelser som eksempelvis terroranslag, vil trening og øvelser være nødvendig for å sikre tilstrekkelig kompetanse, bevissthet samt å utvikle en mental kapasitet for å kunne agere i henhold til trusselen. Likevel er håndtering noe som er forbeholdt visse grupper i organisasjonen, da visse typer øvelser kan ha negativ effekt ved å skape uønsket frykt blant ansatte.

5.3.3 Læring

Reason (1997) argumenterer for at en optimal sikkerhetskultur er en *velinformert* kultur som vet hvor grensen mellom sikkerhet og uakseptabel fare er, uten nødvendigvis å måtte krysse denne. Flere av informantene synes å mene at en optimal sikringskultur kjennetegnes av en forståelse for truslene som organisasjonen står ovenfor, samt en tilpasning av tiltak i forhold til trusselnivået, noe som kan tolkes som en *velinformert* kultur. I lys av dette blir en *lærende kultur* (Reason, 1997) et viktig element i forhold til utvikling av en optimal sikringskultur. Et viktig kjennetegn ved HRO er nettopp evnen til å samle inn og analysere mest mulig data om alle mulige faresignaler og benytte dette som muligheter for læring og forbedring. Ettersom faresignaler i en sikringskontekst kan opptre både eksternt og internt, er man i større grad avhengig av å samle inn informasjon både fra omgivelsene og fra egen

virksomhet. Dermed fremstår læring i fravær av intenderte uønskede hendelser som spesielt utfordrende sammenlignet med i en sikkerhetskontekst, hvor, ifølge Pettersen og Bjørnskau (2014), risikoen er i større grad kjent.

Ifølge litteraturen omfatter organisatorisk læring at organisasjonen kontinuerlig reflekterer over sine praksiser gjennom monitorering, analysering og feedback systemer (Pidgeon, 1998). Våre funn viser at dette er også helt sentralt i en sikringskontekst, hvor informantene vektlegger viktigheten av å samle inn data for å kunne forstå trusselbildet, samt å tilpasse seg for å ligge i forkant av disse. Flere av virksomhetene vektlegger bruken av rapportering og avviksbehandlingssystem for å sikre kontinuerlig læring i organisasjonen. Det påpekes viktigheten av å skape en kultur som kjennetegnes av at ansatte rapporterer mistenkeligheter og avvik fra normalen, noe som kan ses i lys av en *rapporterende kultur* (Reason, 1997). Likevel fremkommer det utfordringer med rapportering, da det nevnes at ansatte kan unngå å rapportere i frykt av konsekvenser dette kan innebære, og at statistikk ikke nødvendigvis stemmer overens med virkeligheten. Dette kan representere en utfordring i forhold til læringspotensialet til virksomheten, ettersom rapportering er viktig for at virksomheten skal kunne fange opp mulige faresignaler.

Litteraturen om sikkerhetskultur vektlegger at i fravær av ulykker, er man avhengig av at mennesker rapporterer selv de minste feil og nesten-ulykker (Reason, 1997). På samme måte vil man i en sikringskontekst være avhengig av at menneskene i organisasjonen rapporterer både egne feil, eksempelvis brudd på prosedyrer, samt atferd eller forhold som oppfattes som avvik fra normalen. Dermed blir behovet for en *rettferdig kultur* helt sentralt, hvor man legger vekt på læring heller enn straff (Reason, 1997). Rapportering er nødvendig for at organisasjonen skal få en oversikt over mulige problemområder og iverksette nødvendige forbedringstiltak. HRO-teorien vektlegger blant annet at feil bør tolkes som sårbarheter i andre deler av systemet og dermed generaliseres (Weick et al., 1999). Blant annet kan rapporterte avvik, eksempelvis at de ansatte slipper fremmede inn i virksomheten, være en indikator på en generell uønsket atferd i organisasjonen som gjør dem mer sårbar overfor potensielle trusselaktører. Å bruke blant annet rapporteringssystemet som grunnlag for lærdom blir dermed viktig for å korrigere eventuelle svakheter i systemet, men kan gi begrenset effekt dersom det er få hendelser som blir rapportert.

Ettersom trusler kan opptre både eksternt og internt, kreves det også andre metoder for å samle inn og analysere informasjon om faresignaler, utover rapporterings- og avviksbehandlingssystemet. I tillegg til innsamling av informasjon internt i selskapet, vektlegges informasjonsdeling og erfaringsoverføring som nødvendig for å kunne oppnå en forståelse for det aktuelle trusselbildet. Blant annet fremheves det samarbeid med myndigheter, eksempelvis PST og NSM, for å holde seg oppdatert. Videre fremheves samarbeid mellom selskapene i petroleumssektoren i forhold til sikringsarbeidet. En sentral utfordring i denne sammenheng er at informasjon er ofte gradert, noe som medfører en begrenset åpenhet. Dette medfører også spesielle utfordringer i forhold til læring, og skiller seg i stor grad fra sikkerhetsfeltet hvor full åpenhet vektlegges og verdsettes. Ettersom sikring dreier seg om beskyttelse mot intenderte uønskede hendelser (Pietre-Cambacedes og Chaudet, 2010), kan åpenhet og samarbeid i bransjen bli spesielt problematisk. Dette kan medføre til en begrenset erfaringsoverføring mellom virksomhetene, spesielt når det gjelder detaljer omkring sikringstiltak. Likevel forteller flere at de har utvekslet erfaringer med andre selskaper i forhold til lærdommer fra sikringshendelser, noe som er positivt for å sikre kontinuerlig forbedring i sikringsarbeidet. Et viktig kjennetegn ved HRO er å monitorere hva som skjer i andre selskaper og lære fra disse (Dekker & Wood, 2010), noe som også vil være viktig i fravær av hendelser i eget selskap. Det fremkommer at noen mener at åpenheten i en sikringssammenheng kunne vært større, eksempelvis knyttet til deling av metodikk og arbeidsmetoder i bransjen. Det kan tenkes at dette kunne medført en større grad av læring i bransjen. Spesielt er dette viktig ettersom sikring er for mange et relativt nytt område som har fått økt fokus de siste årene, og hvor man har lite erfaring med sikringshendelser og dermed et behov for økt kunnskap.

Nyttiggjørelse av data er også sentralt for å kunne sikre læring i organisasjonen (Reason, 2000). I våre resultater påpekes det at trening og øvelser kan brukes til å teste virksomhetens beredskapsplan, og erfaringer fra øvelser blir så benyttet som ny input til planverk. Dette kan også sørge for at sikringsarbeidet ikke er statisk, men heller en kontinuerlig prosess (Ruighaver et al., 2006) noe som er viktig for å sikre læring. Samtidig påpeker teorien at det er viktig at ledere har både kompetansen og viljen til å handle basert på innsamlet data (Reason, 1997). I en sikringskontekst er

den informasjonen virksomheter besitter ofte preget av høy grad av usikkerhet (Albechtsen, 2003). En utfordring i denne forbindelse blir dermed å finne den riktige balansen mellom tiltak virksomheten bør implementere og det gjeldende risikonivået, hvor funn fremhever viktigheten av å unngå "security overload." Her vil blant annet opplevelse av risiko kunne være en medvirkende faktor. Videre kan det være tilfeller hvor beslutningstakere ikke er sikkerhetsklarerte og må ta beslutninger basert på ufullstendig informasjon. Dette kan tenkes å kunne påvirke hvilke beslutninger som tas, med hensyn til eksempelvis hvorvidt sikringstiltak blir implementert.

Et viktig kjennetegn ved HRO er at menneskene i organisasjonen preges av en "kronisk" bekymring, og er dermed konstant opptatt av at feil og svikt kan oppstå (Weick et al., 1999). Funn tyder på at virksomhetene vektlegger å fortelle ansatte om at det finnes trusler og på denne måten formidle informasjon som har betydning for sikringen. Videre fremheves viktigheten av at ansatte er bevisste og årvåkne slik at de rapporterer inn eventuelle avvik. Bevissthet ses dermed som en forutsetning for å skape en rapporterende kultur, og er noe virksomhetene retter fokus på gjennom blant annet bevisstgjøringskampanjer og opplæringsprogram. Likevel fremgår i empirien viktigheten å være realistisk og ikke overdrive trusler, for å unngå å skape frykt og angst blant ansatte. Dermed synes det ikke å være ønskelig å ha kultur som er preget av "kronisk" bekymring, i den forstand at man ikke skal glemme å være redd og forvente at ting vil gå galt (Reason, 1997). Det synes heller å være ønskelig å fremme en overvåkenhet og oppmerksomhet der man "har det litt i bakhodet". En annen utfordring i denne forbindelse er at trusselaktører kan også opptre internt i organisasjon. Dersom man fremmer en kultur preget av "kronisk" bekymring, kan dette medføre et arbeidsmiljø hvor en ikke stoler på sine kollegaer. Det synes å være sentralt å skille mellom det å være mistenksom og det å være observant og overvåken, hvor sistnevnte synes å være et kjennetegn ved en optimal sikringskultur.

Videre vektlegger teori om HRO at et fravær av hendelser eller tidligere suksess er ikke er en garanti for suksess i fremtiden, og det fremheves at en slik tilfredshet kan være et faresignal i seg selv (Reason, 2000). I en sikringskontekst er det spesielt vanskelig å måle effektiviteten av sikringstiltak, sammenlignet med en sikkerhetskontekst (Pettersen & Bjørnskau, 2014). Dermed er det vanskelig å vurdere hvorvidt et fravær av hendelser er et resultat av et godt styringssystem og kultur eller

om det er tilfeldig, da det er ikke gitt at man er et attraktivt mål for en trusselaktør. Uavhengig av dette, er det viktig at virksomheten ser på sikring som en kontinuerlig prosess, hvor læring i organisasjonen er en drivkraft til denne prosessen.

Oppsummering av læring

En lærende kultur fremstår som et viktig kjennetegn på en optimal sikringskultur, noe som støttes både av teori og funn. Det å innsamle, analysere og videreformidle informasjon er viktig både i en sikkerhetskontekst og en sikringskontekst. Likevel ser vi en del ulikheter og utfordringer knyttet til læring i sikringskontekst. Dette kan relateres til et fravær av sikringshendelser, høy grad av usikkerhet, at trusselaktører kan opptre internt og eksternt (Albrechtsen, 2003), samt det er begrenset informasjonsdeling både innad og på tvers av organisasjoner. Dette krever en betydelig større innsats fra virksomhetens side og andre tilnærminger for å være i stand til å kontinuerlig overvåke og respondere på det endrede trusselbildet. En alvorlig sikringshendelse kan ha katastrofale konsekvenser og krever dermed en proaktiv tilnærming for å fange opp faresignaler om trusler før disse akkumulerer. Dette gjøres blant annet gjennom etterretning, samarbeid på tvers av selskapene og myndigheter, rapportering blant ansatte og gjennomføring av sikringsrisikoanalyser og øvelser. Videre blir det sentralt at en nyttiggjør og iverksetter handlinger og tiltak ut ifra de innsamlede data. Her vil opplevelse av risiko, forpliktelse til sikring, og begrenset åpenhet kunne påvirke beslutninger omkring implementering av sikringstiltak.

5.3.4 Tillit

Flere av aspektene knyttet til læring gjennomgått ovenfor, slik som rapportering og begrenset åpenhet er også i stor grad knyttet til tillit. I likhet med Jeffcott et al. (2006) fremhever informantene at tillit er essensielt i arbeidet med å utvikle en optimal sikringskultur, hvor det påpekes at tillit er nøkkelen til å lykkes i enhver organisasjon. I tråd med Haukelid (2001) vektlegges at kulturendringsprosessen må skje gjennom samarbeid og dialog som preges av gjensidig tillitt mellom ledelse og ansatte. Det fremkommer stor enighet om at tillit påvirker samhandling, informasjonsdeling og rapportering, noe som er i tråd med teori om sikkerhetskultur (Jeffcott et al., 2006). Likevel fremkommer det flere utfordringer i forhold til tillit i en sikringskontekst, noe som kan videre ha betydning for utvikling av en sikringskulturen.

I våre funn fremkommer det enighet om at tillit er svært viktig for å stimulere til rapportering av sikringshendelser eller mistenksomheter. Rapportering i en sikringskontekst fremstår likevel som problematisk, hvor enkelte fremhever at terskelen for å rapportere er gjerne høyere sammenlignet med en sikkerhetskontekst. Situasjoner hvor ansatte observerer noe mistenkelig kan tenkes å oppleves som svært ubehagelig da rapportering kan medføre alvorlige konsekvenser for den det gjelder. I empirien fremkommer det at ansatte kan anse det som risikabelt å gripe inn dersom de er vitne til eksempelvis et tyveri på arbeidsplassen. Funn viser også at de ansatte kan i noe tilfeller la være å rapportere, i frykt av hvilke konsekvenser sikringsbruddet kan få for den enkelte. Dette kan ses i lys av behovet for en *rettferdig kultur,* hvor ansatte har en tillit til at ledelsen behandler rapportene og impliserte personer på en rettferdig måte (Reason, 1997). Både funn og teori vektlegger at en må skape en atmosfære av tillitt hvor de ansatte tørr og har lyst til å rapportere. Reason (1997) understreker i den forbindelse betydningen av rask tilbakemelding på rapporterte hendelser. I en sikringskontekst blir dette problematisk, da rapporteringssystemet er til dels lukket, og detaljer rundt sikringshendelser forblir konfidensielt. Likevel kan tilbakemelding foretas på ulike måter, og det synes at det å betrygge ansatte om at problemet blir tatt tak i er en type tilbakemelding som blir viktig i denne sammenheng. Dermed blir det desto viktigere at de ansatte har tillit til at både systemet og relevante personer er i stand til å håndtere problemet.

For å oppfordre til rapportering vektlegger teori om sikkerhetskultur opplæring og trening fremfor bruk av straff og sanksjoner, noe som synes å være viktig i forhold til å skape tillit mellom ledelse og de ansatte (Reason, 1997). Hvorvidt straff vektlegges synes å variere ut ifra funn. Det fremkommer at det er tilfeller hvor sanksjoner anses som nødvendig, på lik linje med Reason (1997), som hevder at det ikke er gunstig å skape en "no blame culture." Resultatene viser at det er en utfordring å finne balansen mellom en "no blame culture" og bruken av sanksjoner. På den ene siden ønsker selskapet at de ansatte rapporterer, på den andre siden kan ikke alle typer atferd aksepteres. Hvilket type utfall en hendelse får synes å avhenge i stor grad av frekvens og alvorlighetsgrad av sikringsbruddet. Blant annet skilles det mellom enkle forglemmelser og brudd som gjøres med "vilje og viten", noe som igjen påvirker bruk av sanksjoner. Hvorvidt akseptabel eller uakseptabel atferd er tydeliggjort for de

ansatte vil kunne virke inn på organisasjonens troverdighet og dermed påvirke hvorvidt ansatte rapporterer eller ikke. I tillegg er det viktig at de ansatte er klar over at informasjon omkring sikringshendelsen blir holdt konfidensielt og at de forblir anonyme gjennom hele prosessen (Reason, 1997), spesielt i lys av at terskelen for å rapportere kan være høyere i en sikringskontekst. Dette synes å være viktige prinsipper for å skape tillit mellom ledelse og ansatte, samt for å fremme en kultur hvor sikringshendelser blir rapportert.

I vår funn fremheves det at begrenset åpenhet i en sikringskontekst kan også medføre utfordringer i forhold til beslutningstaking. Det påpekes viktigheten av selskapet må ha tillit til nøkkelpersoner i organisasjonen fordi de kan besitte informasjon som ikke kan deles med resten av virksomheten. Samtidig vektlegger teori om sikkerhetskultur åpne informasjonskanaler og at ledelsen skal i størst mulig grad være velinformert når de tar sikkerhetsmessige beslutninger (Jeffcott et al., 2006). Ettersom åpenhet og informasjonsdeling er begrenset i en sikringskontekst, tyder dette på at tillit må vektes tungt. Det kan tenkes at tillit vil i denne sammenheng ha en slags kompenserende funksjon. På bakgrunn av dette blir det essensielt at en optimal sikringskultur preges av gjensidig tillit mellom ledelse og sikringsfagfolk, slik at ledelsen stoler på råd og anbefalinger fra sikringsfagfolk og dermed aksepterer at beslutninger må fattes på bakgrunn av et ufullstendig informasjonsbilde.

Teori om sikkerhetskultur vektlegger at mennesket i organisasjonen skal kjennetegnes av en "kronisk bekymring" (Reason, 1997) eller det Hale (2000) referer til som en "kreativ" mistillit til risikostyringssystemet. Generelt i våre funn blir det påpekt viktigheten av at de ansatte derimot har en tillit til at systemet er i stand til å forebygge og håndtere sikringshendelser. Videre påpekes viktigheten av at ansatte har tillit til at de blir informert dersom det skjer en endring i trusselnivået, og at virksomheten vil agere deretter med å iverksette nødvendige tiltak. I slike situasjoner fremheves viktigheten av at de ansatte har en forståelse for at ikke alt av informasjon kan deles. Likevel fremkommer det at ansatte må være på observante og overvåkne i forhold til å oppdage avvik fra normalen, noe som kan tolkes som en slags "kreativ mistillit." Samtidig kan mistillit oppfattes som negativt ladet ord, og i den sammenheng vil det være mer passende med det Reason (1997) kaller for "sunn skepsis." En utfordring i den forbindelse kan være at nordmenn blir av flere

informanter oppfattet som naive og at de har en manglende risikoforståelse. Dersom man har en "det skjer ikke oss" holdning, kan dette medføre at ansatte i mindre grad er oppmerksomme på avvik, samt i mindre grad oppfatter sikringstiltak som meningsfulle. Dette kan dermed tenkes å ha innvirkning på hvorvidt de ansatte innehar en "sunn skepsis." Dette må ses i sammenheng med virksomhetens ønske om å unngå å skape unødvendig frykt og angst som nevnt tidligere, og krever dermed en balansegang.

En spesiell utfordring i en sikringskontekst er at virksomheten kan stå ovenfor innside trusler, noe som medfører at menneske kan ha en tosidig rolle, noe som litteraturen i liten grad belyser. Menneskene kan både bidra til å oppdage faresignaler, men kan også være en trussel dersom de har en intensjon om å skade virksomheten. Et dilemma som oppstår her er hvorvidt organisasjonen skal stole på de ansatte, eller om det er nødvendig med en viss grad av mistillit. Ifølge teori om sikringskultur må det være en viss grad av tillitt til at de ansatte vil handle på riktig måte (Ruighaver et al., 2006). Dette er helt sentralt for å skape en optimal sikringskultur hvor ansatte er motivert til reflektere over sin atferd og på hvilken måte de kan bidra til å øke sikringsnivået i organisasjonen (Ruighaver et al., 2006). Det fremkommer i våre funn at til tross for potensielle innside trusler er tillit helt essensielt i enhver organisasjon. Uten en viss grad av tillit fremmes ikke en kultur som stimulerer hverken til rapportering og læring, heller ei trivsel og godt arbeidsmiljø. Likevel påpekes det at virksomheten har andre systemer og prosesser som har til hensikt å fange opp innside trusler og uakseptabel atferd i organisasjonen, noe som også vektlegges i teori (Ruighaver et al., 2006). Likevel kan det påpekes at hvorvidt de ansatte opplever dette som mistillit fra organisasjonen sin side kan tenkes å påvirke grad av aksept for sikringstiltakene. Eksempelvis hvis det oppfattes som "storebror ser deg" og "nå kommer de for å sjekke meg." Dette kan ses i tråd med forskning gjort innenfor luftfart som viser at security regler kan oppfattes som ulogiske, urettferdige og basert på mistillit (Pettersen & Bjørnskau, 2014).

Oppsummering av tillit

Både teori og empiri anser tillit som et viktig kjennetegn ved en optimal sikringskultur. Tillit synes å være sentralt i forhold til å stimulere til rapportering og læring i organisasjonen, kompensere for begrenset åpenhet, samt i forhold til å skape

aksept for sikringstiltak blant ansatte. Det synes å være sentralt at de ansatte har i større grad en tillit til at systemet er i stand til å forebygge og håndtere sikringsrelaterte problemer sammenlignet med sikkerhetsrelaterte problemer. Likevel fremstår det som viktig å stimulere til at ansatte innehar en "sunn skepsis," i den forstand at de er overvåkne i forhold til avvik fra normalen. Samtidig som det må være en balansegang hvor en unngår å skape uønsket frykt. Menneskets tosidig rolle representerer også en mulig utfordring, hvor organisasjonen må utvise tillit samtidig som prosesser og systemer kan oppleves av ansatte som basert på mistillit. Generelt fremstår tillitt som utfordrende i en sikringskontekst ettersom det er begrenset informasjonsdeling både mellom organisasjonen og de ansatte, samt i noen tilfeller mellom beslutningstakere og sikringsfagfolk. Dette medfører at virksomhetene må blant annet nøye vurdere hvilken type informasjon de gir ut til de ansatte, samt hvordan dette kommuniseres ut, slik at man skaper en forståelse for sikringstiltakene.

6.0 Konklusjon

Avhandlingens formål har vært å undersøke hvilket syn operatørselskapene har på utvikling av en optimal sikringskultur og vurdere hvorvidt sikringskultur begrepet fremstår som hensiktsmessig i arbeidet med å utvikle en slik kultur.

Hva er operatørselskapene i petroleumssektoren sitt syn på utvikling av en optimal sikringskultur og hvorvidt fremstår begrepet sikringskultur som hensiktsmessig i arbeidet med å utvikle en slik kultur?

6.1 Delkonklusjon 1: Hva er operatørselskapene i petroleumssektoren sitt syn på utvikling av en optimal sikringskultur*?*

Studien viser at sikringskultur begrepet fremstår som et relativt nytt og umodent begrep for en rekke av operatørselskapene. Det fremgår en uenighet og begrepsforvirring i oppfatning av begrepene sikring og sikkerhet, hvor studien viser at dette kan ha betydning for om begrepet sikringskultur er tatt i bruk eller ikke. For noen oppfattes sikringskultur som et element av sikkerhetskultur, mens andre ser på sikkerhetskultur og sikringskultur som adskilt på samme måte som safety culture og security culture. Et spørsmål som reiser seg i den forbindelse er om det er mer hensiktsmessig å benytte de engelske begrepene safety culture og security culture, hvor forskjellene mellom disse synes å være tydeligere. Studien belyser et behov for en tydelig begrepsavklaring av de norske begrepene og en mer konsekvent begrepsbruk for å unngå fremtidige misforståelser.

Studien viser at flere oppfatter sikringskulturbegrepet som noe mer enn etterlevelse av regler og prosedyrer, hvor begrepet omfatter antagelser, holdninger, oppfatninger, verdier og atferd i organisasjonen, som kan ha betydning for sikringsnivået til virksomheten. Bruken av sikringskulturbegrepet i sikringsarbeidet synes å medføre en mer reflektert forståelse for kulturens betydning for sikringsnivået samt hva som er ønskelige kjennetegn ved en optimal sikringskultur. Her vektlegges bevissthet, kompetanse, ansvarsfølelse og forståelse for sikring. En optimal sikringskultur kjennetegnes av at sikringstankegangen kommer naturlig og er selvgående, hvor

ansatte intuitivt tar initiativ til sikring. En slik forståelse av kultur innebærer at utvikling av en sikringskultur blir en lang og tidkrevende prosess, hvor endringer i atferdsmønstre, holdninger og verdier gradvis blir tatt for gitt som riktig av organisasjonens medlemmer. Studien viser at kunnskapsdimensjonen spiller en sentral rolle i dette arbeidet. Hvorvidt tiltak og initiativ rettet mot kulturendring vil oppnå ønsket effekt er uvisst, men vi antar at kulturforståelse vil spille en viktig rolle i utvikling av en kultur som støtter opp sikringsnivået.

Med utgangspunkt i vårt teoretiske rammeverk, viser studien at forpliktelse, fleksibilitet, læring og tillit vektlegges i utvikling av en optimal sikringskultur. Studien belyser en rekke ulikheter og utfordringer knyttet til elementene som i ulik grad skiller seg fra sikkerhetskultur-feltet. Dette henger sammen med at sikring har noe særegne karakteristika; at det er en trusselaktør som kan opptre internt og eksternt, det er høy grad av usikkerhet og ofte et fravær av intenderte uønskede hendelser. Et av hovedfunnene i studien er at begrenset informasjonsdeling og åpenhet utgjør en stor utfordring i forhold til muligheter for læring og forståelse for truslene virksomheten står ovenfor, samt å skape aksept og forståelse for sikringstiltak blant ansatte. Dette kan få implikasjoner for både tillit og grad av forpliktelse både blant ledelsen og ansatte. I en optimal sikringskultur vil alle ansatte inneha en "sunn skepsis" i den forstand at de er overvåkne og rapporterer avvik. En utfordring er å unngå naivitet og samtidig ikke skape uønsket frykt og angst blant ansatte. Ledelsens forpliktelse til sikring anses av alle som helt sentralt i utvikling av en kultur som bidrar positivt til sikringsnivået. Hvorvidt dette lar seg gjøre i praksis er utenfor studiens formål, likevel belyser studien at ledelsesforpliktelse er kun én av flere medvirkende faktorer og at det kreves en helhetlig tilnærming til kulturbygging.

Studien viser enighet om at kultur er viktig for å oppnå et høyt sikringsnivå blant operatørselskapene. Likevel eksisterer det ulike syn på hvorvidt det er nødvendig med et eget sikringskulturbegrep. Ved at flere har valgt å ta begrepet i bruk kan dette tyde på et økt fokus på de "myke" sikringshjelpemidlene i sikringsarbeidet blant operatørselskapene. Studien viser også variasjon i kunnskapsnivå knyttet til kulturbegrepet blant selskapene, til tross for at et økt fokus på sikring i petroleumssektoren. Forståelse for kultur og dens betydning for sikringsnivået er dermed et mulig forbedringsområde.

6.2 Delkonklusjon 2: Hvorvidt fremstår begrepet sikringskultur som hensiktsmessig i arbeidet med å utvikle en slik kultur?

På engelsk skilles det mellom safety og security, hvor forskjellen ligger i intensjonsbegrepet. Dermed gir det også mening å snakke om henholdsvis safety culture og security culture. Med dette tar man hensyn til at kultur er viktig både innenfor safety feltet og security feltet, samt at det er ulikheter mellom dem. Dette muliggjør å snakke om en god eller dårlig safety culture, og en god eller dårlig security culture. Problematisk blir det når man har oversatt safety culture, som dreier seg om uintenderte uønskede hendelser, til sikkerhetskultur og HMS kultur på norsk. Her får sikkerhet en bredere betydning og dekker uønskede hendelser, uavhengig om disse er uintenderte eller ei. Det kan stilles spørsmål til hvorvidt virksomheten evner å ta høyde for ulikhetene mellom safety og security ved å benytte ett overordnet begrep. En optimal safety culture er ikke nødvendigvis en optimal security culture og vice versa, samt kan man ha en velutviklet safety culture og en mindre utviklet security culture. Dette vil trolig ikke fanges opp dersom man har ett overordnet begrep som dekker begge aspektene. Vi mener dermed at bruken av ett begrep kan tenkes å skape uklarhet knyttet til hvilket aspekt man egentlig fokuserer på.

Et mulig argument for å benytte sikkerhetskultur som et overordnet begrep, er at det kreves en helhetlig tilnærming til sikkerhetsstyring hvor både safety og security blir sett under ett. Likevel krever dette at virksomhetene faktisk tar hensyn til begge aspektene, også når det gjelder kulturbiten. Tradisjonelt har fokus i stor grad vært rettet mot sikkerhet i forhold til uintenderte uønskede hendelser. Derimot er intenderte uønskede hendelser et sjeldnere fenomen, og risikoen er i større grad ukjent. Bruk av sikringskulturbegrepet betyr ikke at en helhetlig tilnærming ikke bør vektlegges. Det argumenteres at dersom man ikke benytter begrepet, kan dette medføre at sikringselementet blir glemt. Dette gjelder spesielt dersom virksomheten ikke har en klar begrepsavklaring av de norske begrepene, hvor man har tydelig definert sikringsbegrepet. Dette er viktig ettersom flere er av den oppfatning at sikkerhet er det samme som safety og er dermed knyttet til uintenderte uønskede hendelser. Det kan videre stilles spørsmål til hvorvidt tilnærminger til utvikling av en safety culture contra security culture er like, spesielt sett i lys av utfordringene som fremkommer i studiet. Det blir i denne sammenheng viktig å poengtere at sikkerhetskultur og

sikringskultur ikke er separate kulturer, men at begrepene kan brukes konseptuelt for å omhandle de aspektene av organisasjonskulturen som har betydning for sikkerhets- og/eller sikringsnivået.

Studiet vårt illustrerer at en tydelig begrepsavklaring synes dermed å være viktig for å få frem de ulike karakteristikaene ved sikring og sørge for at disse samt relaterte utfordringer blir tatt hensyn til i kulturbyggingen. Å utvikle en kultur som støtter opp sikringsarbeidet lar seg vanskelig gjøre dersom man ikke har et tydelig forhold til sikringsbegrepet og dens særegenheter. Ved å gjøre dette til et kulturbegrep kan det tenkes at man i større grad tar hensyn til disse særegenhetene og hvordan kulturen kan bidra til enten å forsterke eller svekke sikringsnivået i virksomheten.

6.3 Relevans for andre

Det må fremheves at resultatene fra studien ikke nødvendigvis hadde vært det samme for andre sektorer, og at her kan det være andre oppfatninger og meninger omkring sikringskulturbegrepet. Dette er noe videre forskning bør undersøke da dette kan bidra med å belyse andre perspektiver og argumenter for og mot bruk av sikringskulturbegrepet i arbeidet med å utvikle en optimal sikringskultur. Likevel kan det tenkes at andre sektorer kan dra nytte av forskningsprosjektet, og at det belyser betydning av kultur i arbeidet med å optimalisere sikringsnivået i virksomheten.

6.4 Tanker om videre forskning

Sikringskultur fremstår som et lite utforsket område og det er et behov for økt kunnskap på området. Det anbefales å gjøre en mer omfattende studie av sikringskultur fenomenet, hvor også perspektiver fra myndighetene i petroleumssektoren inkluderes. Videre kunne det vært interessant å utforske hvilket syn andre sektorer, eksempelvis utpekt kritisk infrastruktur, har på utvikling av en optimal sikringskultur, og hvorvidt sikringskulturbegrepet er tatt i bruk i disse sektorene. Et annet interessant område ville være å utforske ansatte sine oppfatninger og meninger omkring sikringskultur, herunder balansegangen mellom opplevelse av risiko og implementerte sikringstiltak i virksomheten. Til slutt kunne det vært interessant å utforske hvordan organisering av sikringsarbeidet spiller inn på utviklingen av en sikringskultur i virksomheten.

7.0 Kildeliste

Alhogail, A., & Mirza, A. (2014). *Information security culture: a definition and a literature review.* In proceedings of IEEE World Congress On Computer Applications and Information Systems. Hammamet, Tunisia.
Hentet fra: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6916579

AlHogail, A. (2015). *Design and validation of information security culture framework.* Computers in Human Behavior, 49(0), 567-575

Antonsen, S. (2009). *Safety Culture: Theory, Metod and Improvement.* Farnham: Ashgate Pub

Albrechtsen, E. (2003). *Security vs Safety*. NTNU -
Department of Industrial Economics and Technology Management
Hentet fra
http://www.iot.ntnu.no/users/albrecht/rapporter/notat%20safety%20v%20security.pdf

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K. (2004). *Samfunnsikkerhet*.Oslo: Universitetsforlag

Bang, H. (1995). *Organisasjonskultur.* Otta: Tano AS

Bang, H. (2013) *Organisasjonskultur: En Begrepsavklaring*. Tidsskrift for Norsk Psykologforening. 2013, 50(4), 326-336. Hentet fra
http://www.psykologtidsskriftet.no/pdf/2013/326-336.pdf

Blaikie, N. (2010). *Designing Social Research*. Cambridge UK: Polity Press

Danemark, B., Jakobsen, L., Ekstrøm, M., Karlsson, J,C. (1997). *Generalisering, vetenskapliga slutledningar och modeller för förklarande samhällsvetenskap.* Att förklara samhället. Lund: Studentlitteratur.

Den Norske Dataforening (ingen dato) Informasjonssikkerhet. Hentet fra
http://www.dataforeningen.no/informasjonssikkerhet.134191.no.html
Nedlastet 12.juni

Dejoy, D. M (2005). *Behavior change versus culture change*. *Divergent approaches to managing workplace safety*. Safety Science, 43(2), 105-129.

Dekker S.W.A & Woods, D.D (2010) *The high Reliability Organization Perspective.* Sverige: Lund University School of Aviation

Lekka, C. (2011). *High Reliability Organisations: A review of the literature*. (RR899 Research Report). Hentet fra http://www.hse.gov.uk/research/rrpdf/rr899.pdf

Falcknutec (2015, 01. Januar). *Norske virksomheter er under angrep hver dag, hele året!* Hentet fra

http://www.falcknutec.no/no/nyheter/2015/norske_virksomheter_er_under_angrep_hver_dag_hele_aaret
Nedlastet 14. mai 2015

Flin, R. (2007). *Measuring safeyculture in healthcare: A case for accurate diagnosis.* Safety Science, 45(6), 653-667. doi: http://dx.doi.org/10.1016/j.ssci.2007.04.003

Glendon, A. I., & Stanton, N. A. (2000). *Perspectives on safety culture*. Safety Science, 34(1–3), 193-214.

Guldenmund, F. W. (2000). *The nature of safety culture: a review of theory and research.*
Safety Science, 34(1–3), 215-257.

Guldenmund, F. W. (2010). *(Mis)understanding Safety Culture and Its Relationship to Safety*
Management. Risk Analysis: An International Journal, 30(10), 1466-1480.

Hale, A. R. (2000). *Culture's confusions*. Safety Science, 34(1–3), 1-14.

Haukelid (2001) *Oljekultur og sikkerhetskultur* (del 1). TIK arbeidsnotat nr. 28/2003 (ISBN nr. 82-7986-020-7) hentet fra
https://www.duo.uio.no/bitstream/handle/10852/17818/haukelid.pdf?sequence=1
Nedlastet 19.januar 2015

Helgensen, O.K., & Taraldsen, L. (2013, 20.september) *Statoil forstår ikke forskjellen på "safety" og "security."* Teknisk ukeblad. Hentet fra
http://www.tu.no/petroleum/2013/09/20/-statoil-forstar-ikke-forskjellen-pa-safety-og-security
Nedlastet 5.juni 2015

Helgensen, O.k (2013, 2.september) *Ingen olje- og gassinstallasjoner trenger ekstra "terrorbeskyttelse."* Teknisk ukeblad. Hentet fra
http://www.tu.no/petroleum/2013/09/02/ingen-olje--og-gassinstallasjoner-trenger-ekstra-terrorbeskyttelse
Nedlastet 5. juni 2015

Hsieh, H. F. & Shannon, S.E. (2005) *Three Approaches to Qualitative Content Analysis.* Qualitative health Research, Vol.15, No.9, 1277-1288.

Jacobsen, D.I. (2000). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode.* Kristiansand: Høyskoleforlaget AS - Norwegian Academic Press

Jeffcott, S., Pidegeon, N., Weyman, A. & Walls, J. (2006). *Risk, Trust, and Safety Culture in U.K. Train operating Companies.* Risk Analysis: An International Journal: Oct 2006, Vol. 26. issue 5, p1105-1121. 17p. 1 Chart.

Jore S.H and Moen, A. (2015): *A Discussion of the Risk-Management and the Rule-Compliance Regulation Regimes in a Security Contex*t. Proceedings from the ESREL-conference 2014.

Justis- og politdepartementet (2000) *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet* (NOU 2000: 24) Hentet fra www.regjeringen.no/nb/dep/jd/dok/nouer/2000/nou-2000-24.html?regj_oss=1&id=143248

Justis- og politidepartementet (2006) *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner* (NOU 2006: 6). Hentet fra http://www.regjeringen.no/nb/dep/jd/dok/nouer/2006/nou-2006-6/22.html?id=157694

Justis- og politidepartmentet (2014) *Rapporten for 22.juli kommisjonen* (NOU 2012: 14).
Hentet fra https://www.regjeringen.no/nb/dokumenter/nou-2012-14/id697260/

Kvale, S. & Brinkmann, S. (2009) *Det kvalitative forsknings intervju.* Oslo: Gyldendal Norsk Forlag As

Lewis, Øvebrekk, H. (2015, 15. januar) *Sikkerhetssjefen: Statoil må leve med frykten.* Aftenbladet. Hentet fra http://www.aftenbladet.no/energi/--Statoil-ma-leve-med-trusselen-3609705.html
Nedlastet 19. januar 2015

Malcolmson, J. (2009). *What is Security Culture? Does it differ in content from general Organisational Culture?* Farnborough, UK: QinetiQ. Hentet fra http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5335511
Nedlastet 23.mars 2015

Nasjonal sikkerhetsmyndighet hjemmeside. Hentet fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2015-web.pdf
Nedlastet 12. juni 2015

Nasjonal sikkerhetsmyndighet hjemmeside. https://www.nsm.stat.no/globalassets/dokumenter/presentasjoner/nsm-2014-regionalt-sikkerhetsseminar-egeland-verdivurdering-i-praksis.pdf
Nedlastet 12. juni 2015

Nordby, Y. og Hansen, C.W (2005) *Informasjonssikkerhet atferd, holdninger og kultur* (ROSS (NTNU) 200504). Trondheim: NTNU, Institutt for produksjons og kvalitetsteknikk
Hentet fra http://frigg.ivt.ntnu.no/ross/reports/ROSS2005.pdf

Norsk Olje og Gass (2003, 05. November) 091 Anbefalte retningslinjer for sikring av forsyninger og material i olje og gass industri. Hentet fra https://www.norskoljeoggass.no/Global/Retningslinjer/HMS/Sikring/091%20-

%20Anbefalte%20retningslinjer%20for%20sikring%20av%20forsyninger%20og%20materiell%20i%20olje-%20og%20gassindustrien.pdf
Nedlastet 12. juni 2015

Pettersen, K. & Bjørnskau, T. (2014). *Organizational contradictions between safety andsecurity - Perceived challenges and ways of integrating critical infrastructure.* Safety Science,71, *Part B*(0), 167-177.

Pidgeon, N. (1998). *Safety culture: Key theoretical issues.* Work & Stress: An International Journal of Work, Health & Organisations, 12:3, 202-216.

Piètre-Cambacédès, L. & C., Chaudet. (2010). *The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety"*. International Journal of Critical Infrastructure Protection, Vol. 3:2. S. 55-66.

Petroleumstilsynet (2013) Sikkert grep om sikring. Hentet fra http://www.ptil.no/beredskap/sikkert-grep-om-sikring-article10179-854.html Nedlastet 19.januar 2015

Petroleumstilsyn (2014) HMS og kultur. Hentet fra http://www.ptil.no/publikasjoner/HMS%20OG%20KULTUR/HTML/index.html#/1/ Nedlastet 11.juni 2015

Petroleumtilsynet (2015). Ord og ordtrykk i petroleumsvirksomheten. Hentet fra http://www.ptil.no/ord-og-uttrykk/category38.html Nedlastet: 6.juni 2015

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate

Reason, J. (1998). *Achieving a safe culture: Theory and practice.* Work & Stress: An International Journal of Work, Health & Organization, 12:3, 293.306.

Reason, J. (2000). *Safety paradoxes and safety culture*. Injury Control & Safety Promotion. 7(1): 3-14.

Relf R. & G. Stubblefield (2000). *Countering Petroleum Security Risk.* Global options. Offshore Technology conference.

Reniers, G. L. L., Cremer, K., & Buytaert, J. (2011). *Continuously and simultaneously optimizing an organization's safety and security culture and climatethe Improvement. Achievement and Leadership in Safety & Security (IDEAL S&S) model*. Journal of Cleaner Production*, 19*(11), 1239-1249.

Richter, A., & Koch C. (2004) *Integration, differentation and ambiguity in safety cultures.* Safety Science, 42(8), 703-722.

Schein, E. H. (1984). *Coming to a New Awareness of Organizational Culture*. Sloam Management Review, 25:2.

Ruighaver A. B., Maynard, S.B., & Chang, S. (2006) *Organisational security culture: Extending the end-user perspective.* Computers & Security, 26(1), 56-62.

Schein, E. H. (1987). *Organisasjonskultur og ledelse: Er kulturendring mulig?* Oslo: Mercuri Media Forlag.

Schein, E. H. (2010). *Jossey-Bass Business and Management : Organizational Culture and Leadership* (4. utgave) Hoboken, NJ, USA: Jossey-Bass
Smircich, L. (1983). *Concepts of Culture and Organizational Analysis*. London: Sage Publications, Inc.

Standard Norge, NS 5832 (2014). Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse.

Statoil (2013, 12. september). *The In Amenas Attack.* Hentet fra http://www.statoil.com/no/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf
Nedlastet 19. januar 2015

Statoil (2013, 12. september). *Angrepet mot In Amenas.* Hentet fra http://www.statoil.com/no/NewsAndMedia/News/2013/Downloads/Rapport%20om%20angrepet%20mot%20In%20Amenas.pdf
Nedlastet 19. januar 2015

Talbot, J. & Jakeman, M. (2009) *Security Risk Management - Body of knowledge,* New Jersey: Risk Management Institution of Australasia Limited, John Wiley & Sons, Inc,.Hoboken

Thagaard, T. (2013) *Systematikk og innlevelse - en innføring i kvalitativ metode*. 4. utgave. Bergen: Fagbokforlaget Vigmostad & Bjørke AS

Thomson, K. L., von Solms, R., Louw, L. (2006) *Cultivating an organizational information security culture.* Computer Fraud & Security, 2006(10), 7-11.

Van Nierkek, J.F. & Von Solms, R. (2010) *Information security culture: A management perspective.* Computers & Security, 29(4), 476-486.

Weick, K.E., Sutcliffe, K.M., & Obstfeld, D (1999). *Organizing for high reliability: Processes of collective mindfulness*. Sikkerhet og organisasjon (MSA 230) Stavanger: Universitet i Stavanger.

Zohar, D. (2010). *Thirty years of safety climate research: Reflections and future directions.*
Accident Analysis & Prevention, 42(5), 1517-1522.

8.0 Vedlegg

8.1 Vedlegg 1 – Informert samtykke til informanter

Forespørsel om deltakelse i forskningsprosjektet

"Et studie av temaet sikringskultur"

Bakgrunn og formål
Vi er to studenter på Master i Samfunnssikkerhet ved Universitet i Stavanger som skal gjennomføre en undersøkelse i forbindelse med vår masteroppgave. Formålet med avhandlingen er å utforske begrepet sikringskultur, da dette er et umodent begrep og det er blitt gjort lite forskning på emnet. Begrepet sikring benyttes i denne oppgaven som beskyttelse mot tilsiktede uønskede hendelser. Vi ønsker å undersøke hva operatørselskaper i petroleumssektoren legger i begrepet sikringskultur, samt se nærmere på hva virksomheter anser som en optimal sikringskultur. Vi vil presisere at dette er en utforskende oppgave, der hensikten er å få økt forståelse for emnet sikringskultur både som fenomen og begrep.

Vi har kontaktet deg/dere ettersom vi er ute etter å intervjue personer i operatørselskaper som har kunnskap og kjennskap til virksomhetens sikringsarbeid. Utvalget består av en rekke operatørselskaper fra petroleumssektoren.

Hva innebærer deltakelse i studien?
Datainnsamlingen består av intervju og deltakere vil få forespørsel om de ønsker å få tilsendt intervjuguide på forhånd. Intervjuet vil ha en varighet på ca 1 til 1,5 time. Spørsmålene vil omhandle sikringsarbeidet til den aktuelle virksomhet i forbindelse med kulturbygging samt begrepsbruk. Det vil bli benyttet båndopptaker under selve intervjuet.

Hva skjer med informasjonen om deg?

Prosjektet skal etter planen avsluttes 15.06.15. Alle personopplysninger vil bli behandlet konfidensielt. Kun student, veileder og sensor vil ha tilgang til personopplysninger. Opptakene av intervjuene vil bli transkribert og da vil alle personopplysninger bli anonymisert. Råmateriale vil bli slettet når sensur har gått ut, grunnet sensor kan komme med forespørsel om få tilgang til råmaterialet.

Personopplysninger og virksomhetens navn vil bli anonymisert.

Frivillig deltakelse

Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Dersom du trekker deg, vil alle opplysninger om deg og virksomheten bli slettet.

Dersom du ønsker å delta eller har spørsmål til studien, ta kontakt med:

Caroline Østensjø, tlf: xx xx xx xx

Caroline Irwin Larsen, tlf: xx xx xx xx

Sissel H. Jore, Veileder ved Universitet i Stavanger, tlf xx xx xx xx

Samtykke til deltakelse i studien

Jeg har mottatt informasjon om studien, og er villig til å delta

---

(Signert av prosjektdeltaker, dato

8.2 Vedlegg 2 - Intervjuguide

Introduksjon

- Hvem er forskerne
- Kort informasjon om oppgavens formål og problemstilling
- Gjennomgang av informert samtykke og praktisk informasjon
- Kort om informanten (Navn, stilling, arbeidserfaring, arbeidsoppgaver)
    - Hvordan har din organisasjon organisert sikringsarbeidet?

Begrepet sikringskultur

Hva legger du i begrepet sikringskultur?

Bruker dere dette begrepet i deres bedrift?

Har du gjort deg noen tanker om hvilken betydning kultur har for sikringsarbeidet?

Kulturbygging

Hvilke trusler anser dere som relevante for deres virksomhet?

Hvordan imøtekommer din virksomhet disse truslene?

Hvordan jobber dere med kulturbygging i forbindelse med sikringsarbeidet i deres virksomhet? Kan du gi noen eksempler (opplæringsprogram, atferdsendringskampanjer, kulturprogram og lignende)

Hvilke verdier jobber dere ut ifra og på hvilken måte kan du koble disse verdiene til sikringsarbeidet?

Hvordan jobber dere med å skape bevissthet omkring sikringsrisiko, samt hvordan ansatte kan bidra til å redusere denne risikoen?

Hvordan arbeider dere for å opprettholde ansattes kompetanse og forståelse i forhold til implementerte sikringstiltak og prosedyrer?

Hvordan jobber dere med å involvere de ansatte i sikringsarbeidet?

Elementer ved en optimal sikringskultur

På hvilken måte arbeider dere for å skape ansvarsfølelse for sikring, både blant ansatte og hos ledere?

Har dere formulert en security policy? eventuelt et motto/"quote" for sikringen?

Har dere utarbeidet sikringsmål?

Har dere et opplæringsprogram for alle ansatte i forhold til sikring?

Hvordan arbeider dere for å sørge for at de ansatte er stand til å håndtere en eventuell sikringshendelse?

Hvordan oppfordres ansatte til å rapportere sikringsrelaterte-hendelser/ eventuelt mistenksomheter?

Hvordan sørger dere for kontinuerlig læring i fravær av intenderte uønskede hendelser? Kan du gi noen eksempler?

Hvordan vil du si at dere har blitt påvirket av In Amenas hendelsen?

På hvilken måte mener du åpenhet og tillitt er viktig i en sikringskontekst?

Hvordan håndteres brudd på sikringstiltak, for eksempel å slippe inn fremmede som ikke har adgangskort?

Utfordringer

Hva opplever dere som hindringer eller utfordringer i forhold til å skape de ønskede holdninger, verdier og atferd blant ansatte i forbindelse med sikringsarbeidet?

Oppsummering

Hva mener du er viktige kjennetegn ved en "optimal" sikringskultur?

Tror du andre er enige i ditt syn på sikringskultur?

Til slutt, er det andre ting enn det vi har snakket om som du mener er viktig eller nyttig for oss å vite i forhold til å besvare problemstillingen?

Takk for deltakelse