Universitetet
i Stavanger

Security-kultur

- en organisasjons intensjoner og dens praksis

En studie om sammenhengen mellom hva som sies
og hva som gjøres i en organisasjons arbeid med security

Master i Samfunnssikkerhet
Universitetet i Stavanger

Ellen Caroline Granlund
Våren 2018

Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Masterstudium i Samfunnssikkerhet	Vårsemesteret, 2018 Åpen
Forfatter: Ellen Caroline Granlund	…… (signatur forfatter)
Fagansvarlig: Ole Andreas Engen Veileder: Sissel H. Jore	
Tittel på masteroppgaven: Security-kultur – en organisasjons intensjoner og dens praksis. En studie om det som sies og det som gjøres i en organisasjons security-kultur. Engelsk tittel: Security Culture – an organization's intentions and it's practice A study of what is said and done in an organization's security culture.	
Studiepoeng: 30	
Emneord: Security-kultur, Security, Safety, Sikkerhet, Risiko, tiltak, måling, bevissthet	Sidetall: 75 + vedlegg/annet: 8 Stavanger, 13.07.2018

Innholdsfortegnelse

1. Innledning 1
1.1 Motivasjon for valg av tema 1
1.1.1 Kulturens betydning 2
1.1.2 Sikkerhetsfaglig kontekst 3
1.1.3 Intensjoner og praksis i en organisasjons arbeid med security 4
1.2 Avgrensninger 4
1.3 Problemstilling og presiseringer 6
1.4 Struktur 7
2. Teoretisk rammeverk 8
2.1 Risiko og usikkerhet 8
2.1.1 Trussel, verdi og sårbarhet 9
2.1.2 Sikkerhet 10
2.2 Safety og Security 11
2.2.1 Safety og security på norsk - en begrepsavklaring 11
2.2.2 Hva skiller security fra safety? 12
2.2.3 Ulike styringsmuligheter 14
2.3 Kulturbegrepet 15
2.3.1 Subkulturer 16
2.3.2 Mental software 16
2.3.3 Kan kultur måles? 17
2.3.4 Kulturens forskjellige dimensjoner 17
2.3.5 Organisasjonskultur 19
2.3.6 Sikkerhetskultur 22
2.3.6.1 Resilience engineering 23
2.3.6.2 Black Swan 24
2.3.7 Security-kultur 24
2.3.7.1 Integrert rammeverk for security-kultur 26
2.4 Intensjoner og praksis 28
3. Metode 32
3.1 Metodetriangulering 32
3.2 Kvantitativ tilnærming 34
3.2.1 Datainnsamling 34
3.2.2. Sammensatte mål 34
3.2.2.1 Intensjon og praksis for security 35

3.2.2.2 Intensjon og praksis for safety 35
3.2.3 Vurdering av innholdsvaliditet 36
3.2.4 Reliabilitetsanalyse: Cronbachs alfa 36
3.2.5 Paired samples T-test: signifikanstest av to gjennomsnitt 37
3.2.6 Korrelasjonsanalyse 37
3.3 Kvalitativ tilnærming 38
3.3.1 Utvalg 38
3.3.2 Intervju 39
3.4 Metodiske betraktninger og utfordringer 40
3.4.1 Etiske vurderinger 40
3.4.2 Safetec 40
3.4.3 FM-selskapet 40
3.4.4 Hva kunne vært gjort annerledes? 41
4. Empiri 42
4.1 Statistiske resultat 42
4.1.1 Frekvenser 42
4.1.2 Reliabilitetsanalyse 42
4.1.3 Signifikanstest av gjennomsnitt 42
4.1.4 Korrelasjonstabell 45
4.2 Kvalitative funn 46
4.2.1 Hvorfor har organisasjonen en bedre security-praksis enn bedriftens intensjoner om dette? 46
4.2.1.1 Security: en “blindspot” 46
4.2.1.2 Nytt domene 47
4.2.1.3 Tydelighet 49
4.2.2 Hvordan forstås begrepet security-kultur, og i hvilken grad kan det kartlegges? 50
4.2.2.1 Helhetlig tilnærming 50
4.2.2.2 Kulturkartlegging 52
4.2.3 Hva kan security-kultur-begrepet gi oss? 53
4.2.3.1 Begrepsbruk 53
4.2.3.2 Integrert forståelse 55
4.2.3.3 Kreativt bekymret 57
4.2.3.4 Silotenkning 57
4.2.3.5 Forankret på et samfunnsnivå 58
5. Drøfting 61
5.1 Høyere praksis enn intensjoner for security 61
5.1.1 Hvorfor er det slik? 62

5.1.2 Praksis, men ikke forståelse? 63
5.2 Hvordan forstås begrepet security-kultur, og i hvilken grad kan det måles? 64
5.2.1 Differansen mellom det som sies og det som gjøres 65
5.2.2 Faktorer i spørreskjema 67
5.2.3 Måling 68
5.3 Hva kan security-kultur-begrepet gi oss? 69
5.3.2 «Det man ikke vet» 71
5.3.3 Skal alle vite? 72
6. Konklusjon 74
Litteraturliste 76
Vedlegg 1 80
Vedlegg 2 82
Vedlegg 3 84
Vedlegg 4 86

Sammendrag

Vi lever i et risikosamfunn, hvor vi er preget av nye former for trusler. Terrorhendelser, cyberangrep og bevisste anslag av varierende karakter representerer en del av vårt samfunns risikobilde, og tilkjennegir dermed et behov for egnede tiltak og en kultur som støtter opp under dette. Security-kultur er følgelig et begrep som har oppstått etter tilsiktede uønskede hendelser av ulik karakter. Denne oppgaven er en studie om security-kultur, og herunder er det en antakelse at kultur på mange måter er differansen mellom det som sies og det som gjøres. Masteroppgaven er et samarbeid med Safetec, hvor jeg har benyttet foreliggende spørreskjemaundersøkelser og internskriv i mitt datamateriale. I dette samarbeidet har det vært undersøkt en organisasjon, som jeg anonymiserer som XX. Denne organisasjonen er Facility Management-selskap, hvor safety- og security-kulturen har blitt kartlagt.

I organisasjoner uttrykker og kommuniseres det visjoner og strategiske målsetninger relatert til safety og security, som gjerne formuleres gjennom festtaler eller slagord. Dette er manifesterte holdninger som presenterer virksomhetens virke utad, men kan også tenkes å komme til uttrykk internt i en virksomhet for å fremme et fellesskap rundt hvilke verdier som settes i høysetet «her hos oss». Slike kommuniserte intensjoner, kan sees på som virksomhetens forpliktelse. I tillegg til intensjonene fra virksomheten og dens ledelse, vil det også være tilstede en hverdagslig praksis knyttet til både safety- og security-tiltak. Dette handler om hva som gjøres. Det er en antakelse at sammenhengen, eller et eventuelt gap mellom intensjon og praksis vil kunne si noe om security-kulturen i organisasjonen. «Intended versus done» er følgelig en indeks utviklet ved Safetec Nordic som er et forsøk på å operasjonalisere ord og handling rundt safety- og security-arbeidet i en virksomhet.

I denne studien har jeg benyttet meg av to metodiske tilnærminger. En kvantitativ tilnærming ble benyttet for å se om det var en statistisk sammenheng for mellom det som kommuniseres av visjoner, mål og strategier, og det som foregår av faktisk handling. Videre har jeg utført intervjuer med sentrale security-eksperter, samt representanter fra XX. Her har jeg søkt innsikt i hvorfor det kvantitative resultatet viser som det gjør. Jeg søkte også videre forståelse i security-kultur-begrepet, for å få en større forståelse av hvilket fenomen jeg hadde med å gjøre.

Hovedfunn

Den kvantitative tilnærmingen viser at intensjoner, visjoner og mål rundt security har en lavere score enn den faktiske etterlevelsen for security. Dette kan sees som følge av lavt engasjement hos ledelsen vedrørende relevansen av security-tiltak, i tillegg til høye krav og fysiske barrierer blant kundene hvor XXs ansatte leverer tjenester. Motsatt resultat gjelder for safety, hvor intensjon er høy og etterlevelse lavere. Det argumenteres at selv om praksisen scorer relativt høyt på security, kan det likevel mangle forståelse for hvorfor tiltakene er tilstede. Det argumenteres videre for at safety-aspektet er mer forståelig, da risikokilden synes å ligge nærmere mennesket enn ved security.

Security-kultur kan forstås som de grunnleggende antakelser, ideer og intensjoner som deles blant medlemmer av en organisasjon, som påvirker atferd og som kan ha en påvirkning på security-tilstanden i organisasjonen. Det fremkommer av det empiriske materialet at security-kultur på mange måter er den delen av organisasjonskulturen som virker inn på security-aspektet i en organisasjon. Således betraktes safety- og security-kultur som to sider av samme sak. Dette stilles det spørsmål ved, da security har viktige aspekt ved seg som skiller det fra safety. Blant annet stilles det spørsmål til faktorene informasjonsflyt, og kjennskap til virksomhetens forpliktelse. Det er kanskje ikke ønskelig at alle medlemmer i en organisasjon skal vite alt vedrørende security.

På mange måter er security-kultur *alt* en organisasjon foretar seg. Dette gjør det kanskje vanskelig å måle kultur. Kultur kan gjerne måles, men det er utfordrende og krever stor grad av kompetanse og innsikt. Det er behov for videre studier innen måling av security-kultur, hvorvidt dette lar seg måle, samt hvilke faktorer som er sentrale innen kartlegging av kultur.

Security-begrepet er et nytt og umodent begrep, og det mangler forståelse for hvorfor security-dimensjonen er viktig. Det kan se ut til at det er behov for et kulturbegrep innen security-feltet, da man mangler en bevissthet og forståelse for en rekke tiltak. På en annen side kan det hevdes at kultur i en security-kontekst er problematisk, ettersom det kanskje ikke er ønskelig at flere i en bedrift har høy kunnskap og innsikt i en virksomhets security-strategier. Videre finner jeg at det er behov for en integrert forståelse av security. Det kan synes å være en tendens til et «tunnelsyn», hvor man er opptatt av høy sikkerhet på noen områder, mens andre får lide. Det hevdes at security-bevissthet hos ledelse og sentrale beslutningstakere blir viktig.

Forord

Masterprosjektet representerer siste etappe for meg som student på Universitetet i Stavanger. Det siste halve året har vært preget av nysgjerrighet, læring og frustrasjon. Jeg vandret inn på et utfordrende territorium da jeg benyttet meg av en statistisk tilnærming, og omfavnet denne utfordringen med skrekkblandet fryd. Det har vært en utrolig lærerik prosess, både faglig og personlig.

Først og fremst ønsker jeg å rette en stor takk til alle informantene, og til Safetec som har brukt av sin tid for å bistå i arbeidet. I tillegg ønsker jeg å rette en takk til min veileder Sissel Jore for konstruktive tilbakemeldinger. Mine gode støttespillere hos Safetec må også få en spesiell takk. Gunnar Hauland og Asbjørn Lein Aalberg, dere har vært fantastiske. Jeg ønsker også å rette en stor takk til Randi som har brukt tid i sin ferie på korrektur og faglige innspill. Du er god som gull.

Hjertelig takk til mine enestående foreldre og storebror for omsorg, heiarop og atspredelse, og for å ha lyttet til mine sikkerhetsfaglige monologer. Min flotte svigerfamilie fortjener også en stor takk, for hytteturer og koselig atspredelse og støtte. Kjære Petter, takk for at du har holdt ut med meg i denne tiden, og for å være der for meg. Jeg gleder meg til mer tid sammen med dere alle.

Stavanger, 13.07.2018

Ellen Caroline Granlund

Figurer og tabeller

Figurer	Sidetall	Beskrivelse
Figur 1	12	Sikkerhet, safety og security.
Figur 2	13	Kontinuum av ulike menneskelig intensjoner.
Figur 3	18	Kulturens manifestasjon gjennom ulik dybde og nivå
Figur 4	27	En integrert modell for security-kultur.
Figur 5	31	Grunnleggende antakelser, verdier og praksis.
Figur 6	33	Modell av forskningsprosessen vist ved metodetriangulering
Figur 7	44	Score for praksis og intensjon for henholdsvis security og safety.

Tabeller	Sidetall	Beskrivelse
Tabell 1	15	Ulikheter mellom security-risiko og safety-risiko.
Tabell 2	35	Spørsmål som inngår i intensjoner for security
Tabell 3	35	Spørsmål som inngår i praksis for security
Tabell 4	35	Spørsmål som inngår i intensjoner for safety
Tabell 5	36	Spørsmål som inngår i praksis for safety
Tabell 6	43	Paired Samples Statistics
Tabell 7	44	Paired samples t-test
Tabell 8	45	Korrelasjonstabell av de fire sammensatte mål

Terminologi

Begrep	Definisjon
Risiko	Uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value (Aven & Renn, 2010)
Risiko (security)	«Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (NS 5830, 2012)
Security	Tilstand av sikkerhet mot uønskede tilsiktede hendelser hvor det ligger ond hensikt til grunn. (NOU:2006)
Safety	Tilstand av sikkerhet mot uønskede hendelser, hvor det ikke ligger ond hensikt til grunn.
Security-kultur	De grunnleggende antakelser, ideer og intensjoner som deles blant medlemmer av en organisasjon som påvirker atferd, og som kan ha en påvirkning på security-tilstanden i organisasjonen (basert på Malcolmson, 2009)
Trussel	”Mulig uønsket handling som kan gi negativ konsekvens for sikkerheten til personer eller virksomheter” (NS 5830 2012)
Verdi (security)	«Ressurs som hvis den blir utsatt for en uønsket påvirkning vil medføre en negativ konsekvens for den som forvalter eller drar fordel av ressurser» (NS 5830, 2012)
Sårbarhet	”Manglende evne til å motstå en uønsket hendelse eller å opprette en ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning” (NS 5830, 2012).

1. Innledning

1.1 Motivasjon for valg av tema

Dagens samfunn er et globalt samfunn, preget av nye former for trusler som følger samfunnsutviklingen ellers. Terrorhendelser, cyberangrep og bevisste anslag av varierende karakter representerer en del av vårt samfunns risikobilde, og tilkjennegir dermed et behov for egnede tiltak. Hendelsene i Oslo og på Utøya 22. Juli i 2011, samt angrepet på In Amenas i 2014 var hendelser som viste til manglende fokus mot ondsinnede anslag, og en mangelfull kultur som støttet opp om en slik sikkerhet (Østensjø & Larsen, 2015). Security, eller sikring, viser følgelig til en tilstand av sikkerhet mot uønskede, villede hendelser. Det å ha en våken og risikoerkjennende kultur som stimulerer til riktige beslutninger og security-tiltak, har dermed kommet på dagsordenen når det gjelder både organisasjoner og myndighetsinstitusjoner. I dette ligger også en forutsetning om evne til taktskifte og omstilling.

Security-kultur, gjerne omtalt som sikringskultur på norsk, er et begrep som har oppstått som en forklaring på hvordan organisasjoner kan forhindre terrorangrep eller andre ondsinnede intenderte hendelser. Etter terrorangrepet på Equinors, tidligere Statoils anlegg i In Amenas, ble det konkludert med at manglende *«security culture»* var en viktig årsaksforklaring for at hendelsen skjedde, og at organisasjonens kapasitet og kultur måtte bedres for å være bedre rustet mot trusler i flyktige og komplekse omstendigheter (Jore, 2017).

Vår tids farer er følgelig vesensforskjellige enn tidligere, og det kan tenkes at vi i den digitale verden i dag er mer fremmedgjort når det gjelder sikkerhet. Vi har ikke lenger den samme oversikten over trusselbildet (Justis- og beredskapsdepartementet, 2017). Den tyske sosiologen Ulrich Beck har pekt på at manglende trygghetsfølelse er et kjennetegn ved vår tids risikosamfunn. Da uønskede hendelser i førindustriell tid gjerne var stedsspesifikke, naturskapte og kunne sanses gjennom hørsel, syn eller lukt, er de moderne truslene globale i sin karakter, ikke-sansbare og kjenner ikke landegrenser (Aven, Boyesen, Njå, Olsen & Sandve, 2004). De eksisterer gjennom kunnskapen om dem. Dette er en form for risiko og usikkerhet som gjerne kan føles allestedsnærværende og tilslørt på samme tid. Et digitalt angrep er således ikke synlig for dem som er rammet, og behovet for å øke bevisstheten om

sårbarhetene og sikkerhetstruslene, samt øke kompetansen hos den enkelte, blir dermed stadig mer relevant. At vi ikke lenger har den samme fysiske oversikten over sårbarhetsbildet som tidligere, gjør at vi er mer avhengig av kunnskapsdimensjonen rundt farene.

En markant vekst innen informasjons- og kommunikasjonsteknologien har bundet den nasjonale og internasjonale sfære tett sammen gjennom effektive økonomiske transaksjoner og raskere beslutning- og informasjonssystemer (Aven, et al., 2004). Disse systemene har gitt oss økt produktivitet og lønnsomhet, men fører på den andre side med seg en kompleksitet og sårbarhet for ulike tilsiktede uønskede hendelser. Sommeren 2017 ble flere internasjonale selskaper utsatt for hacking, deriblant shippingselskapet Maersk. Dette påvirket deres drift i stor grad, og førte til enorme økonomiske tap (Moe & Framstad). Slike hendelser, preget av kompleksitet og mer eller mindre grad av usikkerhet, er en del av det globale samfunnets trusselbilde som mange organisasjoner og selskaper må forholde seg til. Det illustrerer behovet for bevissthet, oppmerksomhet og god praksis når det gjelder forståelse og håndtering av denne type trusler; en risikoerkjennende kultur.

1.1.1 Kulturens betydning

Det har de siste årene vært en betydelig interesse for sammenhengene mellom kultur, sikkerhet og sårbarhet i organisasjoner (Engen, Kruke, Lindøe, Olsen, Olsen & Pettersen, 2016). Ettersom mange industriområder og sektorer må forholde seg til og håndtere ulike typer risikoer, har kulturbegrepet, og da særlig begrepet sikkerhetskultur kommet på dagsorden. Hvilke holdninger man i en organisasjon har til ulike former for sikkerhetstiltak, har fått stor oppmerksomhet de senere tiår. Sikkerhetskultur oppsto som begrep i granskingen som fulgte etter Chernobyl-ulykken i 1986, og har fått fotfeste som en forklarende faktor for hvorfor ulykker skjer i organisasjoner, og hvordan sikkerheten kan bedres på bakgrunn av felles praksis og risikoforståelse (Jore, 2017).

Holdninger, kultur og ledelse forstås og defineres på flere ulike måter mellom ulike fagdisipliner, så vel som innenfor de ulike områdene. Man kan si at kultur er et fellesskap av verdier, idéer, normer og kunnskap som deles av en gruppe mennesker, og som de har tilegnet seg gjennom læring og tilpasning. Holdninger og verdier inkluderer det vi tror er riktig, men også hva vi føler eller er tilbøyelige til å sette ut i handling. Følgelig påvirker holdninger også bevisst eller ubevisst de valgene vi tar, enten som individ eller som organisasjon. Dersom

holdninger deles i en organisasjon, påvirker det også hvordan enkeltpersoner løser oppgaver på, og det påvirker hvilken kultur man utvikler innad i en organisasjon (Justis- og beredskapsdepartementet, 2016). Kultur i en organisatorisk forståelse innebefatter således et spekter som går fra holdninger, verdier og mentale kart, til uttalte intensjoner, mål og strategier, som mer eller mindre manifesteres i atferd.

1.1.2 Sikkerhetsfaglig kontekst

I den sikkerhetsfaglige litteraturen skiller man på engelsk mellom to perspektiver, *Safety* og *Security*, hvor forskjellen gjerne er definert ut ifra hensikt og grad av overlegg. Safety-begrepet brukes således om ulykker, eller ikke-tilsiktede hendelser, mens Security benyttes med tanke på hendelser begått med ondsinnet hensikt (Jore, 2017). På norsk har vi ikke en like klar distinksjon mellom de to ulike typer hendelser, men heller en uavklart begrepssituasjon rundt fenomenene (Østensjø og Larsen, 2015). Safety oversettes gjerne til det norske ordet sikkerhet, et begrep som også anvendes om tilsiktede hendelser. Dette gir til kjenne en utfordring rundt begrepet sikkerhetskultur, hvor innholdet blir uklart, og security-dimensjonen synes mer diffus. I den norske oversettelsen av rapporten etter terrorangrepet i In Amenas, ble «security culture» omtalt som nettopp sikkerhetskultur (Østensjø & Larsen, 2015). Dette viser til en inkonsekvent bruk av begrepene, og som også løfter fram behovet for å utvikle fagfeltet security nærmere. Flere aktører og større konsern har imidlertid tatt i bruk begrepet *sikring*, som et forsøk på å få til et skille mellom de to perspektivene. Dog kan det hevdes at sikring som begrep ikke fanger opp det samme meningsinnholdet som det engelske *security* gjør. Derfor vil security og security-kultur benyttes konsekvent i denne oppgaven, bortsett fra direkte sitater fra intervjuobjekter som kan benytte ordet "sikring".

Det foreligger lite forskning og akademisk litteratur rundt konseptet security-kultur, og det mangler studier som tar for seg hva begrepet betyr, og hvordan man kan oppnå en optimal kultur hva gjelder security. Jore har pekt på at mens kulturbygging, risikostyring og resiliens har vært sentrale aspekter i sikkerhetsforskning i flere tiår, har det kun i nyere tid vært rettet oppmerksomhet mot tilsvarende temaer innen security-feltet (Jore, 2017). Følgelig er litteraturen og studier innen safety-perspektivet omfangsrik og del av en lengre forskningstradisjon. Dette gir til kjenne et behov for nærmere studier og teoriutvikling på emnet Security, og da spesielt rundt Security-kultur som har vokst fram som et særlig aktuelt konsept i ulike deler av næringslivet. Et særlig spennende område er hvordan begrepet kan forstås, og operasjonaliseres, og hva begrepet kan tilby oss i en sikkerhetsfaglig sammenheng.

Ved å se på en organisasjons intensjoner, og dens faktiske praksis og atferd vedrørende security, kan det tenkes at organisasjonens håndtering av security-trusler kan betraktes.

1.1.3 Intensjoner og praksis i en organisasjons arbeid med security

I ulike organisasjoner er det ofte utarbeidet uttalte visjoner, verdier og strategiske målsetninger relatert til safety og security, som gjerne formuleres gjennom såkalte festtaler, eller statements som «safety first» og null-visjoner. Dette er manifesterte holdninger som presenterer virksomhetens virke utad, men kan også tenkes å komme til uttrykk internt i en virksomhet for å fremme et fellesskap rundt hvilke verdier som settes i høysetet «her hos oss». Slike kommuniserte intensjoner, kan sees på som virksomhetens forpliktelse (Internskriv, Safetec, 2018). I tillegg til intensjonene fra virksomheten og dens ledelse, vil det også være tilstede en hverdagslig praksis knyttet til både safety- og security-tiltak. Dette handler om hva som gjøres. Det er en antakelse at sammenhengen, eller et eventuelt gap mellom intensjon og praksis vil kunne si noe om security-kulturen i organisasjonen. «Intended versus done» er følgelig en indeks utviklet ved Safetec Nordic som er et forsøk på å operasjonalisere ord og handling rundt safety- og security-arbeidet i en virksomhet. Det er ikke en allmenn kjent indeks, men vil i oppgaven benyttes som del av metodikken for å bygge videre på Safetecs indeks «intended/done», og studere en organisasjon og deres score på variabler operasjonalisert som henholdsvis «intended» og «done».

1.2 Avgrensninger

Som nevnt innledningsvis, har jeg gjennomgående valgt å benytte begrepet «security-kultur» framfor «sikringskultur». Bakgrunnen for et slikt valg er dypere avklart i teorikapittelet i oppgaven. Dog kan det sies at de engelske begrepene security og safety bedre fanger inn den distinkte forskjellen i menneskelig hensikt som tillegges de to fenomenene, enn det som er tilfelle for sikkerhet og sikring. Sistnevnte henviser også til flere ulike former for sikring, slik som fysisk sikring av objekter, eiendom og materiell, informasjon og IKT-infrastruktur, samt personer og personell. De myke security-barrierene i en organisasjon, slik som tanker, ideer og holdninger om å beskytte seg selv og omgivelser mot diverse ondsinnede aktører, inngår i det jeg i oppgaven omtaler for en security-kultur.

Denne oppgaven og dens tema, er et samarbeid med Safetec Nordic, som er et selskap som leverer tjenester innen risikostyring og risikobasert beslutningsstøtte. Temaet for prosjektet

har framkommet i løpet av samtaler med ekstern veileder i selskapet. Oppgaven søker å studere security-kultur, og hvilken sammenheng det er mellom intensjoner i en organisasjon og dens praksis. Jeg har følgelig valgt å avgrense studien til å undersøke en spesifikk organisasjon, nærmere bestemt et Facility Management-selskap, heretter kalt FM-selskap. Selskapet er anonymisert, og i oppgaven benyttes «XX» i stedet for selskapets navn.
Et FM-selskap er en virksomhet som tilbyr ulike former for servicetjenester og leveranser for selskaper. Årsaken til valg av virksomhet for studien er bedriftens avtale med Safetec Nordic, hvorav sistnevnte har gjennomført en omfattende undersøkelse av bedriftens safety- og security-kultur. For å kartlegge dette har det blitt benyttet intervjuer og spørreskjemaundersøkelse. I tillegg til dette, er FM-selskap en interessant virksomhet å studere, da de jobber gjennom flere ledd, som kan representere en utfordring når det gjelder å skape en felles kultur i organisasjonen.

I dette henseende er det vesentlig å påpeke at når det snakkes om intensjoner for security-arbeid, altså virksomheten og dens medlemmers forpliktelse i de interne og/eller eksterne omgivelsene, må det ikke forveksles med intensjonsaspektet som ligger implisitt i safety- og security-distinksjonen. Førstnevnte omhandler intensjoner innad blant organisasjonens medlemmer, mens ved security og safety går intensjonsbegrepet henholdsvis på den ondsinnet hensikt/intensjon, eller fravær av slik hensikt.

En annen språklig avklaring, er begrepet *verdi*. Dette benyttes for det meste i denne oppgaven om de grunnleggende antakelsene som inngår i kultur-dimensjonen. Imidlertid er det viktig å holde denne meningen adskilt for det innholdet som legges i trefaktormodellen «*Trussel, verdi og sårbarhet*». I denne sammenhengen anvendes begrepet *verdi* med tanke på de materielle og immaterielle elementer som mennesker verdsetter og ønsker å beskytte.

Når det gjelder indeksen intended versus done, tar denne også for seg safety-aspektet. Dette vil dog ha en underordnet rolle i studien. Safety-perspektivet behandles derfor sekundært og indirekte, da som et sammenlikningsgrunnlag av behandlingen av security og analysen på security-kultur. Valget om et hovedfokus på security-kultur, har blitt tatt på bakgrunn av manglende forskning og litteratur på emnet, i motsetning til safety-tradisjonen. Det er et økende behov for studier på området security, og da spesielt security-kultur, da målrettede ondsinnede angrep av ulik karakter preger dagens samfunn. Videre er det en antakelse at det i samfunnet er rettet mye oppmerksomhet rundt safety-trusler, og i mindre grad på security.

Helse, miljø og sikkerhet, og forebygging av ulykker er tydelig forankret i den norske arbeidsmiljøloven, og vi har i Norge en lang tradisjon rundt dette. Det kan tenkes at når det gjelder uønskede, tilsiktede hendelser, er ikke forståelsen rundt dette feltet forankret i samfunnet i like stor grad.

1.3 Problemstilling og presiseringer

På bakgrunn av det overnevnte presenteres følgende problemstilling

> *I hvilken grad er det en sammenheng mellom en organisasjons intensjoner og dens praksis når det gjelder security-kultur?*

For best å besvare problemstillingen har jeg operasjonalisert den og utarbeidet en hypotese og tre forskningsspørsmål. Disse er gruppert i henhold til de to metodiske tilnærmingene, hvor det innledes med en hypotese som er utgangspunktet for den kvantitative delen av oppgaven. Videre følges det opp med forskningsspørsmål som utgangspunkt for den kvalitative delen. Det tas utgangspunkt i organisasjonen som studeres.

Hypotesen som legges fram er basert på en antakelse om at det vil være en høyere security-praksis enn hva man ser av intensjoner for security. Denne antakelsen kommer først og fremst av at security for mange er et nytt begrep og et nytt fenomen å forholde seg til i samfunnet som sådan, og ulike bedrifter spesielt. Jeg forstår det derfor slik at man gjerne ikke har kommunisert ut security-strategier eller mål rundt dette. Imidlertid kan det tenkes at det foreligger faktiske tiltak eller krav som holder praksis på et høyere nivå. Med denne bakgrunnen er den kvantitative undersøkelsen bygger på følgende hypotese:

> Det eksisterer et gap mellom intensjoner og praksis på security i virksomheten, hvor praksis scorer høyere enn intensjon.

Ettersom den kvantitative delen av oppgaven ansees å kun gi svar på en del av problemstillingen, ser jeg det som fruktbart for oppgavens formål å i tillegg til en kvantitativ, deduktiv framstilling, også gå mer i dybden på et eksplorativt nivå. En slik framgangsmåte anses som formålstjenlig ettersom security-kultur kan ansees å være et umodent og nytt

område i sikkerhetslitteraturen, som trengs å utforskes i dybden. Jeg har følgelig sett behovet for å forstå begrepet mer inngående. Det vi som mennesker har av grunnleggende antakelser, holdninger og forståelse rundt sikkerhet og arbeid i forbindelse med tilsiktede hendelser, antas i denne oppgaven å påvirke våre intensjoner for arbeidet med security, i tillegg til praksis relatert til security-arbeid. Derfor er det sentralt å også se på hvor «landet ligger» vedrørende slik bevissthet og forståelse i arbeid med security, og hva security-kultur-begrepet kan bidra med i en slik kontekst.

Med denne bakgrunn er forskningsspørsmålene som følger:

1. Hvorfor viser den kvantitative analysen det den gjør?
2. Hvordan forstås begrepet security-kultur, og i hvilken grad kan det måles?
3. Hva kan security-kultur-begrepet gi oss?

1.4 Struktur

I den følgende delen av oppgaven skisseres det teoretiske fundamentet som problemstillingen vil bli belyst ut ifra. Her går jeg særlig inn på safety- og security-perspektivene, samt kulturbegrepet. Videre, i kapittel 3, viser jeg til de metodiske valg og vurderinger som er gjort, og legger fram hvilke analyseteknikker som er benyttet. I kapittel 4 presenteres det empiriske materialet, både det statistiske resultater og kvalitative funn. Siden drøftes disse funnene opp mot de teoretiske perspektivene. Oppgaven rundes så av med en avsluttende kommentar.

2. Teoretisk rammeverk

For å undersøke en organisasjons security-kultur, herunder dens sammenheng mellom det som sies og det som gjøres, vil jeg i det følgende legge til grunn et teoretisk rammeverk som utgangspunkt for den senere analysen. Det vil innledes med en oversikt over risikobegrepet, og dens relasjon til sikkerhet og usikkerhet, da dette er viktige elementer når det gjelder tilsiktede uønskede hendelser. Med de forutsetninger at studien konsentrerer seg hovedsakelig rundt security og security-kultur, vil det videre være avgjørende å gi en faglig begrepsavklaring rundt de norske og engelske begrepene, samt skissere ulikheter og fellesnevnere for safety og security. Videre vil kulturbegrepet, og da særlig teori innen organisasjonskultur bli gjennomgått, da dette utgjør kjernen av oppgaven og dens anliggende.

2.1 Risiko og usikkerhet

Risikobegrepet blir i dag brukt i flere forskjellige sammenhenger, med ulike og til dels uklare betydninger. Vår forståelse og oppfatning av risiko har implikasjoner for vår praksis når det kommer til å styre sikkerhet og risiko (Aven et al. 2004). Ofte forstås risiko som en kombinasjon av mulige konsekvenser og tilhørende sannsynligheter. På et mer generelt plan kan vi si at risiko er et uttrykk for mulige konsekvenser og deres tilhørende usikkerhet (NOU: 2006:6). Disse to forståelsene faller gjerne sammen, da sannsynligheter gjerne benyttes for å uttrykke usikkerhet kvantitativt. Risiko handler ofte om fremtiden, om mulige hendelser eller kjeder av hendelser som kan inntreffe, med et visst utfall. Engen et al. skriver følgelig:

> Risiko viser til noe som kan eller kunne ha skjedd, hvordan hendelsene påvirker samfunnet vi lever i, og hvordan bestemte handlinger kan endre forløpet av en hendelse. De fleste begreper om risiko har til felles at de dreier seg om forholdet mellom mulige og valgte handlinger. Til enhver tid står individer, organisasjoner og samfunn ovenfor et uendelig antall valgmuligheter (muligheten til å ikke handle er også en handling) som har en lang rekke konsekvenser og utfall. Konsekvensene eller utfallene kan være positive eller negative (Engen, et al. 2016, s. 79)

Risikobegrepet er definert på flere forskjellige måter, ut ifra ulike fagdisipliner og tilnærminger. Avhengig av om du for eksempel har en kulturell, økonomisk eller en teknisk-naturvitenskapelig tilnærming, kan risiko forstås henholdsvis som en gruppes delte verdier rundt risikoaktiviteten, kost/nytte (forventet økonomisk tap), eller som en estimert sannsynlighet (Lindøe, Kringen & Braut, 2015).

Aven og Renn knytter risiko opp mot usikkerhet, og forstår risiko som usikkerheten om og alvorligheten av hendelser og konsekvenser (eller utfall) av en aktivitet med hensyn til det som mennesker verdsetter (Aven & Renn, 2010). I denne forståelsen er det også lagt til en dimensjon rundt det som mennesker verdsetter, noe som kan strekke seg fra materielle objekter, eiendom og infrastruktur, til mer immaterielle elementer som helse, liv og velferd. Usikkerhetsdimensjonen kommer også til uttrykk i forståelsen av risiko som den «usikkerhet om hva som blir konsekvensene eller utfallene av en gitt aktivitet» (Aven et al., 2004). Det er således tilstede en grad av usikkerhet når vi snakker om risiko, og denne usikkerheten vurderes ofte individuelt fra en person til en annen. Risiko er følgelig en vurdering sett gjennom øynene på noen, også der hvor man benytter risikovurderinger og analyser for å komme frem til hvilken risiko vi har med å gjøre (Aven et.al., 2004).

Videre har vi alle en ulik oppfatning av risiko; hva som er risiko for meg kan være noe annet enn hva som er risiko for deg eller en annen gruppe mennesker. Den risiko vi selv vurderer, er følgelig basert på den tilgjengelige kunnskapen vi har, eller mangel på sådan. Det er da snakk om en form for usikkerhet. Utfordringene med risiko, er at det er knyttet verdivurderinger, følelser og usikkerheter knyttet til risikoene, som igjen har ulike karaktertrekk (Engen et al., 2015). Ved tilsiktede hendelser, slik som terror, er det ofte sterke følelsesmessige krefter i sving, og det er snakk om trusler som rører ved de sterkeste verdiene vi har, slik som demokrati og følelser om rettferdighet.

2.1.1 Trussel, verdi og sårbarhet

I denne oppgaven betraktes risiko som forholdet mellom de verdier vi ønsker å verne, de trusler som kan tenkes å ramme disse verdiene, og sårbarhetene som verdiene har i relasjon til truslene (NOU: 2016: 19). Risikobildet i samfunnet er i stadig endring som følge av den generelle samfunnsutviklingen, hvor nye verdier skapes, nye sårbarheter etableres, og trusselbildet er dynamisk og i endring (NSM, 2017). Sikkerhetstilstanden er således påvirket av den innsatsen vi legger i å sikre verdiene våre. Kunnskap om egne verdier og sårbarheter, samt en forståelse for at verdiene kan være attraktive for ulike trusselaktører, er således viktig for menneskers risikoerkjennelse. Formålet med virksomheter eller organisasjoners arbeid med security er følgelig å verne om sine verdier. I et større perspektiv er formålet å verne om sentrale og sårbare samfunnsverdier, og ivareta rikets selvstendighet og nasjonale sikkerhetsinteresser (NSM, 2017). Forståelsen av risiko som relasjonen mellom verdier, trussel og sårbarhet er illustrert i figur 1.

2.1.2 Sikkerhet

Både på et organisatorisk nivå, og et samfunnsnivå vil man i mer eller mindre grad være opptatt av sikkerhets- og beredskapstiltak som kan bidra til å redusere risikoene ved dagens trusselbilde. Sikkerhetsbegrepet er således tett knyttet opp til risiko, og benyttes ofte om forebyggende tiltak der hensikten er å redusere sannsynligheten for at noe uønsket skal skje eller redusere konsekvensene ved uønskede hendelser (Aven et.al., 2004).

Sikkerhetsbegrepet benyttes også i en videre betydning, som den evne et system har til å unngå skader og tap. Videre har begrepet også ulike nyanser, hvorav det gjerne henvender seg til det fysiske miljø, slik som teknologiske systemer og materielle omgivelser, eller til de menneskelige, sosiale og organisatoriske faktorer. Da er det gjerne den menneskelige praksis, samfunnets politikk og diskurs, eller de organisatoriske strukturer og virkemåte i fokus (Aven et.al., 2004). I tillegg kan sikkerhet relateres til ulike nivåer; et individnivå (mikronivå), et organisasjonsnivå (mesonivå) og et samfunnsnivå (makronivå). I anledning forandringer i den sivile beredskap på 90-tallet i Norge, samt utviklingen av et master- og sivilingeniørstudium i Stavanger, har begrepet *Samfunnssikkerhet* fått fotfeste i norsk forvaltning og litteratur. Samfunnssikkerhet er beskrevet som «den evne samfunnet har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger» (Aven et al., 2004). Dette begrepet skal videre dekke hele spekteret av ulike uønskede hendelser, også tilsiktede hendelser og trusler om dette mot befolkningsgrupper eller mot nasjonens selvstendighet og eksistens.

Sikkerhetsbegrepet i Norge dekker således både det som gjerne anses som utilsiktede hendelser, slik som ulykker og naturhendelser, i tillegg til tilsiktede hendelser som terror, sabotasje eller cyber-kriminalitet. At vi ikke har et tydelig leksikalt skille på norsk, kan anses som utfordrende. Derfor vil jeg i denne oppgaven ta utgangspunkt i de engelske begrepene security og safety for å adressere de to ulike perspektivene.

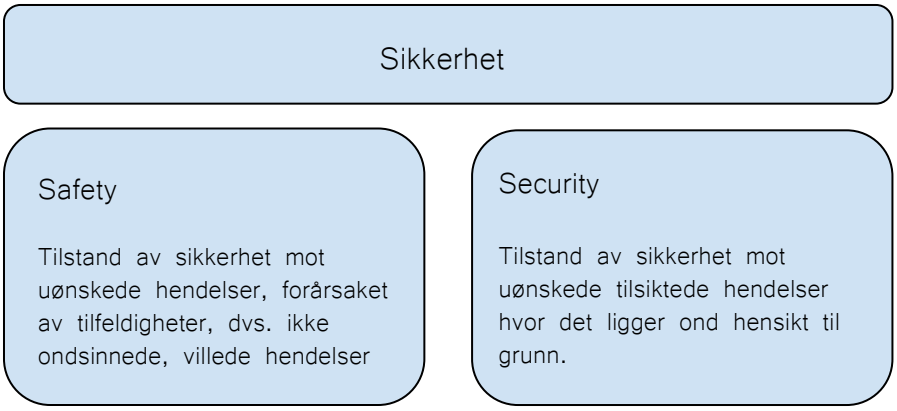
2.2 Safety og Security

I det følgende ønsker jeg å foreta en begrepsavklaring rundt begrepene safety og security, samt gi et overblikk over forskjeller mellom de to ulike aspektene ved uønskede hendelser.

2.2.1 Safety og security på norsk - en begrepsavklaring

Safety og security benyttes gjerne som hjelpeord på norsk for å beskrive ulike aspekter knyttet til sikkerhet og risiko, og vil også anvendes i denne studien. Safety henviser ofte til uønskede ikke-ondsinnede hendelser, mens security benyttes om uønskede, tilsiktede hendelser. Det kan dermed gi mening å snakke om safety culture og security culture. Dog er det gjerne en utfordring at førstnevnte ofte oversettes til det norske ordet sikkerhetskultur, da sikkerhetsbegrepet på norsk også gjerne anvendes om både tilsiktede så vel som utilsiktede hendelser. Det kan tenkes at security-aspektet forsvinner i oversettelsen. Anvendelsen av engelske ord viser til at det ikke eksisterer noe leksikal distinksjon mellom de to typer uønskede hendelser på norsk. Tilsvarende ord på norsk kan anvendes etter skjønn, noe som er legitimt når det springer ut av faglige behov. Det ligger likevel ikke noen automatikk i at slike fastsatte begreper blir tatt i bruk. Innen enkelte organisasjoner og større konsern i Norge har man stipulert norske ord for safety og security, der safety gjerne er satt til sikkerhet og security til sikring (NOU: 2006).

Sikkerhet favner mange områder, og har ulik betydning avhengig av kontekst. Hva gjelder begrepet sikring, benyttes dette på veldig mange områder, slik som fysisk sikring av objekter eller mennesker, fallsikring eller flomsikring, og har derfor et meningsinnhold som går utover det som her gjelder sikkerhet mot intenderte uønskede hendelser. I denne oppgaven vil det engelske begrepssettet Safety og Security anvendes, begrunnet i en klarere distinksjon når det gjelder meningsinnhold, hvorav det hevdes at de tilfører bedre forståelse for intensjonsaspektet i distinksjonen. I tillegg er disse begrepene gjennomgående brukt i akademisk litteratur. Det overordnede begrepet *sikkerhet* benyttes følgelig som et paraply-begrep, i tråd med NOU:2006.



Figur 1: Sikkerhet, safety og security. Basert på NOU: 2006: 6, s. 229, samt Vivold (2015), s. 13.

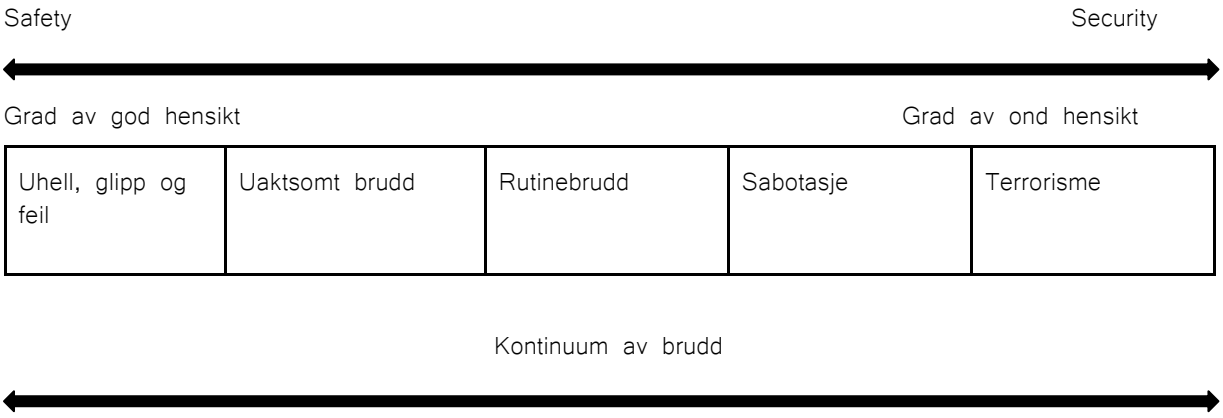
Det skal imidlertid sies at jeg ikke deler den samme begrepsforståelsen av safety-hendelser som noe som er forårsaket av tilfeldigheter, slik det er presentert i NOU:2006. Bred erfaring, samt granskingsrapporter, litteratur og undersøkelser peker på det motsatte (Bjerke, 2010, Ptil, 2013 & Reason, 1997). I etterkant av Piper Alpha-ulykken ble det pekt på årsaksfaktorer som akkumulering av feil, tvilsomme beslutninger og en dårlig kultur (Patè-Cornell, 1993). Det kan dermed sies at safety-hendelser ikke er noe som skjer på bakgrunn av tilfeldigheter, eller «act of God», men hendelser som ofte har bakenforliggende, latente betingelser (Reason, 1997).

2.2.2 Hva skiller security fra safety?

Flere forskere har forsøkt å utdype betydningen av safety og security, deriblant har Boholm funnet at begrepene ofte benyttes som synonymer. Imidlertid har de distinkte forskjeller i meningsinnhold og anvendelse. Ofte er skillet mellom safety og security gitt ut ifra hensikt (Young & Leveson, 2014, Reniers, Cremer & Huytaert, 2011). Selv om security-hendelser ofte defineres som tilsiktede, og safety-hendelser er utilsiktede, betyr ikke det at skillet nødvendigvis er urokkelig. Jore skriver:

> The litterature on organizational safety has long acknowledged that accidents are not something that just happen. Reason (1997) claims that violation is one factor that can contribute to organizational accidents. Reason defines violations as exceptional, routine or reckless. Reason further states that other categories of violations, such as sabotage, also exists. This means that, is contrast to what the definitions of safety and security suggests, human intent plays a role in both safety and security. (Jore, 2017, s. 468).

Et brudd eller avvik kan være tilsiktet, selv om det ikke foreligger et ønske om å påføre noe, eller noen, skade. Derfor kan man gjerne si at distinksjonen mellom Security og Safety beror på en *ondsinnet* hensikt fra gjerningsmannen, som i tilfellet med Security planlegger og kalkulerer et anslag med et visst omfang og karakter. I figuren under, ser vi at avvik og brudd spenner fra uhell, blundere og feil til rutinemessige brudd, sabotasje og til terrorhendelser.



Figur 2. Kontinuum av ulike menneskelig intensjoner. Basert på Jore (2017).

Safety-hendelser som er assosiert med avvik eller brudd som ikke er ment å forårsake skade, ligger på figurens venstre side. Mot høyre finner vi brudd og hendelser som konsekvens av ondsinnet hensikt, altså security-hendelser (Jore, 2017). Et slikt kontinuum mellom ulike menneskelige intensjoner, markerer skillet mellom safety og security. Jore peker følgelig på at et slikt kontinuum kan være nyttig for å skissere spekteret av ulike ondsinnede aktører og hendelser. Noen mulige security-scenarioer kan være sabotasje, lovbrudd, cyber/IKT-kriminalitet eller spionasje. Dette viser således de ulike typer situasjoner som security omfavner. Aktørene spenner fra å være enkeltindivider, slik som en hacker eller ensom ulv-terrorist som opererer på egenhånd, til organiserte grupper og celler, eksempelvis terrorgrupper eller kidnappere, videre til statsnivået hvor det kan foregå spionasje og informasjonskrigføring (Jore, 2017).

2.2.3 Ulike styringsmuligheter

Safety og security har således ulike grunnforutsetninger, også når det gjelder hvordan man tilnærmer seg de ulike typer risikoer. Et scenario der noen ønsker å skade eller angripe et anlegg eller en organisasjon, krever en annen type risikovurdering enn det som ofte gjennomføres i forbindelse med HMS- og safety-trusler (Reniers et al., 2011).

I tilfellet med security vil aktørene videre være påvirket av sine sosiale og fysiske omgivelser, samt av personlige faktorer. Security-perspektivet er følgelig mer kompleks, og innebærer gjerne en symbolsk mening som ligger i sosiale prosesser utenfor tid og rom for selve hendelsen (Reniers et al., 2011). Selv om en virksomhet eller et anlegg kan være arena for et angrep, er ikke nødvendigvis målet for aktøren å skade virksomhetens produksjon, men imidlertid å trekke oppmerksomhet til et politisk eller religiøst budskap.

Hendelsens «røtter» er dermed ikke like synlige som ved safety-hendelser, der sistnevntes årsaker er lokalt forankret med en integrert risiko i selve systemet eller virksomheten. På grunn av en lengre avstand til risikofenomenet ved tilsiktede hendelser, vil en del virksomheter mangle en total forståelse, ressurser og midler til å utføre egnede risikovurderinger for security-hendelser. Det kan virke noe mer uklart, diffust og uhåndgripelig. Videre har ikke organisasjoner selv ressurser til å redusere security-trusler, all den tid det ligger i myndighetenes mandat å oppdage og arrestere mulige angripere (Jore, 2017).

I tilfellet med safety-hendelser foreligger det mer erfaringsdata og statistikk for ulykker og ikke-tilsiktede hendelser, enn for tilsiktede anslag. På bakgrunn av slike data, kartlegges og analyseres derfor safety-hendelser ved hjelp av sannsynligheter og konsekvenser. Hva gjelder tilsiktede hendelser derimot, gjennomføres gjerne såkalte trusselvurderinger der man ser på konsekvenser, sårbarhet og målattraktivitet (Reniers et.al. 2011). I slike tilfeller benyttes gjerne kvalitative metoder, slik som ekspertvurderinger, når det gjelder å beskrive og analysere risiko. Usikkerhetsdimensjonen ved bevisste anslag blir også større da trusselbildet er mer kompleks, og man gjerne har å gjøre med aktører som innehar kapasitet og intensjon, og i tillegg er tilpasningsdyktige og fleksible. En slik usikkerhet vanskeliggjør estimering av sannsynlighet (Egeli, 2014). Figur 2, med utgangspunkt i Reniers et.al., gir en oppsummerende oversikt over viktige forskjeller mellom security og safety.

Security	Safety
• Hendelsens karakter er påvirket av menneskelig handling • Tilsiktet • Menneskelig angrep • På grunn av mindre vanlig forekomst, vil kvalitativ vurdering av security-relatert risiko være tilgjengelig • Risikoen er av symbolsk karakter	• Hendelsens karakter er forårsaket av en iboende risiko • Ikke-tilsiktet • Ikke menneskelig angrep • Kvantitative sannsynligheter og hyppigheter for safety-relatert risiko er tilgjengelig • Risiko er av rasjonell karakter

Tabell 1: Ulikheter mellom security-risiko og safety-risiko, etter Reniers et al. 2011.

2.3 Kulturbegrepet

Studier som omhandler kultur dekker et vidt spekter av perspektiver, og kan således være utfordrende å definere og favne om. Å forsøke å adressere kulturbegrepet, kan sies å være som å åpne en Pandoras eske, som frigjør de fleste samfunnsvitenskapelige konsepter og teorier, og følgelig bringer på bordet en rekke definisjonsspørsmål og analytiske problemstillinger. Kultur er et konsept som er omfattende. Det ligger utenfor denne oppgavens rammer å dykke dypt i kulturbegrepets materie. Imidlertid gis det en oversikt over de vanligste forståelsene rundt begrepet kultur, og da særlig i en organisatorisk forståelse.

Kultur kan forstås som innlærte mønster av antakelser, forventninger om atferd og en tanke om at "slik gjør vi det her hos oss". Det er normer og holdninger som er innlært, snarere enn nedarvet. Antonsen fremhever at den bredeste forståelsen av kultur, er at det favner om alt som ikke kan tilskrives biologi eller de fysiske omgivelsene. Innen et slikt utgangspunkt har utallige antropologer og sosiologer forsøkt å spesifisere mer analytiske definisjoner av kultur (Antonsen, 2009). Å finne en slags orden og mening i tilværelsen er viktig for alle mennesker. Guldenmund påpeker at en viktig funksjon ved kultur, er relatert til reduksjon av usikkerhet. Følgelig vil man oppnå en kontinuitet, da mindre tid brukes på gjensidige tilpasninger mellom mennesker innen en gruppe. Vi vet ofte hva som forventes i ulike situasjoner, f.eks. ved møter, intervjuer eller selskapeligheter, og vi kategoriserer og forstår eksplisitte uttrykk slik som emosjoner, kleskoder og atferdsmønstre (Guldenmund, 2010).

2.3.1 Subkulturer

Som sosiale aktører kan vi tilhøre flere ulike grupper, og vi besitter gjerne forskjellige roller i ulike subkulturer. Slike mangefasetterte tilhørigheter kan gjøre studier av kultur særlig utfordrende, da det kan være krevende å avgjøre til hvilken bestemt kultur man skal tilskrive observerte eller vurderte regelmessigheter i en gruppe (Guldenmund, 2010). Subkulturer er deler av en kultur, som må inneha distinkte forskjeller i form og karakteristikker som således skiller dem fra vertskulturen (Clarke, Hall, Jefferson & Roberts, 1975). Slike grupper er gjerne konsentrert rundt bestemte aktiviteter, verdier, eller bestemt anvendelse av materielle artefakter eller territoriale rom. Imidlertid påpeker Clarke et al. at de også deler signifikante likheter med vertskulturen, men at det ofte er et ønske om en egen gruppeidentitet. Således vil man i slike delkulturer, eller subkulturer, kunne ha ulik oppfatning av hva som er anerkjent, hva som prioriteres, og hva som er riktig å tenke «hos oss».

2.3.2 Mental software

Hvert menneske bærer på mønstre av tanker, følelser og potensiell handling som er lært gjennom personens livsløp. Mye av dette erverves i tidlig barndom (Hofstede, 2010). Ved å benytte en analogi for hvordan datamaskiner er programmert, forstår Hofstede slike mønster av tanker, følelser og handling for *mentale programmer,* eller «software of the mind». Forfatteren forklarer følgelig kulturbegrepet som «den kollektive programmeringen av sinnet, som avgrenser medlemmer fra en gruppe eller kategori av mennesker fra en annen» (Hofstede, 2010, s. 6). Hofstede skiller mellom tre nivåer av slik mental software: (1) universal menneskelig natur, (2), kollektiv kultur og (3) individuell personlighet.

Menneskets natur omfatter de funksjonelle programmene som alle mennesker er født med, slik som behov for å reprodusere, behov for mat, å unngå smerte. Det omfatter således det grunnleggende nivået i vår mentale software (Hofstede, 2010). Iboende i mennesket har vi også et omfangsrikt følelsesregister. Slike grunnleggende karakteristikker kan imidlertid påvirkes av både kollektiv kultur og individuell personlighet. Den felles forståelsen i et samfunn, kollektiv kultur, samt individets personlige karakteristikker, vil kunne påvirke måten et menneske uttrykker sinne på. I tillegg inngår også situasjonelle omstendigheter.

Dog er kultur adskilt fra menneskelig natur og individuell personlighet, hvorav kultur handler om noe som er felles og delt i en distinkt gruppe mennesker. Dette kan ikke sies om naturen

og individers personlighet. Ofte er kultur ansett å være «kollektiv hukommelse» av en gruppe, og er følgelig sammenvevd i historien til denne gruppen.

2.3.3 Kan kultur måles?

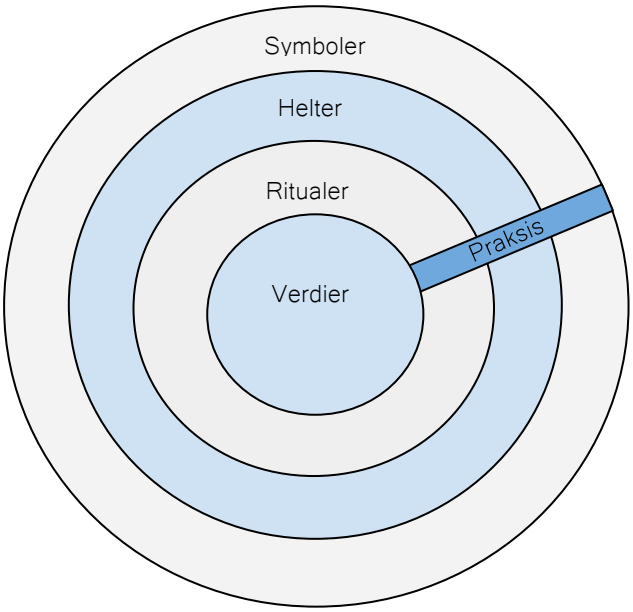
Det har vært hevdet at det kan synes problematisk når man ønsker å benytte «naturvitenskapelige» metoder for å måle kultur og kulturelle fenomener (Haukelid, 2001). Forfatteren skriver: «En slik sterk fokusering på målbarhet og lovmessigheter kan sikkert ha sin misjon innenfor andre deler av samfunnsvitenskapene, men innenfor kulturforskning blir slike tilnærminger mindre fruktbare (Haukelid, 2001, s. 7». Kai Roer hevder på sin side at de som mener at en organisasjons kultur vanskelig lar seg måle, mangler de riktige egenskapene for å måle det han kaller «soft skills». Forfatteren peker følgelig på at kulturen reflekteres i atferd. I vår teknologiske tidsalder er en stor del av atferden loggført og kan slik også spores tilbake. (Roer, 2018). Det handler ifølge han om kunnskap og kompetanse, og om anvendelse av riktige teknikker og analyseverktøy.

Oplenskedal har videre funnet at det er mulig, men vanskelig å måle sikkerhetskultur, hvor forfatteren peker på at det kan bli gjort feilmålinger hvor det igjen fører til feil fokus rundt tiltak. Imidlertid kan det bidra til å gi en pekepinn på hvor «landet ligger» dersom dette kan gjøres korrekt. Det er følgelig strid omkring måling av kultur, og hvorvidt dette kan ha noe for seg. RNNP, som er en måling av risikonivået av norsk petroleumsvirksomhet, er en kartlegging av risikonivået i norsk petroleumsvirksomhet, og følgelig en kan det oppfattes som en måling av kulturen i næringen. Haukelid mener det er utfordrende når det har blitt nærmest et ideal å uttrykke flere forhold kvantitativt, også når det gjelder «myke faktorer», slik som kultur er. (Haukelid, 2001). Således kan det hevdes at det er flere forhold som kanskje ikke fanges opp ved en kvantitativ undersøkelse alene.

2.3.4 Kulturens forskjellige dimensjoner

De fleste forskere ser på kultur som bestående av en kjerne som igjen er omgitt av flere lag, noe som kan minne om en løks utforming (Gundelmund, 2010). Mens kjernen og kulturens etablerte verdier er noe som ligger skjult i dybden, vil kulturen vise seg gradvis gjennom og helt ut til de ytterste lagene. Slik vil de ytre lagene som er observerbare, også være de som er lengst vekk fra kjernen av kulturen. Dermed kan man ikke studere en kultur ved å bare iaktta de ytre lagene. Guldenmund poengterer også at «...similarly, the more deeply a layer is located, the more difficult it becomes to actually change it». Likeledes vil man mest effektivt

kunne endre en kultur dersom man starter med praksisen i de ytterste lag, og ikke verdiene i kjernen (Guldenmund, 2010). Endringer i grunnleggende verdier foregår gjerne svært sakte og gradvis. I en organisasjonskultur vil ofte kjernens verdier samsvare med nasjonale verdier i det landet hvor organisasjonen er lokalisert (Hofstede, i Guldenmund, 2018). Dette bidrar til kulturens reproduksjon og stabilitet over tid.



Figur 3: Kulturens manifestasjon gjennom ulik dybde og nivå. Kilde: Hofstede (2010)

Ord, fakter, bilder og objekter er eksempler på symboler som bærer med seg en bestemt mening som anerkjennes av de som deler kulturen. Ord og språklige uttrykk, «sjargongen», samt kleskoder statussymboler og frisyrer tilhører denne kulturelle kategorien. Nye symboler utvikles, og gamle blir utdatert (Hofstede, 2010). I tillegg vil symboler fra en kulturell gruppe ofte kopieres fra andre grupper. En slik dynamisk endring er også grunnlaget for at symboler gjerne tillegges det ytre lagene, slik som vist i figur 3.

Det laget som er nest ytterst, helter, henviser til de personer som enten er i live eller ei, ekte eller imaginære, og som representerer karakteristikker og egenskaper som er særlig anerkjent og høyt ansett innad i kulturen. Slik fungerer disse personene som forbilder for ønsket atferd (Hofstede, 2010). Slike rollemodeller, eller «helter», kan blant annet være talspersoner og frontfigurer fra politiske parti, frontfigur i et band innen en bestemt musikksjanger, eller for eksempel leder av en interesseorganisasjon. Offentlig opptreden og visuell framtoning, både i

tradisjonelle medier og nyere former for medier, er viktige plattformer som brukes av slike forbilder.

Kollektive ritualer er aktiviteter som gjennomføres for sin egen skyld og har ikke et teknisk formål. Slike begivenheter, som kan være hilsener, taler og religiøse eller sosiale seremonier er ansett å være essensielt i mellommenneskelige konstellasjoner. Hofstede poengterer at det i forretningsmiljøer, næringsliv og i den politiske sfære ofte arrangeres møter og samlinger som tilsynelatende er til for rasjonelle formål, men som i realiteten bærer preg av et rituelt meningsinnhold (Hofstede, 2010). Festtaler, 0-visjoner og uttrykk som «safety first» kan være eksempler på opptredener og språkbruk som i praksis er ritualer. Slike aktiviteter handler om diskurs, måten språket brukes i daglig interaksjon, både i tekst og tale for å kommunisere budskap og tro.

Som vi kan se av figuren, er praksiser en del av kulturens ritualer, helter og symboler. Selv om dette er observerbart og fysisk synlig for utenforstående, vil det kulturelle meningsinnholdet rundt slike praksiser være usynlig for utenforstående. Denne forståelsen vil kun foreligge gjennom måten "innsidere" i gruppen tolker og forstår slike praksiser på (Hofstede, 2010). Figuren viser også kulturens kjerne, bestående av verdier. Verdier, slik det forståes her, betegner tendensene til å foretrekke noen situasjoner eller sosiale fenomener over andre. Verdier er følelser, hvor man kan tenke seg et skille, der en imaginær pil følgelig indikerer en minusside og en plusside. Typisk kan man skille mellom ond og god, farlig og trygt, moralsk og umoralsk, eller mellom åpenhet og hemmelighold (Hofstede, 2010).

En slik sosial læring, av hva som er riktig og hva som er galt, skjer over tid, og gjennom erfaringer som er delt av en stabil sosial enhet. Dersom en slik gruppe mennesker har delt tilstrekkelig mange viktige erfaringer i forbindelse med at de har løst interne og eksterne problemer, kan man anta at slike delte erfaringer også har gitt dem en felles oppfatning av virkeligheten rundt dem og deres plass i den (Schein, 2010). I en organisasjonskontekst, vil det kunne sies at kultur er et lært resultat av erfaringene i en gruppe hvor det eksisterer en avgrenset gruppe med en historie av en viss betydning.

2.3.5 Organisasjonskultur

Det som er fremstilt ovenfor omkring kulturbegrepet og dens ulike lag, kan også sees i lys av en organisatorisk kontekst. I det følgende vil jeg skissere Edgar Schein sin forståelse av

organisasjonskultur, hvor han har gitt en definisjon av kulturbegrepet i en organisasjonssammenheng:

> Kultur er et mønster av grunnleggende antakelser - skapt, oppdaget eller utviklet av en gitt gruppe etter hvert som den lærer å mestre sine problemer med ekstern tilpasning og intern integrasjon - som har fungert tilstrekkelig bra til at det blir betraktet som sant og til at det læres bort til nye medlemmer som den rette måten å oppfatte, tenke og føle på i forhold til disse problemene (Schein, 1987), s.7).

Schein anvender begrepet "grunnleggende antakelser", der andre gjerne benytter ordet verdier, for å poengtere at det handler om noe som ligger i underbevisstheten, og som man ikke er klar over selv. I denne definisjonen kommer det videre fram at kultur er noe som læres videre, og som dermed reproduserer de felles antakelsene. Schein behandler grunnleggende antakelser som det essensielle, det kultur egentlig er, og anser videre verdier og atferd som observerbare uttrykk for den kulturelle essensen.

Grunnleggende underliggende antakelser er dypt forankrede tanker og oppfattelser av hvordan menneskene i en organisasjon forholder seg til omgivelsene, og hvordan de oppfatter seg selv i relasjon til samfunnet og naturen som sådan. Er organisasjonen i stand til å beherske sine omgivelser, risikoer og utfordringer? Slike antakelser handler gjerne om hvilke områder organisasjonens medlemmer anser som viktige, om det er de teknologiske, økonomiske, politiske eller sosiokulturelle forhold som er de viktigste å ta hensyn til.

Enhver kultur rommer sentrale bakenforliggende antakelser om hva det vil si å være menneskelig, og hvordan våre menneskelige instinkt fungerer. Dette er ubevisste, usynlige betingelser for *vår væren* i en organisasjon. I vår vestlige tradisjon er menneskets natur betraktet som modifiserbar; mennesker antas å kunne forbedre seg ved innsats, og vi betraktes videre som ansvarlige og som samfunnets grunnleggende enhet for utvikling (Schein, 1987). En viktig del av enhver kultur er, ifølge Schein, et sett med antakelser om hva som er «virkelig og hvordan man avgjør og oppdager hva som er virkelig. Slike antakelser er således forbundet med hvordan medlemmene i en organisasjon griper saken an, hvordan de avgjør hva som er relevant informasjon og når de har nok av denne informasjonen til å bestemme seg for hvordan de skal handle i praksis (Schein, 1987).

Dersom de overforstående antakelsene om virkeligheten, organisasjons omgivelser og menneskets natur legges til grunn, vil de kunne fungere som rettesnorer for hva som er det rette å gjøre for mennesker. Disse bakenforliggende betingelsene gjør det mulig for oss å forstå og formidle hverdagslige hendelser – handlinger og atferd blir forståelig for oss, og det blir følgelig bekreftet etter stadig gjentakelse.

Verdier kan, basert på Scheins forklaring, forstås som mer bevisste enn de grunnleggende antakelsene, og er ofte eksplisitt uttalt i en organisasjon. Gjerne fungerer de normativt eller som et moralsk kompass, ved at de hjelper organisasjonens medlemmer å håndtere bestemte nøkkelsituasjoner. Schein skriver: «på denne måten kan et sett verdier som blir inkorporert i en ideologi eller organisasjonsfilosofi virke som retningslinjer og som en måte å takle den usikkerheten som er forbundet med ukontrollerbare eller vanskelige hendelser på» (Schein, 1987, s. 14). Verdier predikerer således mye av den atferd som kan observeres.

Dersom verdiene derimot ikke har grunnlag i tidligere kulturell læring i organisasjonen, kan de bli sett på som det Arguris og Schön kaller forfektede verdier. Ettersom verdiene ikke er forankret i organisasjonen, kan de gjerne gi uttrykk for hva som *sies* i organisasjonen, men forutsier ikke hva som *gjøres* i situasjonene hvor verdiene burde ha vært virksomme (Arguris & Schön i Schein, 1987).

I Scheins typologi viser artefakter til den faktiske atferd og de synlige manifestasjoner av fysisk og sosial karakter, det som gjerne er forstått som symboler av Hofstede. På dette nivået kan den romlige utformingen studeres, samt det som gruppen leverer av produkter, dens skrift- og talespråk, samt medlemmenes observerbare praksis av hverdagslige oppgaver og gjøremål (Schein, 1987). Slik atferd kan vise til hva som prioriteres i organisasjonen, og i mer eller mindre grad gjenspeile verdier og antakelser som ligger dypere forankret.

Selv om artefaktene er synlige, kan de dog være vanskelige å tyde. Det er lett å observere artefakter og atferd, selv de mest subtile, slik som måten medlemmene demonstrerer status eller stilling på. Problemet kommer gjerne i det man ønsker å studere hvilke dype mønstre de kan gjenspeile og hvilken betydning de har – dersom de i det hele tatt har noen. Med tanke på at kulturens «insidere» ikke alltid er klar over egne artefakter, kan man gjerne ikke spørre om dem. Imidlertid kan man studere og betrakte dem på egen hånd (Schein, 1987).

Videre er det gjerne slik at organisasjonens medlemmer tilhører ulike kulturer og subkulturer, der tilhørende artefakter og atferd kan komme til uttrykk i den bestemte organisasjonen. Dessuten er også vertskulturen – den større helhetlige kulturen utenfor organisasjonen - bestemmende for hva som er aksepterte antakelser, verdier, atferd og artefakter. Et eksempel i Norge kan være et stort nasjonalt fokus på HMS, og arbeidsmiljøloven som sådan. Det settes således høye krav til beredskap og internkontroll i organisasjoner. Dette kan videre komme til uttrykk i en organisasjonskultur, som ved hjelp av offentlige insentiver utvikler artefakter og sosiale roller (beredskapsplanverk, skilt om å holde seg i rekkverk, verneombud) i tråd med gjeldende nasjonalt lovverk og nasjonalkultur, som igjen kan være forskjellig fra tilsvarende områder i for eksempel Malta, som ikke har den samme HMS-tradisjonen som Norge. Her beveger vi oss over i det som gjerne omtales som en organisasjons sikkerhetskultur.

2.3.6 Sikkerhetskultur

«*Few things are so sought after and yet so little understood*» (Reason, 1997).

Mange har forsøkt å definere og skrive om sikkerhetskultur, eller *safety culture.* Dog finnes det ingen faglig konsensus om hva begrepet betyr (Hopkins, 2006). Det er likevel noen felles trekk som kan sies å gå igjen. En organisasjons sikkerhetskultur kan gjerne forstås som en del av den helhetlige organisasjonskulturen. Til tross for at safety- og security-hendelser har ulike karakteristikker når det gjelder foranledning og forankringen av årsakene, handler det likeledes i en kulturkontekst om delte antakelser, kunnskap og tankemønstre, hvilke visjoner man forplikter seg til, samt hvilken praksis som er anerkjent som den riktige i en organisasjon. Hale definerer safety-kultur som «… the attitudes, beliefs and perceptions shared by natural groups as defining norms and values, which determine how they can act and react in relation to risks and risk control systems» (Hale, 2010, s. 7). Også Aven et al. sier at det handler om en felles forståelse, og der denne forståelsen gir føringer for hvilke valg som tas. Forfatterne skriver:

> (...) den kollektive forståelse av hva som er farlig og hvordan en bidrar til å redusere farene. Ofte vil valg av sikkerhetstiltak bli avveid mot økonomiske og tidsmessige hensyn, og organisasjonens sikkerhetskultur vil kunne virke avgjørende for om en velger snarveier og lettvinte løsninger på bekostning av målene for sikkerhet (Aven, et al. 2004).

Sikkerhet handler om atferd, og å forstå kultur i en sikkerhetskontekst handler således om hvilken atferd som er anerkjent som den riktige. Hopkins sier at hver organisasjon har en kultur, eller en serie subkulturer, og at denne kan forventes å påvirke sikkerhet (Hopkins, 2006). Noen virksomheter og sektorer har gjerne en bedre evne til å håndtere uforutsette hendelser og usikkerhet, og skape robusthet og såkalt resiliens i organisasjonen.

2.3.6.1 Resilience engineering

Ved forklaringer på organisasjoners robusthet og deres respons på ulykker eller katastrofer, har begrepet resiliens vokst fram som et sentralt begrep. Resiliens har vært tillagt ulike betydninger og meningsinnhold, men er ofte forstått ut ifra en organisasjons evne til tilpasning når noe uforutsett skjer, eller evne til organisatorisk og mellommenneskelig læring, samt å vokse seg sterkere etter en krise (Engen et al., 2016). Perspektivet «Resilience engineering» tar for seg en ny måte å tenke om sikkerhet på, fortrinnsvis når det gjelder uønskede utilsiktede hendelser, hvor det viktige er å rette oppmerksomhet på suksess og det som går riktig for seg (Hollnagel, 2012). Ifølge Hollnagel har det vært for mye fokus på det som går galt, og det å reagere etter en hendelse har inntruffet. Denne måten å tenke sikkerhet på kaller Hollnagel for Safety I. Han fremhever at det vi bør konsentrere oss om i arbeidet med sikkerhet, er å forstå den «hverdagslige praksis», nemlig når det ikke går galt. Han skriver:

> Doing so will change the definition of safety from `avoiding that something goes wrong´ to `ensuring that everything goes right´ - or more precisely to the ability to succeed under variying conditions, so that the number of intended and acceptable outcomes (in other words, everydag activities) is as high as possible. The consequence of this definition is that the basis for safety and safety management now becomes an understanding why things go right, which means an understanding of everyday activities. (Hollnagel, 2012, s. 813).

I et safety II-perspektiv er det dermed ønskelig å forsikre seg om at hverdagens aktiviteter utspiller seg på en god og riktig måte, slik at hverdagsaktivitetene oppnår sine formål. Hollnagel peker på at man må bort fra den reaktive, hendelsesstyrte måten å betrakte sikkerhet på, og være proaktiv, forutsigende og på jakt etter endringer og ulike signaler. For å klare dette, kreves det en forståelse av hvordan systemene fungerer, samt søke kontinuerlig innsikt i hvordan omstendighetene og samfunnet rundt utvikler og endrer seg (Hollnagel, 2012). I tillegg vil det være fruktbart å se på hvordan ulike funksjoner og delsystemer er avhengig av og påvirker hverandre. For å finne slike mønstre, er det ifølge Hollnagel

nødvendig å ta seg tid til å forstå og sette seg inn i hva som kan skje, i stedet for å bruke alle ressurser på brannslukking. En slik *mindfulness*, eller bevissthet, kan også sies å være viktig i en security-kontekst. Vivold har blant annet funnet at perspektivet «resilience engineering» kan være treffende for en del av de utfordringer som noen organisasjoner opplever med tanke på security-trusler (Vivold, 2015).

2.3.6.2 Black Swan

«Black swan»-teorien har fått sitt navn etter den første oppdagelsen av Australia, hvor man på forhånd hadde en akseptert tro på at alle svaner var hvite. Man hadde følgelig ikke observert noe annet, derfor var ikke den sorte svanen en del av den etablerte kunnskap. «Black swan»-teorien er basert på en metafor som beskriver hvordan alvorlige, uønskede hendelser, gjerne tilsiktede angrep som terroraksjoner, er svært uventede, og kommer som en overraskelse. Det er dermed knyttet stor usikkerhet til en slik situasjon. Terrorangrepet den 11. September i 2001 er et eksempel på en slik «black swan». I følge Taleb er den sorte svane et bilde på vår kollektive og individuelle kunnskapsbegrensning, og er således ikke et objektivt fenomen. Terrorangrepet i New York i 2001 var en sort svane for ofrene og samfunnet som sådan, men ikke for gjerningspersonene. En slik usikkerhet og mangel på kunnskap om fremtiden, stiller oss over utfordringer for hvordan vi i organisasjoner og virksomheter, og i samfunnet som sådan, skal håndtere en slik type risiko. Taleb fremhever at det er viktig å tørre å innse det vi ikke vet. Han skriver: «Black Swans being unpredictable, we need to adjust to their existence (rather than naively try to predict them). There are so many things we can do if we focus on antiknowledge, or what we do not know» (Taleb, 2010, s. XXV). Følgelig kan du ikke se inn i glasskulen og forutsi hvor og hvordan en hendelse utspiller seg.

2.3.7 Security-kultur

Det foreligger lite forskning og litteratur på security-kultur, og det er ingen enighet om en definisjon, ei heller en akseptert måte å måle fenomenet på som kan anvendes utenfor smale domener (Malcolmson, 2009). Østensjø og Larsen har funnet at det er behov for en tydelig begrepsavklaring for å belyse karakteristikkene rundt security, og at begrepet fremstår som nytt og umodent (Østensjø & Larsen, 2015). På et generelt grunnlag kan man gjerne si at grunntrekkene i kultur-begrepet i stor grad går igjen, og Roer viser til at security-kultur kan forstås som en subkultur innen en organisasjons kultur, og således kan betraktes som den delen av den helhetlige organisasjonskulturen som fokuserer på security-aspektet i

virksomheten. Kai Roer definerer security-kultur som «the ideas, customs and social behaviours of a particular people or group that helps them be free from threat and danger» (Roer, 2015, s. 12). Hvordan passord håndteres i en virksomhet, eller hvordan ansatte oppdager og håndterer en fremmed person som er i bygningen, er en del av security-kulturen i organisasjonen. Videre vil også måten man definerer og implementerer retningslinjer på, samt trener ansatte i security-atferd også påvirke security-kulturen i en organisasjon (Roer, 2015). Følgelig hevder Roer at all sosial praksis i en organisasjon vil påvirke ens security-kultur, og at security-kultur også påvirker all praksis i en organisasjon. Det er kanskje dette som ligger i kulturbegrepet, den kontinuerlige, dynamiske reproduksjon av sosial atferd. Det er noe som skapes, og gjenskapes.

Også Malcolmson er opptatt av at security-kultur handler om atferd, og hvordan vi forholder oss til de organisatoriske omgivelsene. Han henviser til en studie gjennomført av QinetiQ, som er et britisk ingeniør- og forskningsselskap, som har funnet at et security-system i stor grad vil være påvirket av holdninger og atferd av ansatte, og deres interaksjon med security-prosedyrer, teknologi og systemer. De organisasjoner som evner å forstå og forbedre sin security-kultur hvor security-dimensjonen er en kritisk faktor for suksess, er bedre i stand til å oppnå sine primærmål og beholde sitt rykte.

I studien som Malcolmson refererer til, ble det utviklet flere forskjellige temaer som hevdes å inngå som del i security-kultur-begrepet. Noen av disse er: infrastructure, physical security, information security, human resource actitivies, organisational staff og management (Malcolmson, 2009). Forfatteren går ikke inn på hvert enkelt tema, men de ulike faktorene kan forstås som en kombinasjon av menneskelige, teknologiske og organisatoriske elementer. Security-kultur kan på mange måter omfatte svært mange av de komponenter i en organisasjon, både det som blir gjort, men også det som uttrykkes, og er tilstede som artefakter eller objekter. Malcolmson viser også til en forskjell mellom fysisk security og security med tanke på informasjon. Dette er en interessant distinksjon, da det kan tenkes at medlemmer i en virksomhet kan ha en annen tilnærming og atferd til fysisk security, enn det som gjelder security rettet mot IKT og informasjonssikkerhet. De temaene som er utbrodert som følge av studien er følgelig utgangspunktet for følgende definisjon av security-kultur:

> Security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organisation, and behaviours they perform, which could potensially

> 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).

Denne forståelsen viser til at security-kultur handler om de antakelser, verdier og holdninger som organisasjonsmedlemmer har, og samsvarer videre også med Scheins forståelse av kultur, som grunnleggende antakelser og verdier, som kan påvirke sosial praksis. Malcolmson viser i sin definisjon, at security-kultur følgelig kan påvirke security-tilstanden i organisasjonen.

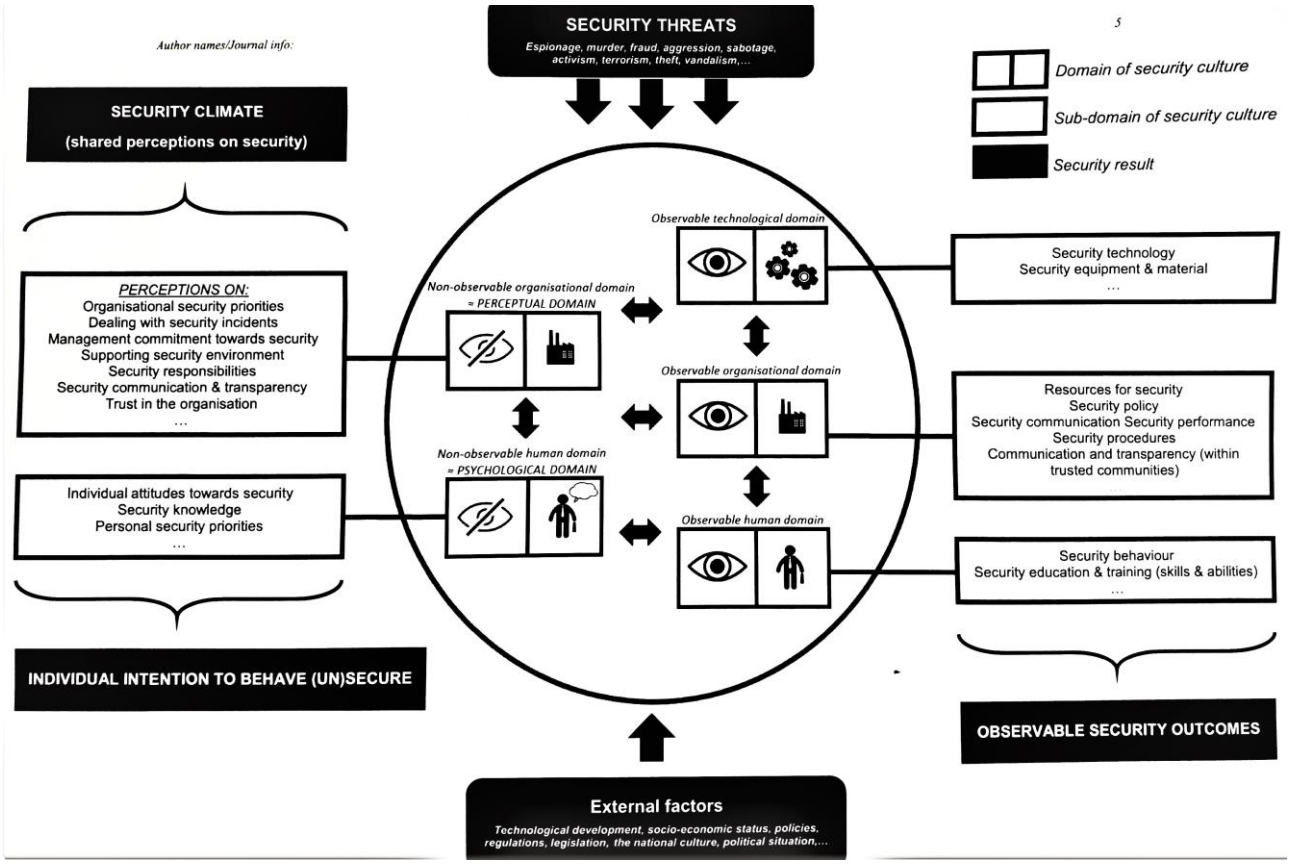
Imidlertid er det blitt påpekt utfordringer ved begrepet security-kultur, særlig med tanke på umodne teoretiske perspektiver på området. Svært mange teorier og perspektiver fra safety-kultur har vært anvendt i forsøk på å forklare og forstå security-kultur. Dog kan dette være problematisk da man gjerne ikke ønsker den samme form for bevissthet, eller mindfulness, i relasjon til security-utfordringer. Jore (2017) stiller følgelig spørsmålstegn ved om en mindful kollega i en organisasjon, kan bety å være mistenksom ovenfor sidemannen. Hva gjør dette med tilliten i organisasjonen? Videre pekes det på at kultur, i en organisatorisk kontekst dekker stort sett alt en organisasjon gjør. Således kan det være utfordrende å kartlegge kulturens påvirkning på security, da «alt» blir kultur.

2.3.7.1 Integrert rammeverk for security-kultur

Det har vært hevdet at forskning rundt security har manglet en helhetlig tilnærming (van Nunen, Sas, Reniers, Vierendeels, Ponnet & Hardyns, 2018). Både safety og security kan betraktes som en del av den totale organisasjonskulturen, og impliserer at både safety og security bør integreres i andre bedriftsprosesser. Van Nunen et al. argumenterer for at man bør integrere safety og security i et holistisk rammeverk. Videre blir det vektlagt at det oftest er de teknologiske aspektene ved security-kultur som oppnår oppmerksomhet, og hevder at det er nærmest ingen referanser til andre typer security-utfordringer (van Nunen et al., 2018). Rammeverket er en kombinasjon av tre domener, et teknologisk, et organisatorisk og et menneskelig domene. Dette kan sees opp mot den mer kjente teorien om MTO, hvor samspillet mellom mennesker, teknologi og organisasjon trekkes fram (Rollenhagen, 1997). Rammeverket er basert på en tilsvarende forståelse for safety-kultur utviklet av Vierendeels et al. (2018).

Følgelig består den integrerte tilnærmingen av: 1) et teknologisk domene, knyttet til security-teknologi, materiale og utstyr som er tilgjengelig i bedriften, 2) et organisatorisk domene,

hvor security management, bedriftens security policyer, samt ressurser som er tilgjengelig for security inngår, og 3) et menneskelig domene, som omhandler kunnskap, holdninger, antakelser og beslutninger, i tillegg til atferd av individer med tanke på security. Security-kulturen av en organisasjon er påvirket av eksterne faktorer, slik som teknologisk utvikling eller sosio-økonomisk status av regionen, samt politikk og regulering. Videre er security-kultur uunngåelig koplet til trusler som en spesifikk organisasjon er eksponert for.
De mørke boksene med innholdet «security climate», «individual intentions to behave (un)secure» og «observable security outcomes» viser til det som forfatterne kaller for security results.



Figur 4: En integrert modell for security-kultur. (van Nunen et al., 2018)

Ved de tre observerbare domenene, vil subdomener som ressurser, policy`er, kommunikasjon og atferd gi utslag i observerbare security-resultater. Ved det ikke-observerbare organisatoriske (perseptuelle) domenet gir de ulike subdomenene, slik som organisatoriske prioriteringer og forpliktelser angående security, utslag i security-klimaet i en organisasjon. Videre vil det ikke-observerbare menneskelige (psykologiske) domenet, med subdomener

som omhandler personlige prioriteringer og holdninger, resultere i en intensjon for atferd, enten en sikker eller usikker atferd.

Forfatterne hevder at rammeverket tilbyr et utgangspunkt for å måle og kontrollere en organisasjons security-kultur. Dette er en interessant uttalelse, da det kan stilles spørsmål ved om kultur lar seg måle. Van Nunen et al. fremhever imidlertid også betydningen av kontinuerlig oppmerksomhet rundt security-dimensjonen, i tillegg til verdien av en helhetlig tilnærming for å involvere hele organisasjonen i henhold til å oppnå bærekraftige forbedringer i security-feltet (van Nunen et al., 2018).

2.4 Intensjoner og praksis

Det er en antakelse i denne oppgaven, at selve kjernen av security-kultur ligger i differansen mellom intensjoner, og den faktiske praksis som gjelder security-relaterte aktiviteter. I utarbeidelsen av indeksen som favner over intensjoner og praksis, har det blitt formulert ni safety- og security-kulturfaktorer. For hver faktor er det tilknyttet et ideal, eller en norm for hva som ansees å være en god kultur, derav en felles forståelse av «slik gjør vi det her hos oss» Disse benyttes således i spørreundersøkelsen som ligger til grunn for den kvantitative analysen, hvor spørsmålene er delt inn i de ulike temaene. Utviklingen av temaene er det Safetec som har stått for, og er følgelig et resultat etter bred litteraturgjennomgang. De temaer som har blitt utarbeidet, er: Virksomhetens forpliktelse, organisering og læring, informasjonsflyt, bevissthet om security, felles risikoforståelse, nærmeste leders rolle, avviksrapportering, prosedyrekvalitet og håndtering av arbeidspress. Holdninger, verdier og de grunnleggende antakelse, er dermed bakt inn i en av de ni faktorene. I det følgende vil jeg presentere temaene som benyttes i den videre empirien.

Virksomhetens forpliktelse. Virksomhetens forpliktelse handler om hva virksomheten overordnet kommuniserer som sin intensjon, for eksempel i form av visjoner, verdier og strategiske målsetninger relatert til security eller safety. Når virksomhetens intensjon kommuniseres ut, kan det forstås som en forpliktelse. Typiske eksempler av virksomhetens intensjoner er gjerne formuleringer som «Safety first», «Høyt fokus på sikkerhet», «best på sikkerhet/security» eller lignende. *Det er en felles norm* at alle, både ledere og personalet, skal kjenne virksomhetens intensjoner når det gjelder safety og security, og følge opp intensjonen i

daglig handling. I tillegg skal det være et samsvar mellom ord og handling, også kjent som «walk the talk».

Håndtering av arbeidspress. Videre opplever mange organisasjoner situasjoner hvor ulike mål kommer i konflikt. En typisk konflikt er gjerne sikkerhet versus produksjon, eller sikkerhet versus frihet. Å nedprioritere rutiner knyttet til security, til fordel for andre mål, kan sies å være en av flere faktorer som påvirker security-praksisen i en organisasjon, og som videre påvirker security-nivået i en virksomhet. Denne forståelsen er i tråd med det som ble skissert i forbindelse med Malcolmson tidligere. *Det er en felles norm* at alle ansatte har en bevissthet om at målkonflikter eksisterer og at disse kan gi arbeidspress. Arbeidspresset må videre håndteres, slik at safety og security-hensyn ikke blir skadelidende. Temaet er nært knyttet til ledelse, ettersom lederes uformelle og formelle sanksjoner i stor grad avgjør hvordan målkonflikter håndteres.

Bevissthet om security. Det ligger i naturen av arbeidet med security, at en del av security-vurderingene er hemmelige. Dermed vil også bevisstheten rundt security kunne variere. Dog kan man ha forestillinger og oppfatninger om hva som er skjermingsverdige verdier i virksomheten, samt at organisasjonens medlemmer forstår behovet for å beskytte disse verdiene fra noen som kan tenkes å skade dem. En slik bevissthet eller mangel på sådan, kan si noe om virksomhetens intensjon rundt security-arbeid. *Det er en felles norm* at de ansatte er klar over hvilke verdier man har med å gjøre, og at personellet forstår at det også kan være intern trussel i virksomheten.

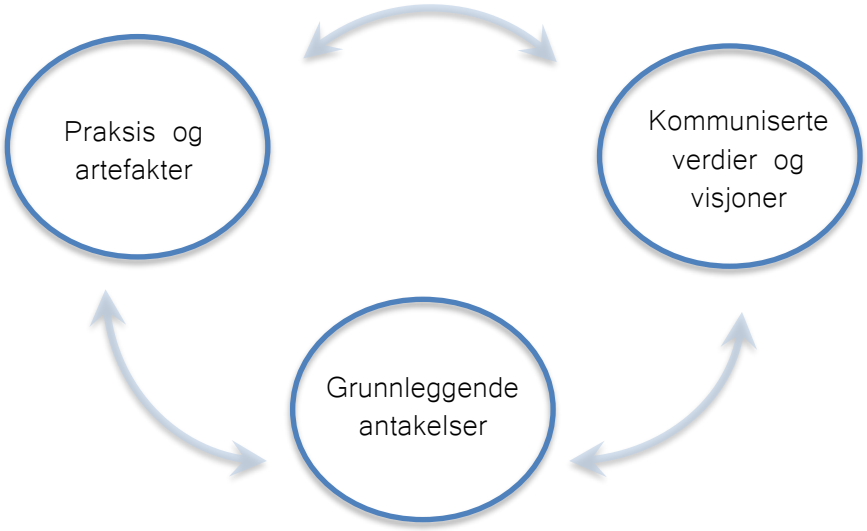
Avviksrapportering. Avviksrapportering handler om den formelle rapporteringen av nesten-hendelser og hendelser relatert til safety og security. Temaet dekker datainnsamlingsdelen av læringsprosessen, og overlappes av temaet som går på organisering og læring. *Det er en felles norm* at det struktureres og etableres en rapporteringskultur, som en del av sikkerhetskulturen, og som oppfattes som noe positivt av alle. Det skal videre være en fungerende læringssløyfe som del av en kontinuerlig forbedring: Avvik rapporteres, tilbakemeldinger gis, man utfører analyser av trender og bakenforliggende årsaker, samt utarbeider tiltak som følges opp av ledere.

Informasjonsflyt. Informasjonsflyt handler om samhandling innen og mellom organisatoriske enheter og henspiller på at personalet deler informasjon, og/eller koordinerer oppgaver for å

oppnå et felles mål. Dette handler følgelig om samarbeid og informasjon som enten deles formelt eller i uformelle nettverk. Igjen kan vi trekke linjer til Malcolmson og hans argumentasjon rundt at samhandling både ved menneskelige ressurser, og mellom systemets komponenter, er en vesentlig faktor av security-kultur (Malcolmson, 2009). *Det er en felles norm* at lærdom fra hendelser og ulykker deles for å nyttiggjøre seg ervervet kunnskap på tvers av organisatoriske enheter.

Nærmeste leders rolle. Ledere har en vesentlig rolle i en organisasjons security-kultur, blant annet gjennom oppfølging av personalet når det gjelder safety- og security-relatert arbeid, og hvorvidt linjeledere godtar at personalet gjør feil. *Det er en felles norm* at ulike menneskelige feil erkjennes som uunngåelige. Det er et fundamentalt prinsipp i styring av safety og security at det er menneskelig å feile. På et overordnet plan skal linjeledelsen bidra til å jobbe for å imøtekomme alle normer tilhørende de faktorer/temaer i kartleggingen av safety- og security-kultur.

Oppsummerende kan man i tråd med Schein´s typologi hevde at medlemmer i en organisasjons security-kultur, sitter på grunnleggende antakelser rundt hva som er virksomhetens intensjon med tanke på security. Videre kan de ha en bevissthet rundt hvilke verdier man bør skjerme, samt en forestilling om hvilke trusselaktører som er aktuelle. Man utvikler grunnleggende antakelser om status quo, men også gjerne en forutsigbarhet om mulige hendelser eller aktiviteter. Dette manifesteres så i verdier, som kan uttrykkes i form av «policies» eller visjoner som igjen legger føringer for atferd og artefakter i virksomheten. Essensen i de grunnleggende antakelsene, verdiene og de manifesterte artefaktene læres bort til nye medlemmer som den rette måten å tenke, føle og handle på i forhold til visse utfordringer og problemer. Slik kan kulturen reproduseres og vedlikeholdes i en organisasjon. Dette oppsummeres i figuren på neste side.



Figur 5: Kultur som prosess: grunnleggende antakelser, verdier og praksis. Basert på Scheins forståelse av kultur.

3. Metode

En forskningsmetode er en framgangsmåte, eller et middel til å belyse og løse vitenskapelige problemer og spørsmål, og komme fram til ny kunnskap (Hellevik, 1999). Det handler således om å samle inn, analysere og bearbeide informasjon.

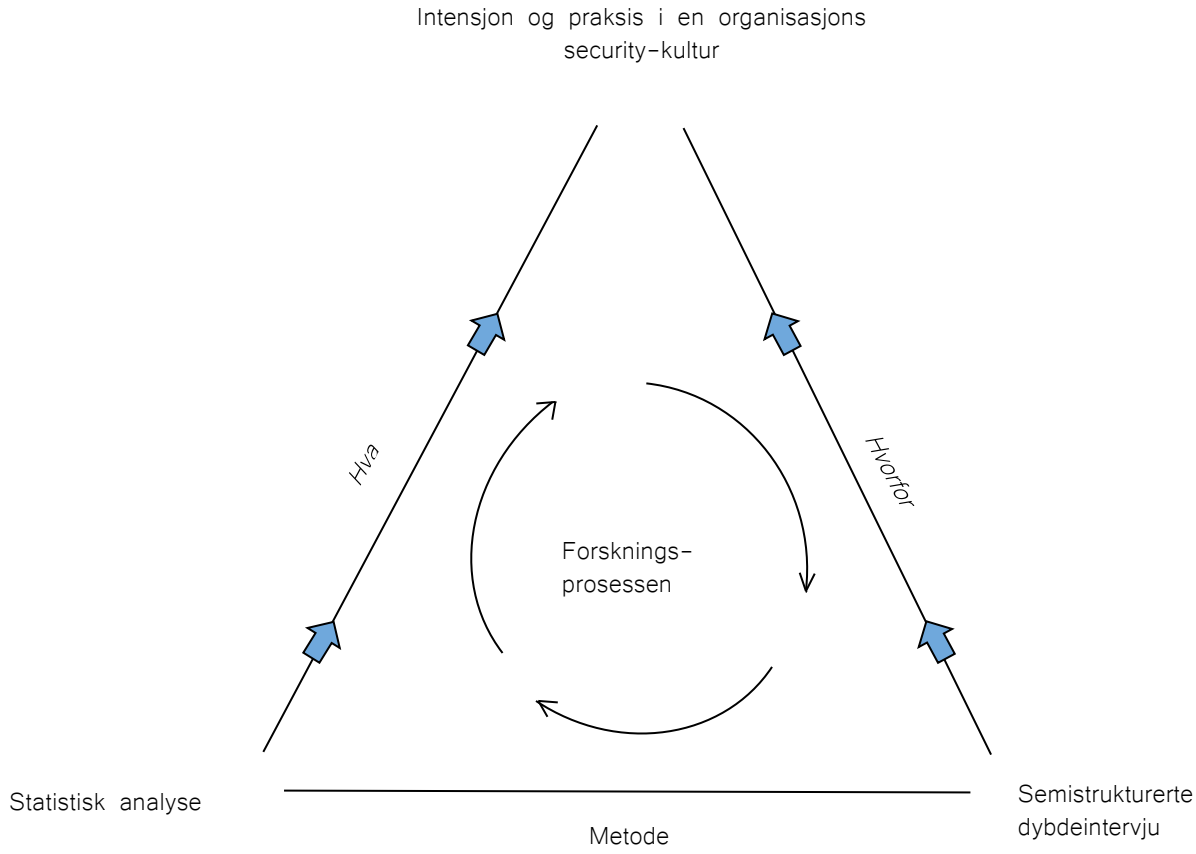
Problemstillingen legger opp til både en kvantitativ og en kvalitativ tilnærming. En slik kombinert framgangsmåte er mest hensiktsmessig, da kvantitativ og kvalitativ metode tilbyr ulike verktøy for å belyse oppgavens problemstilling. For å undersøke et eventuelt gap eller samsvar mellom organisasjonens intensjoner og dens faktiske praksis, vil det være formålstjenlig å benytte surveydata fra større grupper av enheter, som kvantifiseres ved hjelp av statistiske metoder. Dette legger til rette for en bred behandling av data, som ved hjelp av ulike framstillinger, figurer og statistiske mål tilbyr en overordnet oversikt over datamaterialet.

Etter en slik deskriptiv analyse, vil det være formålstjenlig med en mer induktiv og eksplorerende tilnærming for å forsøke å skape innsikt og forståelse rundt *hvorfor* de statistiske resultatene viser det de gjør. Ettersom security og security-kultur vurderes som et umodent og nytt område i sikkerhetslitteraturen, er det hensiktsmessig å gå dypere i materien og forsøke å undersøke perspektiver og oppfatninger rundt hva security-kulturbegrepet er, hvorvidt det kan kartlegges, samt få et innblikk i hva begrepet som sådan kan gi oss.

3.1 Metodetriangulering

Kvalitativ og kvantitativ metode, samt kombinasjonen av disse metodene, mixed method, representerer ulike tilnærminger til kunnskapsproduksjon i samfunnsvitenskapene (Morgan, 2014). Bruken av *mixed methods* involverer innsamling, analyse og kombinasjon av både kvantitative og kvalitative data i en studie. Blaikie poengterer at samfunnsvitenskapelig forskning må anses som en prosess bestående av å bevege seg fram og tilbake mellom ulike steg, som nødvendiggjør anvendelse av forskjellige metoder og tilnærminger i ulike faser av forskningen (Blaikie, 2010). En mixed method-tilnærming har blitt benyttet i denne studien da forskningsspørsmålene ikke kan besvares ved enten kvalitativ eller kvantitativ metode alene. I tillegg til en statistisk tilnærming, hvor jeg finner ut *hva* som foreligger, har det vært ønskelig å kaste lys over betraktninger om *hvorfor* dette foreligger. I forlengelse av dette ligger det også implisitt et behov for å søke mer innsikt i hva dette begrepet kan gi oss i arbeidet med en

organisasjons sikkerhet og hvordan det bør inngå i en bedrifts helhetlige kultur og arbeid med sikkerhet generelt, og security spesielt.



Figur 6: Modell av forskningsprosessen vist ved metodetriangulering

---

Forskningsprosessen begynte med et ekstensivt design, hvor det ble utviklet en hypotese for senere kvantitative analyser. Denne deduktive framgangsmåten ga interessante funn, men jeg ønsket videre kunnskap om hvorfor disse funnene forelå. Dermed supplerte jeg også med et mer eksplorerende opplegg, med fem dybdeintervjuer. Studien bærer derfor preg av hypotese-testing, i tillegg til å være teoriutviklende. Denne metodikken gjør meg i stand til å være fleksibel, og spenne over et bredt kunnskapsgrunnlag for oppgavens siktemål. I figuren nedenfor presenteres forskningsopplegget som er lagt til grunn for denne studien.

3.2 Kvantitativ tilnærming

I det følgende vil jeg vise hvordan jeg har gått fram i datainnsamlingen som ligger til grunn for min studie, i tillegg til de påfølgende statistiske analyser og tester. All databehandling hva gjelder statistikk er gjennomført i statistikkprogrammet SPSS.

3.2.1 Datainnsamling

Grunnlaget for undersøkelsen har vært en spørreundersøkelse som er utført av Safetec for et Facility Management-selskap. Undersøkelsen har en svarprosent på 57 %, der nettoutvalget er på 878 respondenter. En lav svarprosent kan påvirke den eksterne validitet, og således gyldigheten for undersøkelsen. Imidlertid vurderes svarprosenten i undersøkelsen å være tilstrekkelig for generaliserbarheten i den gjeldende organisasjonen, særlig på grunn av et tilfredsstillende antall respondenter. Alle personlige data om respondentene i spørreundersøkelsen er anonymisert.

3.2.2. Sammensatte mål

Sammensatte mål bygger på en eller flere indikatorer, og er i denne oppgaven benyttet i analyser av data fra spørreundersøkelse. Sammensatte mål kan fange inn flere fasetter ved et rikt teoretisk begrep enn det som gjerne er tilfelle med en enkel indikator (Ringdal, 2001). I denne oppgaven benyttes begrepet indeks, som kan forstås som et sammensatt mål hvor indikatorene former verdiene på den latente variabelen. I denne oppgaven er det benyttet fire slike indekser, som er «security work as intended», «security work as done», «safety work as intended» og «safety work as done». For hver av disse målene er det tilknyttet spesifikke spørsmål som er operasjonalisert i henhold til områder for praksis og for intensjoner på henholdsvis safety og security. Svaralternativene for hvert spørsmål er på ordnial-nivå, altså kategorier som kan rangordnes (Ringdal, 2001), og ble kodet fra 1 (det laveste) til 5 (det høyeste). Indeksen som sådan har en langt større variasjon, og ved kodingen er det et absolutt nullpunkt. Nullpunktet, samt at indeksen nærmer seg en kontinuerlig skala, viser slektskap med variabler på forholdstallsnivå. Det er følgelig vurdert å behandle variablene ut ifra et kontinuerlig målenivå. Spørsmålene som har inngått i indeksene er gjengitt i tabellene nedenfor. Som det kan sees av spørsmålene nedenfor, er det spurt om hvor ofte noe blir gjort, da dette vurderes som en god måte å fange inn og operasjonalisere begrepet på

3.2.2.1 Intensjon og praksis for security

Faktor i spørreskjema	*Spørsmål*
Bevissthet om security	Vi er bevisste på at noen kan utnytte XX for å skade andre mennesker og samfunnet utenfor virksomheten
Bevissthet om security	Jeg kan se for meg at noen kan ønske å skade XX i fremtiden
Bevissthet om security	Vi er bevisste på at egne ansatte kan ønske å skade oss
Virksomhetens forpliktelse	I XX har vi høyt fokus på sikring av virksomheten

Tabell 2: Spørsmål som inngår i intensjoner for security

Faktor i spørreskjema	*Spørsmål*
Håndtering av arbeidspress	Hvor ofte velger dere å få jobben gjort effektivt fremfor å beskytte XX mot noen som kan ønske å skade virksomheten?
Håndtering av arbeidspress	Hvor ofte går XXs behov for å dele informasjon knyttet til deg på bekostning av din rett til privatliv?
Håndtering av arbeidspress	Hvor ofte går beskyttelsestiltak, for eksempel overvåking, på bekostning av trivsel på jobb?
Håndtering av arbeidspress	Hvor ofte velger dere sikring fremfor sikkerhet, i situasjoner der begge deler er viktige?

Tabell 3: Spørsmål som inngår i praksis for security

3.2.2.2 Intensjon og praksis for safety

Faktor i spørreskjema	*Spørsmål*
Virksomhetens forpliktelse	Ledelsen i XX jobber forebyggende for å hindre ulykker
Nærmeste leders rolle	Min nærmeste leder oppfordrer alltid de ansatte til å fokusere på sikkerhet
Virksomhetens forpliktelse	I XX har vi høyt fokus på sikkerhet

Tabell 4: Spørsmål som inngår i intensjoner for safety

Faktor i spørreskjema	*Spørsmål*
Informasjonsflyt	Hvor ofte mottar dere informasjon om hendelser/ulykker som har skjedd i andre avdelinger?
Håndtering av arbeidspress	Hvor ofte bryter dere rutinene/prosedyrene på grunn av XXs krav til effektivitet?
Håndtering av arbeidspress	Hvor ofte er det nødvendig å ignorere sikkerhetsregler for å få jobben gjort?
Håndtering av arbeidspress	I praksis, hvor ofte går hensynet til produksjon foran hensynet til sikkerhet?
Avviksrapportering	Hvor ofte blir avvik fra regler og rutiner/prosedyrer rapportert?
Avviksrapportering	Hvor ofte blir nestenulykker/tilløp systematisk rapportert?
Informasjonsflyt	Hvor ofte deler dere sikkerhetskritisk informasjon med kolleger?

Tabell 5: Spørsmål som inngår i praksis for safety

3.2.3 Vurdering av innholdsvaliditet

Validitetsbegrepet tar for seg hvorvidt man måler det teoretiske begrepet man ønsker å måle. Innholdsvaliditet viser til om utvalget av indikatorer dekker en hypotetisk populasjon av indikatorer, følgelig om målet dekker de viktigste aspekter ved begrepet (Ringdal, 2001). Ved operasjonaliseringen av intensjoner for security, var det følgelig viktig å inkludere de spørsmål som synes å representere bevissthet, samt visjonen om at sikkerhet er viktig i XX. Det er verdt å merke seg at det sammensatte målet som går på praksis for security, er alle fra faktoren «håndtering av arbeidspress». Dette kan utfordre validiteten noe, da det meste her går på målkonflikter. Imidlertid kan det hevdes at nettopp dette er en sentral del av hvordan security-atferd foregår, nemlig hvordan man prioriterer. På de resterende målene for safety er det en blanding av ulike faktorer, og det er følgelig forsøkt å dekke de ulike nyanser av begrepene.

3.2.4 Reliabilitetsanalyse: Cronbachs alfa

Informasjon om reliabilitet er vesentlig for å kunne vurdere hvorvidt et indikatorsett representerer en tilfredsstillende operasjonalisering av et begrep. Ved homogene indikatorsett

kan Cronbachs alfa gi uttrykk for den indre konsistens, altså en type reliabilitet (Ringdal, 2001)

Det har vært gjennomført en reliabilitetsanalyse for å estimere den indre konsistensen til de fire indikatorsettene «security work as intended», «security work as done», «safety work as intended» og «safety work as done». Cronbachs alfa viser i hvilken grad resultatet ville blitt det samme dersom indikatorsettet ble byttet med et nytt indikatorsett fra samme indikatorunivers.

3.2.5 Paired samples T-test: signifikanstest av to gjennomsnitt

T-test er en enkel og oversiktlig måte å kartlegge forskjellen mellom to grupper. En «paired samples t-test» sammenligner gjennomsnittet av to sammenholdte grupper av mennesker eller tilfeller, eller sammenligner gjennomsnittet av en gruppe som undersøkes på to ulike tidspunkt. I denne studien er det gjort en paired samples t-test for å sammenligne gjennomsnitt mellom «security work as intended» og «security work as done» som det ene paret, og mellom «safety work as intended» og «safety work as done» som par nummer to. Dette for å finne om det er noen forskjell mellom intensjoner og praksis både for safety og security.

Det er satt et konfidensintervall på 95%. Konfidensintervallet viser til intervallet som vi med 95 % sannsynlighet kan si at populasjonsgjennomsnittet ligger innenfor. Statistisk signifikans indikerer sannsynligheten for at den observerte forskjellen mellom datasettene skyldes tilfeldigheter.

Når vi skal ta stilling til om en hypotese skal forkastes eller ikke, må vi velge et nivå for hvor stor forkastningsfeil vi er villig til å akseptere. Ettersom det i analysen er satt et konfidensintervall på 95 %, er signifikansnivået 5% ($\alpha = 0{,}05$). Hvis nullhypotesen er riktig godtar vi 5% sjanse for å gjøre en forkastningsfeil.

3.2.6 Korrelasjonsanalyse

Det er utført en korrelasjonsanalyse for å finne om det er statistisk sammenheng mellom indikatorsettene, og hvor sterk denne sammenhengen er. Dette er ønskelig for å se på om høy score på intensjon for security også betyr høy eller lav score for praksis for security. Jeg har

for dette formålet benyttet Pearsons korrelasjonskoeffisient. Det viktig å påpeke at denne analyseteknikken ikke sier noe om kausalitet, men viser en sammenheng mellom de to indikatorsettene. Det som er særlig interessant ved denne analysemetoden, er at den også graderer styrken på forholdet. Det kan være en negativ sammenheng, hvor den ene verdien stiger og verdien på den andre synker, eller en positiv korrelasjon hvor en høy verdi på en variabel også tilsier høy verdi på en annen. *R* varierer følgelig mellom -1 og 1, hvor 0 er ingen sammenheng. Jo sterkere sammenheng, jo nærmere 1 eller -1 vil *r* være.

3.3 Kvalitativ tilnærming

I oppgaven er det også anvendt en mer dyptgående framgangsmåte, der det har blitt utført dybdeintervjuer med fem personer. Med en teoretisk forankret oppgave, i tillegg til statistikk, var det ønskelig å kunne få mer innsikt i hvordan security-kultur er annerledes enn den mer etablerte safety- eller sikkerhetskulturen, og se på videre hva som kan være årsaken for den kvantitative undersøkelsen av selskapets security-kultur. Ettersom security-kultur framstår som et umodent begrep, var det også ønskelig for meg å gå dypere inn i fenomenet, for å kartlegge hva som menes med begrepet og hva dette begrepet kan gi oss faglig.

3.3.1 Utvalg

Utvalget i den kvalitative delen av oppgaven er valgt ut ifra hensyn til kompetanse rundt sikkerhet og security. Dette utvalget består av fem informanter, hvorav to personer er representanter fra organisasjonen XX. Den ene av disse arbeider med selskapets styringssystem på et overordnet plan via deres hovedkontor, og har følgelig et kvalitet-, miljø, og sikkerhetsansvar. Inkludert i dette ligger det en grensegang mot security, hvor ansvaret deles mellom de to informantene som representerer organisasjonen i oppgaven. Den andre informanten fra dette selskapet er ansvarlig for å følge opp alle securityleveranser i selskapet, og har en lederstilling opp mot security.

I tillegg til de to informantene fra FM-selskapet, er det valgt tre security-eksperter fra sikkerhetskonsulentfirmaet Safetec, som begge har bakgrunn fra forsvaret. Fra samme selskap har jeg også intervjuet en leder med bred kjennskap og kompetanse innen sikkerhetskultur, med bakgrunn i luftfart, jernbane og maritim.

3.3.2 Intervju

Et intervju er en samtale med et formål (Ringdal, 2001). Når vi gjennomfører intervjuer med mennesker, gjør vi det for å få innblikk i menneskelige opplevelser fra deres eget ståsted (Brinkmann & Tangaard, 2012). Intervjuet gir oss således en privilegert tilgang til informantenes livsverden, deres meninger, oppfattelse og opplevelse av den. Hensikten med intervjuene, var å få et innblikk i hvordan informantene mener og opplever at kultur har betydning for security-arbeidet, samt hvilken oppfatning de har av hvordan security-mål kommuniseres og praktiseres i ulike deler av vårt samfunn. Målet var videre å komme så tett som mulig på informantenes forståelse for siden å formulere et koherent og teoretisk velinformert tredjepersonperspektiv på fenomenet, som siden presenteres i tekstlig format (Brinkman & Tanggaard, 2012).

Kvale og Brinkmann peker på at det i forskningsintervjuet foregår en kunnskapsproduksjon i samspillet mellom den som intervjuer og informanten (Kvale & Brinkmannn, 2012). For å legge til rette for et slikt samspill, anså jeg det som hensiktsmessig å ha en semi-struktur i alle intervjuene. Dette var særlig ønsket da fagfeltet som er tema for undersøkelsen er nokså nytt og umodent, og at det derfor var nyttig med en åpen tilnærming i intervjuene. Det var likevel en trygghet for meg å kunne benytte intervjuguidene som en slags mal og "kompass" for intervjuene, særlig dersom jeg så det nødvendig å peile inn informanten på riktig spor igjen. Imidlertid var det ofte viktig å følge opp og lytte til historier som informantene fortalte om, da det kom fram interessant informasjon. Det kunne gjerne se ut til at personen hadde pratet seg litt bort, men etter hvert landet informanten interessante poeng ved hjelp av historier, som gjorde at de selv kom inn på noe av det som jeg hadde tenkt å ta opp. Dette overrasket meg som intervjuer, og viser at informantene har forstått og reflektert rundt temaet og hva jeg som forsker er ute etter. Om et slikt fenomen skriver Brinkmann og Tanggaard:

> "Den konkrete interaksjonen med intervjupersonen kan nettopp kreve at man forfølger fortellingen som intervjupersonen er mest opptatt av å fortelle. Ofte kan det faktisk vise seg at man ved å lytte til intervjupersonen og skubbe sine egne prefabrikkerte spørsmål litt i bakgrunnen allikevel kommer til de oppsatte temaene. (Brinkmann & Tanggaard, 2012, s. 28).

Alle intervjuene startet med relativt åpne spørsmål. Dette ble valgt for å få informantene til å snakke seg litt varme på noe som kunne føles overkommelig, og således legge til rette for mestring og oversikt over temaet som sådan. Gjennom intervjuet kom jeg med

oppfølgingsspørsmål hvor dette ble vurdert som hensiktsmessig, i tillegg kan det tenkes at informantene da også fikk en opplevelse om at jeg var opptatt av hva de hadde å si. Intervjuene ble tatt opp med lydbånd, og transkribert anonymt like etterpå. Jeg opplevde det som særlig nyttig å transkribere intervjuet raskest mulig etterpå, helst samme dag, slik at jeg fremdeles hadde en følelse av stemningen i rommet. I tillegg gjorde dette at jeg ikke satt på sensitive bedrifts- og personopplysninger lenger enn strengt tatt nødvendig.

3.4 Metodiske betraktninger og utfordringer

I det følgende ønsker jeg å kaste lys på ulike utfordringer og begrensninger jeg har møtt på, samt ulike vurderinger jeg har gjort i arbeidet med oppgaven.

3.4.1 Etiske vurderinger

Konfidensialitet i forskningen går ut på at private data som identifiserer deltakere og organisasjonen som studeres, ikke avsløres (Kvale & Brinkmann, 2012). Dette har jeg i undersøkelsen ansett som svært viktig, og har også derfor anonymisert alle persondata. Spørreundersøkelsen har pseudonymiserte data. Dybdeintervjuene ble tatt opp elektronisk, anonymt transkribert like etterpå og deretter ble lydopptakene slettet slik at dette ikke er sporbart. Det er derfor blitt vurdert å ikke melde inn prosjektet til Norsk senter for forskningsdata.

3.4.2 Safetec

Det har vært viktig å være klar over at Safetec har sin agenda i møte med meg som masterstudent. Som en bedrift som tilbyr tjenester innen risikostyring og risikobasert beslutningsstøtte, kan det tenkes at Safetec ønsker dokumentasjon rundt hvorvidt security-kultur kan måles, eventuelt viktigheten av kultur i sikkerhetsøyemed. Dette har vært en av de viktigste betraktningene hva gjelder samarbeidet med Safetec.

3.4.3 FM-selskapet

Virksomheten som har vært gjenstand for studien, er et Facility Management-selskap som i stor grad arbeider ute hos kunder, med mer eller mindre store selskap. Det kan dermed tenkes at en slik spredt arbeidslokalisasjon også gjør kulturdimensjonen mer kompleks og utfordrende å kartlegge hos et FM-selskap. Likevel gjennomgår de ansatte opplæring og oppfølging i FM-selskapet, og er en del av en felles virksomhet med en tilhørende kultur. Da

selskapet fremstår som dynamisk og flerdimensjonalt er det følgelig spennende å se nærmere på security-kulturen i XX. Det skal også sies at studien er en undersøkelse av ett spesifikt selskap, og funnene kan dermed ikke generaliseres til å gjelde flere selskap.

3.4.4 Hva kunne vært gjort annerledes?

Det kan tenkes at oppgaven gjerne kunne vært styrket dersom jeg selv var mer involvert i arbeidet med spørreundersøkelsen, samt prosessen rundt den primære datainnsamlingen. Dette kunne i større grad bidratt til enda større innsikt rundt intended/done-indeksen. Dog har dette vanskelig latt seg gjøre, da denne prosessen skjedde før arbeidet med masteroppgaven startet.

Det kan godt tenkes at jeg burde hatt flere informanter som del av den kvalitative fremgangsmåten, da dette gjerne kunne fått fram flere nyanser i temaet mitt. Dersom jeg skulle utvidet det kvalitative utvalget, kunne det følgelig vært hensiktsmessig med en informant fra FM-selskapet som arbeidet på et operativt nivå ute blant kunder og var bruker av security-tiltak og den faktiske praksis. Det kunne således vært nyttig å sett hvilken oppfatning en slik ansatt har av hvordan intensjoner rundt security har blitt kommunisert, og hvorvidt det er en bevissthet hos denne personen vedrørende security. Likevel vurderes det, med hensyn til begrenset tid og samtidig anvendelse av kvantitativ metode, at de opprinnelige informantene er tilstrekkelig for oppgavens formål.

4. Empiri

I det følgende vil det først presenteres resultater fra den kvantitative delen av undersøkelsen, hvor jeg viser hvilken statistisk sammenheng det er mellom intensjoner og praksis for security. Etter en gjennomgang av dette, blir det presentert funn fra dybdeintervjuene som er foretatt.

4.1 Statistiske resultat

I denne delen av empirien vil jeg vise til de resultatene som har framkommet av den kvantitative tilnærmingen. Det presenteres frekvenser av utvalget, reliabilitetsanalyse, signifikanstest, samt en korrelasjonsanalyse av datamaterialet.

4.1.1 Frekvenser

Nettoutvalget består av 878 respondenter. Kvinner utgjør 57,2 % av utvalget, mens et mindretall på 42,8 % er menn. Videre har flertallet i undersøkelsen norsk nasjonalitet (87 %), mens Polen og Sverige utgjør henholdsvis 2,5 % og 1,7 % av utvalget. Resten er godt spredt.

4.1.2 Reliabilitetsanalyse

Det sammensatte målet for «security work as intended», er satt sammen av fire elementer (α = 0,705), det sammensatte målet for «security work as done» er satt sammen av fire elementer (α =0,832). Videre består det sammensatte målet for «safety work as intended» av tre elementer (α = 0,765) og endelig er det sammensatte målet for «safety work as done» bestående av sju elementer (α = 0,691.)

4.1.3 Signifikanstest av gjennomsnitt

For å undersøke hvorvidt det foreligger en sammenheng mellom intensjoner og praksis for security, har jeg gjennomført en to-halet paired samples t-test der security (intended og done) og safety (indended og done) er henholdsvis to par med to utvalg hver.

Nullhypotesen for undersøkelsen er at det ikke vil være noen forskjell mellom intensjoner og praksis for organisasjonens security-kultur. Den alternative hypotesen er at det foreligger en forskjell mellom de to, i retning av at praksis er høyere enn intensjon.

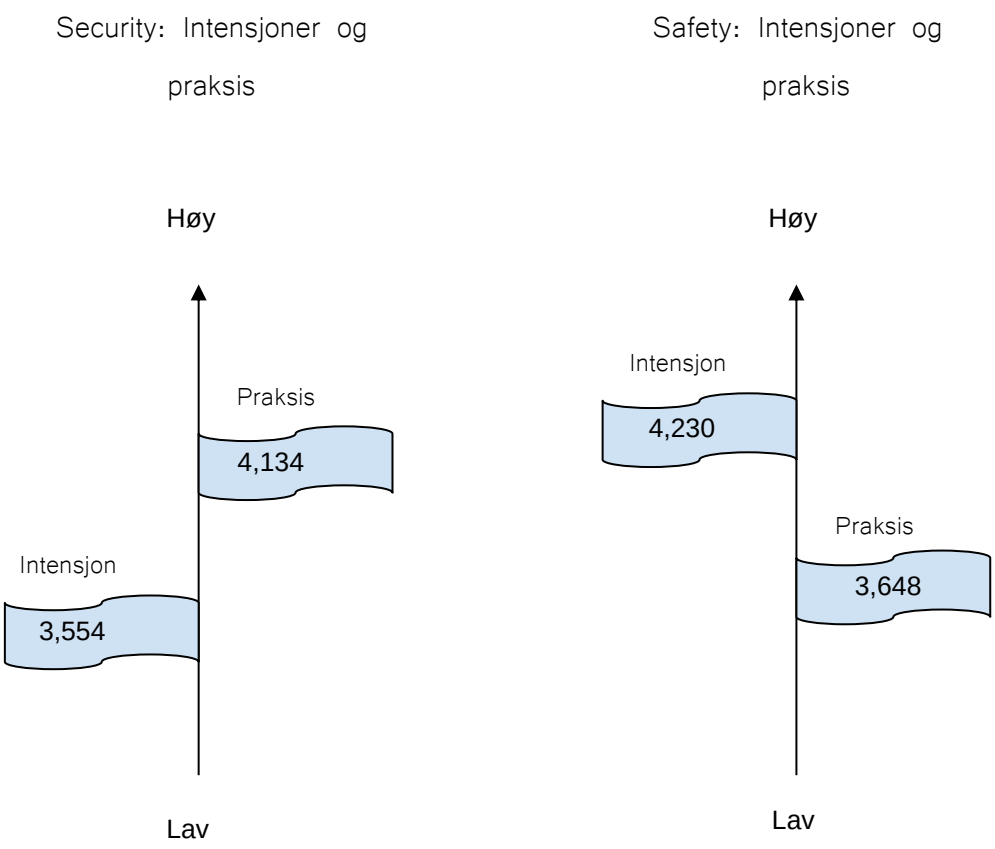
H_0 = ingen forskjell H_1 = forskjell

Paired samples statistics i SPSS viser gjennomsnitt og standardavvik for hver av de sammensatte målene. Her benyttes listwise missing method, da respondentene må ha besvart begge de sammensatte mål innen hvert par. N er derfor noe annerledes enn det totalet nettoutvalget. Paired t-test kan kun benytte variabler som har *non-missing values* for begge de parrede målene. Grunnen for at det er noen verdier som mangler (som ikke har besvart begge mål), er at de som har svart "vet ikke" er kodet bort.

		Mean	**N**	**Std. Deviation**	**Cronbachs alfa**
Par 1	Security work as intended	3,5543	756	,75724	,705
	Security work as done	4,1337	756	,97905	,832
Par 2	Safety work as intended	4,2297	836	,74737	,765
	Safety work as done	3,6476	836	,69796	0,691

Tabell 6: Paired Samples Statistics. Bearbeidet etter output fra SPSS.

Det er en signifikant forskjell i score for security work as intended (M=3,554, SD=0,757) og security work as done (M=4,134), SD=0,979). Det er videre en signifikant forskjell i score for safety work as intended (M=4,230 SD=0,747) og safety work as done (M=3,648 SD=0,698). Dette viser at det er en bedre praksis på security i organisasjon XX, enn det som blir kommunisert ut av visjoner, verdier og strategiske målsetninger. Safety viser motsatt tendens, nemlig at intensjoner og "fest-taler" har høyere score enn den faktiske etterlevelsen. Disse resultatene er illustrert i figuren på neste side.



Figur 7: Score for praksis og intensjon for henholdsvis security og safety.

	Par	**St.d**	**T**	**df**	**Sig. (2-tailed)**
Par 1	Security work as intended & Security work as done	1,23405	12,91	755	,000
Par 2	Safety work as intended & Safety work as done	,82996	20,28	835	,000

Tabell 7: Paired Samples T-test

Med et konfidensintervall på 95 % og et signifikansnivå på 5 % ($\alpha = 0{,}05$), ser vi at $p < .05$, og differansen mellom intensjon og praksis på security er forskjellig fra null. Nullhypotesen forkastes. Også på safety er $p < .05$, og differansen mellom intensjon og praksis på safety er forskjellig fra null. Nullhypotesen forkastes. Den alternative hypotesen beholdes.

4.1.4 Korrelasjonstabell

Det er utført en bivariat korrelasjonsanalyse for å se om det er samsvar mellom de sammensatte målene.

		Security work as intended	Security work as done	Safety work as intended	Safety work as done
Security work as intended	Pearson Correlation	1	,006	,411**	,238**
Security work as done	Pearson Correlation	,006	1	,147**	,373**
Safety work as intended	Pearson Correlation	,411**	,147**	1	,342**
Safety work as done	Pearson Correlation	,238**	,373**	342**	1

Tabell 8: Korrelasjonstabell av de fire sammensatte mål.

Det er ingen samvarians mellom «security work as done», og «security work as intended» ($r = 0{,}006$, $p = 0{,}886$), dvs. forholdet mellom variablene er ikke signifikant. De resterende korrelerte mål gir en positiv korrelasjon ($p < ,001$) som er signifikant men dog med relativt svake sammenhenger.

4.2 Kvalitative funn

I det følgende vil det presenteres data som er samlet inn gjennom dybdeintervjuer med fem informanter. Dette legges fram og struktureres ut fra forskningsspørsmålene.

4.2.1 Hvorfor har organisasjonen en bedre security-praksis enn bedriftens intensjoner om dette?

4.2.1.1 Security: en "blindspot"

Det kommer fram i de statistiske resultatene ovenfor, at respondentene fra spørreundersøkelsen gir en høyere score på de spørsmål som er kodet som "done", enn dem som er kodet som «intended» på security. Dette uttrykker følgelig at det er bedre etterlevelse hva gjelder security, enn det som uttrykkes av securitymål og visjoner innad i organisasjonen XX. En representant fra organisasjonen som har et HMS-, kvalitets- og styringsansvar har følgende svar på spørsmålet om hva vedkommende mener er sammenhengen på det som kommuniseres ut og det som gjøres:

> *Hvis vi tar det som snakkes ut, så er det mindre som snakkes ut enn etterlevelsen. Og det viser jo også undersøkelsen. Fordi at man er hos kundene, og kundene informerer våre medarbeidere og stiller krav lokalt. Og derfor vil praksisen være bedre enn intensjonen som er kommunisert ut.*

Videre sier informanten at organisasjonen lagde et statement sentralt i fjor, om å bli det FM-selskapet som har best intern security-kultur. Imidlertid er dette en visjon som ikke har blitt kommunisert ut i særlig grad. Informanten fortsetter:

> *(…) så godkjente ledergruppa den, men så har vi ikke fått gjort så veldig mye mer på den interne biten etterpå da. Har fokusert på å få security-leveransene først skikkelig opp på beina. Så det har aldri vært kommunisert skikkelig ut nei, ikke i nærheten på samme måte som vi har en policy på HMS, hvor vi har kurs og opplæring og alt sånt. Statement´en er ikke kjent for alle, det kan jeg garantere at den ikke er.*

Man har altså ikke begynt å systematisk arbeide mot en kulturbygging på security hos XX. Vedkommende mener at dette nok kommer på plass, men at problemet er at safety kommer foran security. «Vi har 95 % fokus på safety, og resten på security, kanskje», sier personen. I

den kvantitative analysen ser vi tydelig at fokuset og kommunikasjon (intensjon) rundt HMS er høyere enn tilsvarende på security.[1] For å forklare hvorfor, sier informanten videre:

> *(...) vi må på en måte ha en veldig høy intensjon på safety, for vi kan ikke akseptere at folk skader seg. Men det er vanskelig å få folk til å etterleve alle sikkerhetsrutiner og prosedyrer. Og det tror jeg er grunnen til at det er et gap der mellom intensjon og praksis.*

Vedkommende sier at den største security-trusselen, sett fra deres synspunkt, handler om at XX kan brukes for å nå mål hos kundene. Informanten sier:

> *Det er høyst sannsynlig at noen kan ha lyst til å gjøre det – i den grad et angrep er sannsynlig da. Men så er jo det en fin vei inn. (...) Så er det mange påvirkbare ressurser, og vi har veldig mange ressurser hos oss med tilgang til kundens anlegg (...) Pluss at vi har veldig mye informasjon, vi har all informasjon om eiendommene til mange av kundene våre. Hvis jeg vil ta den eiendommen, så ville jeg fort kunne tenke på oss som et svakt ledd, og finne informasjon om anlegget via oss i stedet for via målet.*

Det uttrykkes av samme person at security har vært en blindspot, og ikke vært noe fokus i virksomheten der man har betraktet det som et viktig fagområde. Vedkommende utdyper:

> *Vi har så mye å jobbe med innen safety, at vi ikke har kommet ordentlig i gang med security. Også er jo dette en split mellom han som leder tjenesteansvaret på security, og fagdimenjonen security, og jeg som har kvalitet, HMS og styring.*

4.2.1.2 Nytt domene

Informanten med et HMS- og kvalitetsansvar fra XX sier følgelig at de ikke har fått satt seg ned og pratet skikkelig om security-dimensjonen, da det har vært såpass store avvik på safety-biten. Vedkommende sier: "(...) og det må vi ta tak i først for det er på en måte sånn `license to operate´ i større grad". Informanten peker også på at security er et umodent felt. Det vises

[1] Se figur 6, s. 29

til at security ligger der hvor safety var før. Da vedkommende startet i XX i 2013, da var det ingen som snakket om HMS. Informanten sier:

> *Da var intensjonen dårligere enn praksisen, for folk gikk jo ikke helt hazardspill med eget liv. Folk sikret seg og folk tok jo valg, og gjorde jo riktige ting. Så jeg tror egentlig det er ganske likt det vi ser på sikring i dag. Og den undersøkelsen vi gjorde da viste at man identifiserte ikke ting som safety. Så selv om man var forsiktig når man gikk opp en stige, så snakket man ikke om det som safety eller sikkerhetstiltak. Det var bare sunt vett, det var bare sånn man gjorde jobben sin.*

Security er således et nytt felt, og informanten sier at man følgelig ser den samme tendensen på security i dag som man gjorde på safety tidligere. Man benytter adgangskortet, og da slipper man kun seg selv inn. Imidlertid snakker ikke folk om dette som security eller security-tiltak. "Du hiver det ikke i en boks. Og det er jo en del av den bevisstgjøringen og opplæringen, den handler jo bare om å putte det i rett boks", sier informanten med kvalitet- og hms-ansvar i XX.

En informant fra samme selskap med et ansvar for security, tror også at intensjonene og det som blir kommunisert ut av security-strategier scorer lavt på grunn av at det både er et nytt begrep å anvende for folk flest, og i tillegg ikke er blitt satt særlig fokus på i virksomheten. Informanten sier:

> *Safety-scoren kan jeg nok tenke meg at forklares med at vi har høye ambisjoner og høye mål når det gjelder HMS-arbeidet. Det samme er ikke tilfelle for security, det er et veldig nytt begrep og er kanskje ikke så tydelig som det HMS-kravet.*

Vedkommende sier at det som blir viktig å gjøre, er å løfte intensjonen, og å være tydelige på å kommunisere hvorfor security-kultur er viktig. Vedkommende sier:

> *Hvorfor skal vi ha sikring? Hvorfor skal sikring være en del av vår totale leveranse? Så vil det også kanskje sørge for at vi lager det gapet mindre, og da når man kanskje det målet.(…) Her handler det mest om å kommunisere seg opp for å bygge den kulturen, så når du det nivået. Så gjelder det å løfte begge med tiltak.*

Informanten med hms- og kvalitetsansvar sier også at dersom vi ser på visjonen om security, så er denne høy isolert sett. Men den er ikke forankret i hele virksomheten. Vedkommende tar en pause og fortsetter:

> *(...) hvis vi ser på ledelsen engasjement i dette...veldig lav, per i dag. Det kan nok endres over tid. Men det er ikke en skikkelig forståelse enda. Det er ikke det altså. Det mangler forståelse og kunnskap. Og kapasitet.*

4.2.1.3 Tydelighet

Informanten forteller at det er så mye å gjøre innen risikostyring, compliance (etterlevelse) og sier at "(...) og det er en av grunnene til at, selv om det er mitt fag, at jeg har latt det ligge og ikke har mast så mye om det, for vi må få orden på safety hele veien først". På spørsmål om vedkommende tror at prioriteringen mellom safety og security kan handle om hva som er mest "synlig" og forståelig, sier informanten at safety er mye tydeligere og konsekvensene er mer synlige. Personen spesifiserer ytterligere: "Sykemelding, fravær - statistikken blir veldig tydelig. Så en av de tingene vi nå skal gjøre, er å få inn sikring som egen kategori i avvikssystemet igjen." Det var tidligere en del av avvikstallene, men sier at de tok dette ut da "ingen forsto hva det var, så de brukte det til alt mulig rart". Nå mener informanten at tiden er moden for å bygge mer bevissthet rundt security, og å bygge en kultur rundt dette. Vedkommende fortsetter:

> *Også tror jeg at ved å styrke sikringsleveransene våre - vi leverer jo, med underleverandører, mye vektertjenester, vakt og sikring, alarmsystemer og sånt - det er også med på å bygge forståelse og kultur, at vi har fagmiljøer som kan dette. Vi har en lang, lang vei å gå på sikring. Min erfaring som konsulent er at det er ikke bare her.*

På den andre siden sier informanten fra XX som arbeider med security at man møter security-barrierene mer tydelig og fysisk, særlig i forbindelse med fysisk tilgang til bygg og eiendommer Vedkommende sier:

> *Du må bruke kortet ditt for å gå gjennom døra. Du må ikke holde deg i gelenderet når du går ned en trapp. Det må en aktiv tanke til. (...) Så praksisen oppleves hele tiden,*

for den er så mye mer fysisk. Mens HMS-fokuset ligger mye mer på alt det du skal huske på å gjøre for ikke å skade deg. Dt er mer ullent da. Derfor tror jeg forskjellen er akkurat der rett og slett.

Informanten som arbeider med security legger også vekt på at innenfor XX eier de HMS-tiltaket, men på security, så er det for det meste kunden som eier tiltakene. Vedkommende sier:

Det er kunden som eier systemet som vi bruker kortet for å komme gjennom, vi blir tildelt kortet for å kunne bruke kundens eiendom. Mens når vi går inn til kunden og begynner å vaske, så er det vårt HMS-arbeid i vårt hode og i vår kropp som avgjør hvor flinke vi er til å bruke sunn fornuft (...) Mens security-delen gir seg litt selv, for du må gjennom den døra som er låst, og da må du bruke kortet.

4.2.2 Hvordan forstås begrepet security-kultur, og i hvilken grad kan det kartlegges?

4.2.2.1 Helhetlig tilnærming

Det kommer frem blant flere av informantene, at security-kultur handler om den samlede kunnskap, forståelse og atferd som man har rundt security. I tillegg er det en tendens, særlig blant informantene fra Safetec, at security-kultur forstås som en av flere søyler innad i en organisasjons helhetlige kultur. En security-ekspert fra Safetec sier at du ikke kan se securitykultur som noe på siden av organisasjonens safety-kultur, eller helhetlige organisasjonskultur. Det er noe som er integrert i den helhetlige organisasjonens "ryggmarg":

Når du tenker sånn på det, så er sikkerhetskultur noe du har på toppen, så har du safety og security innunder som to pilarer innenfor den store, hvis du skal ta med alle aspektene i det. Du kan godt skille det når du skal snakke om det og lære noen om det, men som organisasjon så mener jeg at man bør tenke sikkerhetskultur. Men det er gjerne enkeltpersoner som tenker mer security og andre tenker mer safety...men sammen skal det bli en kultur. For har du en sikringskultur bare for seg selv, så blir det for en sånn showstoppere..., det er jo ikke der vi ønsker å være, vi ønsker å skape et mulighetsrom.

En annen security-ekspert i Safetec, har samme oppfatning. Denne informanten har følgelig en forståelse av at security-kultur deler en del av de samme egenskapene som safety-kultur som sådan. Vedkommende sier:

> *Men summa sumarum da, hvis man snakker om sikkerhetskultur eller sikringskultur, eller integrerer det for så vidt og, så prater man egentlig i stor grad om faktorer som ledelse, håndtering av målkonflikter, bygge en robust organisasjon og ikke minst styring og kompetanse for å kunne bygge det, og ha en god enten sikkerhetskultur eller sikringskultur , alt ettersom da.*

På spørsmål om hva en leder i Safetec, legger i begrepet security-kultur, sier vedkommende at det forstås slik at man bytter ut begrepet safety med security. Personen sier:

> *Jeg er åpen og på jakt etter hva som eventuelt er annerledes i sikringskulturbegrepet. Men vi jobber ut i fra en antakelse om at kultur som sådan.... Sikkerhetskultur er ikke noe annet enn den delen av organisasjonskulturen som virker inn på sikkerhet, og følgelig så tenker jeg at sikringskultur er den delen av organisasjonskulturen som virker inn på sikring.*

Når vi fortsetter å gå inn på fenomenet security-kultur, og innholdet i dette, peker samme informant på at security-kultur, slik personen forstår dette, er knyttet opp mot de temaene, de ni faktorene som benyttes når de går ut i selskaper og organisasjoner og snakker med folk, og som ligger til grunn i spørreundersøkelsene. Vedkommende peker på at representantene fra selskapene undrer seg hele tida når de spør om disse ganske spesifikke temaene. Informanten sier dette om hva som ligger i kulturbegrepet i en organisasjons arbeid med sikkerhet:

> *Det er sånn som company vision, på engelsk. Hva sier organisasjonen om sikkerhet og sikring, hva er visjonene, hva er policy´en, hva sier lederen på møter og samlinger? Og ikke minst hva gjør de i praksis - stemmer det med det de faktisk gjør? En sånn walk-the-talk-indeks.*

4.2.2.2 Kulturkartlegging

Vedkommende peker på at alle organisasjoner har en kultur, at det ikke finnes en egen sikkerhetskultur som ligger i en skuff eller "borti der et sted". Det samme gjelder for security, ifølge informanten. Vedkommende uttrykker usikkerhet i forbindelse med hvorvidt temaene og normene som Safetec benytter for å kartlegge sikkerhetskultur, også er dekkende for security-kultur:

> (...) *når vi operasjonaliserer kulturbegrepet, for det gjør vi jo, når vi går ut og jobber med sikkerhetskultur, så jobber vi med noen helt konkrete temaer. Vi har en norm som vi sier at "dette er dit organisasjoner vil". Om de er dekkende for sikringskultur, det er jeg ikke sikker på. Det er rett og slett fordi jeg ikke vet det...jeg synes det er et spennende spørsmål".*

På spørsmål om hvorvidt kultur kan kartlegges og måles, sier vedkommende videre:

> *Jeg tenker at det å måle kultur utelukkende ved bruk av spørreskjema - det går ikke. Du må ut og snakke med folk. Og det er ikke bare noe jeg mener, det er godt beskrevet i artikler og bøker også det… Jeg har et veldig godt eksempel fra den første kulturkartleggingen vi gjorde for jernbaneverket i 2010, det er en offentlig rapport, så det er ikke noe hemmelig. Der svarte jo jernbaneverket på alle de spørsmålene i spørreskjemaet som inneholdt ordet sikkerhet - så svarte de "vi er best i verden".*

Lederen i Safetec forteller at de svarte veldig annerledes på de spørsmålene som ikke hadde "sikkerhet" i formuleringene, men som for øvrig handlet om det samme. Det var en veldig markant forskjell, ifølge vedkommende, som sier videre at de i intervjuene framsto som en organisasjon som hadde et veldig statisk sikkerhetsbegrep. "Vi er sikre", hadde jernbaneverket uttrykket. Informanten hadde spurt hvordan, med påfølgende svar om at det forelå så mye prosedyrer og de hadde så fin teknologi, så dette var det orden på.

> *Så gikk det to minutter inn i intervjuene, og så begynte de å fortelle om alle de prosedyrene de ikke kunne følge, og om teknologien som sviktet. Så de forklarte det veldig godt selv. Hvorfor svarer de best i verden når det står sikkerhet i spørsmålet - det er fordi de er hjernevaska, sa de. "Vi er så vant til å høre at vi er flinke på sikkerhet, vi tenker oss ikke om, vi bare sier `yes´".*

Videre forteller vedkommende at når spørsmålene ikke inneholdt sikkerhet, stoppet de opp, tenkte seg om og svarte helt annerledes. Informanten sier følgelig at dette var snakk om en organisasjon som tenkte og trodde som en helt fundamental organisatorisk antakelse at de var helt sikre. Det var noe som man fikk fortalt. Vedkommende forteller videre:

> *Men når du bryter det ned, så rakner det fullstendig. Sånn som NN, en kollega som nå er i SINTEF sa, at vi forutså jo Alnabru-ulykka i den ene rapporten der. Den skjedde forøvrig mens vi jobbet med dette. Så… du kan ikke måle kultur med spørreskjema alene, du må snakke med folk.*

På spørsmål om det er en god ide å forsøke å måle security-kultur, sier den ene security-eksperten fra Safetec at dette kan være gunstig for å se hvorvidt man går i riktig retning. Vedkommende sier at man på et eller annet vis må måle kulturen for å få en pekepinn på hvordan det ligger an. Den andre security-eksperten er noe mer forbeholden når det gjelder å skulle måle kulturen. Informanten sier:

> *"Samtidig er jeg litt usikker på i hvor stor grad alt lar seg måle da. Vi må jo passe på at det ikke bare er de målbare tingene som blir viktig (...) Jeg er litt opptatt av at man ikke må sette en tallkode eller måleparameter på absolutt alt. Man må innse at ikke absolutt alt er målbart.*

4.2.3 Hva kan security-kultur-begrepet gi oss?

I det følgende vil det presenteres empirisk materiale som omhandler informantenes oppfatning og deres opplevelser om hvorfor security-kultur er relevant i en security-kontekst. Det blir særlig vektlagt hvilke utfordringer som foreligger når det gjelder arbeid med security, og som således danner grunnlaget for en diskusjon omkring behovet for et security-kultur-begrep.

4.2.3.1 Begrepsbruk

Det kommer blant samtlige informanter fram at det er behov for et kulturbegrep i relasjon til security og relaterte sikkerhetstiltak. Enkelte av informantene mener det handler om en

modenhet, og at det er en prosess hvor man må erverve forståelse av hvorfor dette er viktig. Det kommer også fram at det er behov for et eget begrep for å favne om de utfordringene som finnes i forhold til tilsiktede hendelser. En av security-ekspertene i Safetec, med bakgrunn fra Forsvaret mener at det handler om å bygge opp en innsikt og forståelse om mulige trusselaktører, både på makronivå i samfunnet, men også i organisasjoner. Det handler ifølge informanten om å ta inn over seg og studere trusselbildet som endrer seg og er dynamisk, skape en forståelse over hva som rører seg.

Også security-ansvarlig i XX sier at det er behov for begrepet security-kultur, og at dette er viktig å benytte for å ikke bare falle ned mot sikkerhet og safety, men at security er en del av det totale kulturbildet. Vedkommende sier:

> *Jeg tror det er litt misforstått, fordi veldig mange oppfatter at når du snakker om sikkerhet, så definerer du også security inn under sikkerhet, men sikkerhet i veldig mange sammenhenger er knyttet til hms-begrepet og safety. Og der er det litt av det engelske ordbruket kommer inn i bildet, med safety og security hvor det er et mye tydeligere skille enn det er i Norge hvor man har puttet alt inn i sikkerhetsbegrepet. Også har man ikke vært tydelige på hvordan man definerer det sikkerhetsbegrepet da.*

Også den andre informanten fra FM-selskapet XX, med styring, kvalitets- og HMS-ansvar, sier at det er et stort behov for å skille mellom safety- og security-kultur, i den grad man må skille mellom villet og ikke villet, da det er stor forskjell på hvordan man tenker om og beskytter seg mot at uhell skjer og at noen kan utrette skade.

Security-ansvarlig i XX peker også på at dersom man snakker om en sikkerhetskultur, vil det være avhengig av mottakeren og hva denne mottakeren forstår sikkerhetskultur som. Vedkommende sier:

> *Hvis du er hos en kunde som har et veldig tydelig skille på sikkerhet og sikring, så vil de forstå begrepet sikkerhetskultur som safety. Mens en kunde som ikke har den samme oppfatningen vil forstå sikkerhetskultur som noe som også inneholder sikringskulturen. Så, igjen, det er veldig avhengig av mottakeren, og derfor så har vi tenkt at det er viktigere for oss å være tydeligere på å skille mellom sikkerhetskultur og sikringskultur.*

Informanten sier videre at i det øyeblikket man skiller slik på begrepene, så skaper de også et spørsmål om hva som er security-kultur og hva som er safety-kultur. "Hvis du bare sier at du skal ha en sikkerhetskultur, og du tenker at sikringsbegrepet ligger inni der, så vannes det veldig mye mer ut", sier vedkommende. Informanten viser til at de tar det ene begrepet, legger det på siden og kaller det noe eget, for slik å tydeliggjøre dette skillet mellom safety og security. Vedkommende eksemplifiserer:

> *En renholder, for eksempel, som vi tenker har en sikkerhetskultur, er jo opptatt av at han ikke skal skade seg på jobb og han skal ivareta safety-biten. Det går jo veldig mye på at du ikke skal skade deg selv. Men hvis vi da også løfter inn sikringskultur, så betyr det at den personen som da jobber hos en kunde, som har sikringskulturen inne også, den personen har fått opplæring i at når han eller hun går inn en dør, og det kommer en inn etter deg i den døren, så skal din ryggmargsrefleks være at her må du snu deg og spørre "hvorfor går du inn etter meg, uten å bruke kortet ditt?" Da har du en sikringskultur med deg.*

4.2.3.2 Integrert forståelse

På spørsmål om hvorvidt det kan være utfordrende å benytte kulturbegrepet i en security-sammenheng, forteller den ene security-eksperten fra Safetec at det kan være problemer i en begynnende fase, før man får tydeliggjort hva man mener og hva man bør gjøre. Vedkommende sier:

> *Hvis jeg bruker et eksempel fra Forsvaret, så har vi jo et direktiv som sier noe om "hvor langt du kan tøye strikken"...altså, du må forholde deg innenfor en del barrierer når du skal øve, uten at du skyter hverandre og sånne ting, så har du en del sikkerhetsvinkler som du må forholde deg innenfor. Mange ser på det som en begrensning, mens det det handler om i stor grad er jo å finne det mulighetsrommet det gir deg da.*

Begge security-ekspertene med bakgrunn i Forsvaret peker på at man må tenke helhet og integrert forståelse, hvor security-kultur må være en av søylene for å holde "slottet oppe",

som del av den totale bedriftskulturen. Det må være gjennomsyret fra en avdeling til det overordnede nivå. Den ene av de to security-ekspertene fra Safetec, sier:

> *I kulturbegrepet ligger det mye verdier og holdninger (...) du må ha en helhetlig tanke, og du må vite at mennesket er en risikofaktorer i seg selv. Når du putter inn en minnepenn i feil maskin, så gikk det en rød lampe, så fikk du straks en telefon om at det må du slutte med eller legge maskinen på rens, holdt jeg på å si. Du må ha noen sånne typer barrierer i tillegg, det må være en helhetlig tanke og ikke bare være opp til den enkelte.*

Begge to holder fast på at organisasjonens medlemmer som sådan må operasjonalisere visjoner på security i det daglige "sånn at det ikke er valgfag hos den enkelte ansatte", som den ene sier. Det skal inkorporeres og skape forutsigbarhet. Det poengteres av samme informant at for å få til en god praksis, og innarbeide og etterleve en god security-kultur, er det viktig å ha klare føringer og standarder på hvordan man skal håndtere ulike system. Vedkommende sier:

> *Du må ha rutinebeskrivelser på hvordan man for eksempel bruker systemer. Det må være atferdskontrollerte måter å gjøre ting på. (...) Du må redusere usikkerheten blant alle ansatte i den daglige driften da, for å kunne ta bort elementet menneskelig feil.*

Flere av informantene snakker om ord som samarbeid, informasjonsflyt og en holistisk tilnærming til arbeidet med security. Informanten som arbeider med security-leveranser i XX sier at det viktigste med å etterstrebe en security-kultur er å få en forståelse for "hvorfor". Vedkommende sier:

> *Hvorfor ønsker vi å ha en sikringskultur, hvorfor skal jeg bry meg om sikring? Det handler jo litt om din egen sikring, og det handler om forståelsen av hva vi leverer til en kunde. Og ikke minst at den sikringskulturen vi bygger i selskapet, det er en "added value" til vår kunde. Hvis de forstår at det er en added value som de kan tilføre kunden, så er jo de med på å løfte hele selskapet. Det er en viktig grunnpilar.*

4.2.3.3 Kreativt bekymret

Lederen fra Safetec snakker om at risikobevissthet er sentralt. Vedkommende bruker begrepet "kreativt bekymret" for å vise til at du skal ha følere ute for at noe kan skje. Informanten sier:

> *Hvis du har jobbet på et lite prosessanlegg hele din karriere i 25 år, det er et lite anlegg og det har aldri skjedd noe der. Du har ingen informasjon om ting som skjer i tilsvarende anlegg andre steder i verden, og du har aldri eksponert for noe som helst. Da vil du etter hvert komme i en situasjon hvor du tenker at «her kan det jo ikke skje noe». Og da mister du den evnen til å være kreativt bekymret. Det samme så vi hos toglederne i Banenor i den første rapporten, de trodde at det de var bekymret for, det var et utslag av individuelle svakheter (...) De trodde at det bare var de som gjorde feil, og ingen andre gjorde det. Så det er en del du skal ha tilgang på av informasjon og kunnskap for å være kreativt bekymret. Men det som av og til hevdes, er jo at det er umulig å fange opp disse såkalte svarte svanene. Ja, men det er jo ikke det som er poenget! Du vet aldri hva det er som kommer til å skje. Men du kan være bekymret for "har vi egentlig kontroll på alt". Det er veldig forskjellig. Jeg tror at en organisasjon som er passe sånn… litt sånn på vakt etter "hva er det vi ikke vet nå", "hva er det som kan dukke opp" - de vil mye fortere og mye mer effektivt fange opp en sort svane enn de som tenker "nei, du har kontroll på alt*".

4.2.3.4 Silotenkning

Ordet "forståelse" går igjen hos samtlige av informantene. Dette kommer også fram hos den ene informanten som arbeider innen security hos Safetec. Vedkommende vektlegger at det er en tendens til en slags "silotenkning" rundt security. Informanten sier:

> *Jeg syns jeg ser en tendens til at de som driver med systemer på cyber, de er veldig bevisst på akkurat det, men de er ikke så veldig bevisst innenfor fysisk sikring. De er veldig gode på sitt fagområde og klarer å sikre seg innenfor det, men så står døra vid åpen på andre siden. Det er det jeg synes man er for dårlige på i dag, man klarer ikke å se den helhetstankegangen. (...) Du må ha pilarer å stå på, hvis du står på "enern", så står jo hele slottet og balanserer. Men klarer du å dytte inn to-tre stykker, så får du en helhetlig kultur da.*

Lederen i Safetec poengterer også denne "silo-tekningen", og henviser til et pågående prosjekt som de jobber med nå, hvor informanten opplever at virksomheten er genuint opptatt av security, og vil gjerne prestere godt. "Men en del av de tingene de gjør undergraver effekten i budskapet", sier lederen. Vedkommende utdyper:

> *Det er veldig høy bevissthet på security som trussel, alle nevner det, lederne er veldig opptatt av det. De har stedvis ekstreme fysiske sikringstiltak, og en del av de samme stedene brytes prosedyrer og rutiner konsekvent hele tida.*

Informanten viser til at virksomheten har en port og et kamera på denne porten. Videre forteller informanten at den personen som har ansvar for å åpne opp porten, ikke har tilgang til å styre hvilket bilde han eller hun ser på. Vedkommende sier:

> *Så hvis det ringer på og bildet hun har på sin skjerm viser noe annet, så vet hun at det tar tredve sekunder før det kommer dit. Hva gjør du da? Jo, du bare slipper inn, hele tida. Så da har du en situasjon hvor du har en høy talk-indeks, så har du en ganske lav walk-indeks. Du har tidvis en veldig god IT-organisasjon som gjør veldig mye bra, de blant annet...sender ut sånne fishing-mail med vilje som et mål på organisasjonens evne til å fange opp og la være å trykke på, det er kjempevellykket. Også har de samtidig ulåste PC`er og sender vedlegg med mailer som man ikke burde gjøre. Og tilsvarende - de har fått en svær, ny, og fin, dyr port som står åpent stort sett hele døgnet og varetransport kan sette fra seg store paller som ingen vet hva er, utenfor døra til kontrollrommet.*

4.2.3.5 Forankret på et samfunnsnivå

På spørsmål om hvordan vi evner å ta inn over oss eventuelle security-trusler i et større perspektiv i samfunnet, svarer den ene security-eksperten fra Safetec med et eksempel om de svenske myndighetene som har sendt ut brosjyrer for krisehåndtering i tilfelle krig eller krise. Vedkommende sier at da dem intervjuet personer på dagsrevyen, virket tanken på ulike security-scenarier fjern. Informanten sier:

> *Jeg sier ikke at du skal hamstre inn masse mann og hermetikk og alt i den duren, men det virker så far fetched, at det kan skje i det hele tatt. (...) Og jeg tror ikke dette bare gjelder i samfunnet, jeg tror det også gjelder en del bedrifter.*

Den andre security-eksperten forteller at vedkommende opplever at bevisstheten om ulike trusselaktører og det som rører seg er ganske lav i samfunnet som sådan. Informanten mener at Norge er et forholdsvis naivt land, og når det er snakk om trusselnivå opplever vedkommende at det er en lav kompetanse utenfor de enkelte security-miljøer om hva som rører seg i verden og som kan ramme dem.

Også informanten med kvalitet og styringsansvar fra XX sier at personen opplever at det er en "ekstrem umodenhet" rundt security på generell basis i samfunnet. Vedkommende sier at man gjennom nedbygging av forsvarssystemer og redundans i ulike systemer forteller befolkningen at security ikke er noe viktig, for "her kan det ikke skje noe farlig", sier informanten.

> *Å være en del av et samfunn der safety er kjempeviktig, fra hvordan du bygger et hus, til jobben din, bilkjøring - alle steder er safety viktig. Security, det har på en måte falt veldig mye bort, med ett unntak kanskje, og det er flytrafikk, og der har det blitt så voldsomt at folk bare tenker "jaja, dette er jo nyttig".*

Informanten tenker at det ikke bare er et problem for selskap, men at det er forankret i samfunnet som sådan. Vedkommende presiserer imidlertid at det er store forskjeller mellom selskaper: "Vi har kunder som er på helt forskjellige planeter på security, det tror jeg også gjør det vanskelig å bygge lik kultur i XX».

Vedkommende med HMS- og kvalitetsansvar i XX sier at samfunnet er svært hendelsesstyrte, og informanten tror at vi trenger å se en større uønsket hendelse nært på oss her i Norge for at vi skal få til å bygge en bedre kultur og awareness rundt security. Vedkommende sier: "For at det virkelig skal skje noe så tror jeg nok kanskje at man må se noen mer konkrete hendelser, et angrep på et landanlegg, en stor fabrikk, store anslag på IT/Cyber (...) Informanten sier videre at det er så fjernt for så mange. Personen poengterer at man nok kan gjøre noe i forhold til bevissthet og kulturbygging, men at man ikke forstår relevansen av det før det faktisk skjer noe spesifikt. Vedkommende sier:

Samfunnet har glemt security som nødvendighet. Man har bygget ned redundans i telesystemer, og IT-infrastruktur (...) og man har bygget ned forsvar og sivilforsvar, finnes ikke tilfluktsrom lenger, ingen råd fra myndighetene om «basic ting». Det er noe galt et sted. Det er ikke et tankesett i samfunnet om redundans på sikring og beredskap. Og det tror jeg kanskje er på vei inn igjen. Men når man planlegger å legge en bussterminal oppå toget som ligger på Oslo S over t-banen, fordi det er så praktisk - det er jo dårlig samfunnssikkerhet da. Så hvordan skal vi få våre renholdere til å være opptatt av det når politikerne på Stortinget ikke er det?

5. Drøfting

I denne delen av oppgaven vil de empiriske funnene bli diskutert og belyst opp mot det teoretiske rammeverket presentert tidligere. Det vurderes som hensiktsmessig å strukturere drøftingen ut ifra hypotesen og forskningsspørsmålene. Innledningsvis vil den formulerte hypotesen, samt resultatene fra den kvantitative undersøkelsen diskuteres opp mot forskningsspørsmålet om hvorfor dette resultatet foreligger. Deretter følger jeg opp med en diskusjon om hva som ligger i security-kulturbegrepet, hvorvidt den kan kartlegges, og endelig hva security-kulturbegrepet kan gi oss i en faglig og praktisk sammenheng.

5.1 Høyere praksis enn intensjoner for security

Som del av den kvantitative tilnærmingen ble det gjennomført en reliabilitetsanalyse for å undersøke den indre konsistensen i de fire sammensatte målene «security work as intended», «security work as done», «safety work as intended» og «safety work as done». Ifølge Ringdal har en indeks en tilfredsstillende reliabilitet dersom alfa ligger over 0,7 (Ringdal, 2001). Imidlertid kan det hevdes at man kan, og bør benytte skjønn i vurderingen dersom alfa ligger tett opp mot 0,7. En svært rigid tolkning av grenseverdien på 0,7 vurderes som lite formålstjenlig. Tre av målene viser en alfa over 0,7 og anses tilfredsstillende, derimot har «safety work as done» $\alpha = 0{,}691$. Det kan argumenteres med at verdien er såpass tett opp mot 0,7 at denne kan vurderes som tilfredsstillende. En verdi mellom 0,6 og 0,7 kan man stille spørsmålstegn ved, men da alfa for «safety work as done» er såpass nært opp mot 0,7 blir det i denne sammenheng ansett som et tilfredsstillende mål på indre konsistens. De fire målene anses å ha en tilfredsstillende intern reliabilitet.

Det ble utført en Paired Samples t-test, hvor det ble funnet en signifikant forskjell i score mellom security work as intended (M=3,55) og security work as done (M=4,13). Dette viser til en høyere score for praksis av security enn det som kommuniseres ut av visjoner, strategier og målsetninger. Også for safety var det en signifikant forskjell mellom intensjon og praksis, men viste et motsatt resultat hvor intensjon og de uttalte målene om å arbeide sikkert var høyere (M=4,23) enn den faktiske etterlevelsen (M=3,65). Hypotesen som ble presentert innledningsvis i denne oppgaven, beholdes. Videre så vi av korrelasjonsanalysen at det ikke var noen statistisk sammenheng mellom intensjoner for security, og praksis for security. Dette sier oss at praksis for atferd ikke øker i korrelasjon til intensjonene for security.

5.1.1 Hvorfor er det slik?

Med det overforstående som et beskrivende utgangspunkt, valgte jeg å gå i dybden, for å få en forståelse og forklaring av hvorfor dette resultatet foreligger. Gjennom den kvalitative empirien har det kommet fram at det hos XX er satt et mål sentralt om å bli best på intern security-kultur. På tross av at en slik visjon er formulert, er ikke denne kommunisert ut hos selskapets ansatte, og security som sådan er ikke prioritert hos ledelsen i XX. Dette kan betraktes som det Arguis og Schön forstår som forfektede verdier, ettersom verdiene ikke er forankret i virksomheten. Ser man på visjonen isolert sett, er det en høy intensjon om å følge opp security, men kommunikasjon fra ledelsen og virksomheten vedrørende security, er følgelig dårlig. Dette gir utslag i en lav score på intensjon for security. Dette kan sees i lys av en manglende forståelse for hvorfor security-tiltak og security-bevissthet er viktig, og er gjerne en underliggende forklaring på hvorfor intensjonene ikke er kommunisert ut og verdsatt. Det kommer fram av empirien at security-hendelser tidligere var innlemmet i avvikssystemet, men at kategorien ble brukt til «alt mulig rart». Dette viser til en manglende forståelse og kompetanse rundt security blant de som skal benytte seg av systemet.

Safety-aspektet er høyere prioritert hos både ledelse og i virksomheten som helhet. Det kan tenkes at hendelser knyttet til uhell og skader av ulik karakter er mer synlig og håndgripelig for de fleste. Reniers et al. (2011) viser følgelig til at security representerer en risikoform av symbolsk karakter, og hvor safety-dimensjonen innehar en risiko innad i organisasjonen. Slik kan det hevdes at security er vanskeligere å favne om, og kan oppleves som mer uforståelig og mindre relevant i en virksomhets nære omgivelser. Dette kan knyttes opp mot Hofstedes begrep, mental software, hvor de mentale programmene for hvordan man unngår personlig skade og tar vare på egen helse er forankret tydeligere hos oss som mennesker, enn for eksempel teknologisk cyberangrep som følgelig angriper organisasjonen eller «noen andre». Security-hendelser kan forstås som noe mer diffust. Dette kan således være en årsaksfaktor for at det i større grad er rettet oppmerksomhet på safety-aspektet i virksomheten når det gjelder sikkerhetstiltak. Det blir trukket fram at det her foregår opplæring, kurs og klare policy' er. Således er de manifesterte verdiene, i Scheins ordelag, mye tydeligere forankret på safety-fronten.

Interessant er det at praksisen rundt safety er dårligere sammenlignet med security, selv om intensjonene er høyere ved safety. Den ene informanten fra virksomheten peker på at det *må*

være høye intensjoner på safety, da man ikke kan godta at noen skader seg på jobb. Imidlertid skjer det uhell iblant, da det er menneskelig å glemme og gjøre feil. At det foreligger en høy praksis på security-dimensjonen, utdypes av security-ansvarlig fra XX, ved at det er tydelige barrierer ute hos kundene. Selv om det ikke er høy forståelse for security-risikoer, og at det gjerne oppleves som noe fjernt, er det likevel tydelige barrierer som benyttes, slik som adgangskort. Dog varierer dette sterkt fra anlegg til anlegg. Det fremholdes at bevisstheten for security, dersom det er noen, ligger i *bruken* av for eksempel et adgangskort, og ikke nødvendigvis som mental software som ligger latent hos den som benytter det. I en situasjon hvor du går ned en trapp, er det et bevisst valg som må tas ved å holde seg i gelenderet eller ha på en hjelm. Det er ikke tilfellet ved å benytte adgangskort, dette må benyttes uansett. Dermed kan forståelsen og bevissthet rundt security være lav, selv om man benytter seg av de faktiske tiltakene. Kultur er, i tillegg til å ha et styringssystem, også en forståelse av hvorfor man gjør det man gjør. Således må du i tillegg til praksis og anvendelse av systemet, ha en forståelse av *hvorfor* du anvender systemet. Det holder ikke med en fin prosedyre, du må også leve den, og skjønne den.

5.1.2 Praksis, men ikke forståelse?

Dersom vi ser på Hofstede sine forskjellige «lag» av kultur[2], er praksis inkorporert gjennom alle lagene. Dette kan gjerne være tilfellet i de situasjonene hvor praksis har en dypere mening, og er uttrykk for kulturen. Imidlertid fremgår det av den kvalitative empirien at det ved security ikke er en forståelse av hvorfor man benytter de ulike security-tiltakene. Dermed kan security-kulturen sies å ikke være dypt forankret i det som Hofstede viser til som verdier, innerst i kjernen av kultur (Hofstede, 2010). Imidlertid skal man være forsiktig å avskrive at de ansatte i XX som arbeidet ute hos kunder, kan være påvirket og inkorporert i organisasjonskulturen hos den spesifikke kunde man arbeider hos. Denne faktoren gjør det gjerne særlig utfordrende å kartlegge kulturen hos FM-selskapet XX, da man kan være en del av flere ulike kulturer.

Ved security-dimensjonen kan det argumenteres for at det ikke er forankret en god kultur. Det foregår følgelig en praksis ettersom det eksisterer fysiske security-barrierer du må gjennom, men disse praksisene foregår hos kundene og er således ikke noe som er et resultat av delte antakelser. Dette kan holdes opp mot korrelasjonsanalysen, som viste at det ikke forelå noen

[2] Figur 3: Kulturens manifestasjon gjennom ulik dybde og nivå, s. 18 (Hofstede, 2010).

statistisk sammenheng mellom intensjoner og prakis for security. Følgelig vil ikke praksis nødvendigvis øke i sammenheng med at intensjoner øker, eller motsatt. Således ser vi at praksis dermed er noe adskilt fra intensjoner fra XX. Praksis foregår hos kundene, mens intensjonene eventuelt blir kommunisert sentralt fra FM-selskapet. Selv om praksis scorer høyt i undersøkelsen, er det således ikke en *felles* praksis, og ikke det som Schein kaller for et mønster av grunnleggende antakelser, som er delt av en gruppe og læres videre (Schein, 2010).

Det framkommer av empirien at begrepet security, eller sikring, som noen av informantene bruker, er et såpass nytt begrep å anvende, både blant folk flest, men også at det ikke er blitt satt særlig fokus på i virksomheten. Det kan hevdes at security-begrepet således er i en modningsprosess, hvor også dagens trusselbilde og samfunnsutviklingen som sådan krever nye måter å tenke sikkerhet på. Imidlertid er oppmerksomheten i XX i mye større grad rettet mot safety enn security. Det skal påpekes at safety er et viktig satsingsområde, men det som også framkommer i empirien er at kanskje den største security-risikoen er å anvende som middel for å nå mål hos kunder. Kvalitet- HMS- og styringslederen i XX sier at dette absolutt er en reell situasjon, i den grad et angrep er reelt. Det er derfor behov for en større kompetanse og bevissthet rundt det trusselbildet som finnes der ute, for å heve intensjon hos ledelse og virksomhet som sådan. En utfordring blir således å heve både intensjon og praksis, og følgelig få til en god harmoni mellom både intensjoner og etterlevelsen. Det kan tenkes at dersom intensjoner og praksis er på et noenlunde likt og høyt nivå, kan det være et uttrykk for en «god security-kultur». Imidlertid, som vi skal se, kan det tenkes at en slik kartlegging av kultur kan være problematisk.

5.2 Hvordan forstås begrepet security-kultur, og i hvilken grad kan det måles?

I det følgende ønsker jeg å diskutere hva som ligger i begrepet security-kultur, og hvordan dette inngår i arbeidet med security. I tillegg fører jeg en diskusjon rundt hvorvidt security-kultur kan kartlegges.

Det kommer fram av den kvalitative empirien, at security-kultur blir oppfattet som den samlede kunnskap, forståelse og atferd som virker inn på security-dimensjonen. Fra den empiriske gjennomgangen, kan det på mange måter synes at det foreligger oppfatninger om at

security- og safety-kultur er to sider av samme sak, hvor forskjellen i stor grad ligger på de områdene kulturen virker inn på. Vi ser av det teoretiske rammeverket om ulikheter mellom safety og security, at det likevel er distinkte forskjeller når det gjelder forankringen av risikokilden[3]. Dermed kan det diskuteres hvorvidt safety og security har såpass mange likheter at vi kun «bytter ut» sikkerhetsbegrepet med security. Security er mer komplekst, omfattende og mindre håndterbart enn safety-aspektet. Det handler således om helt andre årsakskilder. Det som er kjernen av kultur på mange måter, delte antakelser, ideer og felles praksis, vil kanskje ikke få det samme fotfeste i en security-dimensjon, ettersom det hevdes at det ikke er hensiktsmessig eller ønskelig å dele alle mulige felles antakelser, ideer og praksis med alle i en virksomhet når det gjelder security-arbeid i en organisasjon.

Security-kultur betraktes gjerne som en del av en felles organisasjonskultur, og noe som må være integrert i hele organisasjonens system og «ryggmarg». Det framstår ikke som noe eget eller separat, men en komponent som skal være en naturlig del av hele kulturen i bedriften. En slik tankegang stemmer godt overens med det integrerte rammeverket foreslått av van Nunen et al., som tar for seg både tekniske, organisatoriske og menneskelige aspekter sammen i det som hevdes å være en sammenhengende og helhetlig forståelse av security-kultur (van Nunen et al., 2018)[4]. Kulturen rundt security må være forankret på et strategisk nivå, som således får en helhetlig styring og kan se til at områdene som skal vektlegges, faktisk prioriteres.

5.2.1 Differansen mellom det som sies og det som gjøres

Uttrykte budskap trekkes i empirien fram som en viktig del av security-kulturen, om hva som kommuniseres rundt security, hva ledelsen sier, og hva som er den gjeldende policyen. Dette kan også sees i lys av van Nunen et al., som en del av den synlige organisatoriske delen av rammeverket hvor kommunikasjon, prosedyrer og policy uttrykkes. Det er imidlertid verdt å merke seg de doble pilene mellom det ikke-observerbare og det observerbare, som viser til den dynamiske og gjensidige påvirkningen mellom det perseptuelle og psykologiske domenet, og de mer synlige uttrykk for security-kultur (van Nunen, 2018). Individuelle holdninger, kunnskap og ikke-kommuniserte forpliktelser og prioriteringer, vil kunne påvirke hvilke teknologier man benytter seg av, retningslinjer og prosedyrer, og være førende for atferd.

[3] Tabell 1: Ulikheter mellom security og safety, s. 15
[4] Figur 4: et integrert rammeverk for security-kultur, av van Nunen et al. 2018, s. 27

Dette kan sees i lys av Scheins kategorisering av grunnleggende antakelser, verdier og artefakter, som følgelig også er et bilde på de ulike lag av kultur (Schein, 2010).

Den hverdagslige praksis kan altså forstås som en output som følge av de mer bakenforliggende verdier og grunnleggende antakelser. I det kvalitative empiriske materialet er atferd, aktivitet og praksis særlig vektlagt, og da særlig sammenhengen mellom det som sies, og det som gjøres. Praksis handler følgelig om den hverdagslige gjennomføring av oppgaver, hvordan man utfører arbeidet, en forståelse av «everyday practice». Det kan i denne sammenhengen hevdes at det vil være essensielt å rette oppmerksomheten mot det som går riktig for seg i virksomheten, i stedet for det som går galt. Hvordan foregår en suksessfull deling av informasjon? Videre kan det handle om å betrakte god håndtering av arbeidspress og målkonflikter i virksomheten, og således se på hvordan dette fungerer riktig. I Hollnagels perspektiv, bør man se på det som går bra, da det er denne tilstanden man ønsker å ha i en virksomhets hverdag (Hollnagel, 2012).

Det kan hevdes at bevisstheten en organisasjons medlemmer har når det gjelder trusselbildet og mulige scenarier, forståelsen om hvilke verdier som må skjermes, samt betydningen av security-tiltak, bør være inkorporert i organisasjonens filosofi rundt sikkerhet. Dette kan sees som en særlig sentral del av security-kulturen i en organisasjon. Videre kan disse verdiene, manifesterte i intensjoner, policyer og skrevne prosedyrer, tenkes å fungere som retningslinjer for håndtering av usikkerhet forbundet med ukontrollerbare trusler og aktiviteter. Dette er en viktig funksjon ved kultur, nemlig å håndtere usikkerhet og skape en forutsigbarhet for den hverdagslige aktivitet, for å sikre at ting går bra, i tråd med Hollnagels perspektiv om resilience engineering (Hollnagel, 2012).

Basert på det teoretiske rammeverket og foreliggende empiriske materiale, kan security-kultur forstås som de grunnleggende antakelser, ideer og intensjoner som deles blant medlemmer av en organisasjon som påvirker atferd, og som følgelig kan ha en påvirkning på security-tilstanden i organisasjonen (basert på Malcolmson, 2009). De grunnleggende antakelsene kan synes å være innlemmet i våre i visjoner, ideer og policyer, og videre påvirke faktisk atferd og artefakter, all den tid kultur omhandler grunnleggende antakelser som legger føringer for atferd. Det kan hevdes at en differanse mellom intensjoner og praksis er kjernen av security-kultur. Ut ifra en slik tanke kan det argumenteres for at jo mindre gap det er mellom intensjoner og praksis, jo bedre kultur vil man ha. Dog vil nødvendigvis dette kun gjelde dersom scoren er på et relativt høyt nivå. Lave intensjoner og lav praksis kan vanskelig kalles

en god security- eller sikkerhetskultur som sådan. Motsatt vil en kartlegging hvor gapet er stort, kunne vitne om en dårlig forankret security-kultur, hvor det som sies ikke stemmer overens med det som gjøres. Likevel kan det tenkes at det kan være vanskelig å måle kultur. Man kan stille spørsmål om hva som egentlig er kultur, da det kan virke så altomfattende og favne bortimot alt som finnes i en organisasjon (Jore, 2017). Således tar jeg også en kritisk tilnærming til min egen studie, og hypotese som sådan.

5.2.2 Faktorer i spørreskjema

Det er en forståelse av representanter fra Safetec at de ulike temaer som inngår i kartleggingen av sikkerhetskultur, fanger inn sentrale aspekt ved security-kulturbegrepet. Her inngår temaer som virksomhetens forpliktelse, bevissthet rundt security, informasjonsflyt, leders rolle og håndtering av arbeidspress[5]. Det er kan imidlertid synes problematisk at de samme temaene benyttes for både security og safety-kultur. Det er elementære forskjeller mellom safety og security når det gjelder kilden for risiko (Reniers et al., 2010, Jore, 2017), og således må det benyttes ulike framgangsmåter for å kartlegge de to fenomenene, om det i det hele tatt kan kartlegges.

Det er et funn fra empirien at bevissthet, forståelse og kompetanse rundt security-tiltak er viktig i en god kultur for security. Det kan tenkes at en sentral del av kulturaspektet handler om deling av informasjon, og være på «samme side» når det gjelder forståelse rundt hva som er viktig å bry seg om vedrørende security. Imidlertid kan det tenkes at informasjonsflyt innen security kan være problematisk, da det vil kunne være lite hensiktsmessig, og kanskje også skadelig, dersom flere mennesker sitter på mye informasjon vedrørende security.

Det kan imidlertid tenkes at informasjon som omhandler hendelser, slik som phishing-mails man ikke skal trykke på, vil være verdifullt at man har en god flyt på innad i en virksomhet. Det som derimot er mer problematisk, er deling av informasjon som kan benyttes av en «utro tjener» fra virksomheten, og det faktum at sensitiv informasjon blir mer sårbar når det er delt mellom flere personer og flere datamaskiner. Det skal likevel sies at selv om man ikke kan dele all informasjon med alle, så kan man ha en bevissthet om hva som bør beskyttes, hvem som skal ha tilgang til sentrale bygg eller avdelinger, samt hvorfor dette er viktig.

[5] Se 2.4, intensjoner og praksis s. 28

Informasjonsflyt er følgelig en av faktorene som inngår i Safetecs kulturkartlegging av security i virksomhet XX. En annen av disse temaene er det som går på «virksomhetens forpliktelse». I tillegg til å ta for seg det som uttrykkes av mål og sikkerhetsstrategier, inngår det også at «alle, både ledere og personalet, skal kjenne virksomhetens intensjoner når det gjelder safety og security[6]». Hva gjelder safety, kan dette gjerne være hensiktsmessig, men jeg stiller spørsmål ved om det er like uproblematisk på security-feltet. Skal alle virkelig kjenne til virksomhetens security-strategi? Det hevdes følgelig at dette er lite hensiktsmessig, da det kan tenkes at dette kan virke mot sin hensikt.

Det kommer også fram av empirien at det foreligger oppfatninger om at bevisstheten rundt såkalte «inside threats» er lav. Dette kan sees av informasjonsdeling, og jeg reiser spørsmål om hele personalet skal ha kjennskap til bedriftens security-strategier. En tanke om at det kan eksistere mulige insidere som kan ha et ønske om å skade virksomheten eller andre verdier, virker følgelig fjerntliggende. På den annen side skal man ikke mistenkeliggjøre sine ansatte, da det hevdes at dette kan gå på bekostning av tillitsklimaet i en organisasjons virke og hverdag. Her må det gjerne trekkes en fin linje. Likevel kan det argumenteres for at det ikke er et område som bør bære preg av naivitet, men derimot en bevisst innstilling for hvordan man forvalter den kunnskap og informasjon man sitter på. Det handler om å være klar over hvem som har tilgang til hva og utøve varsomhet i dette henseende.

Som følge av at jeg er skeptisk til noen av temaene for kartlegging av kultur, har jeg også et kritisk blikk på egen måling av security-kultur. Likevel anser jeg målingen for valid, da jeg mener at spørsmålene som er benyttet i indeksene fanger opp begrepet på en dekkende måte. Følgelig er spørreundersøkelsen og utviklingen av metodikken knyttet til denne utviklet av kompetente mennesker som kan sitt felt. Roer peker således på at en god måling av kultur handler om ferdigheter og kunnskap rundt slik måling (Roer, 2018).

5.2.3 Måling

Det kan hevdes at ikke alt i en organisasjon lar seg måle, og da særlig de underliggende antakelsene som er tatt for gitt. Det er framholdt i empiriske grunnlaget, at kultur ikke lar seg måle med spørreundersøkelser alene, og at det er nødvendig å inngå i dialog. Det ble påpekt av lederen i Safetec av en undersøkelse av Jernbaneverket, at det var store forskjell på

[6] Se 2.4, intensjoner og praksis s. 28

spørsmål som inneholdt ordet «sikkerhet». De var således «programmert» til å score høyt på slik. Da man operasjonaliserte indikatorene annerledes, fikk man også andre svar.

Dette viser til både svakheter og styrker ved måling. Du kan, dersom du har kompetanse og er bevisst metodikken og formuleringer, kunne fange inn svært interessante nyanser av en organisasjons sikkerhet- og security-kultur. Dog kan det også hevdes at resultatene kan bli uriktige og gi en feil måling, ut fra at intervjuobjektene kan ha mentale strategier eller har en slags forhåndsbestemt innstilling. I tillegg kan det stilles spørsmål ved om det er mulig å komme inn på de innerste verdier som kan sees i lys av Hofstedes «lag av kultur»[7]. Som vi også kan se av denne figuren, kan det tenkes at slike verdier også reflekteres i atferden. Roer argumenterer følgelig for at de som hevdes kultur ikke lar seg måle, ikke evner å se at kultur og bevissthet reflekteres i praksis. Imidertid, slik vi så av rammeverket til van Nunen, er en del av kulturen også ikke-oberverbar. Hvordan måles persepsjoner og tanker som man ikke selv er bevisst over? Det kan hevdes at ikke alle verdier og bakenforliggende antakelser er synlige i praksis, all den tid vi så av virksomhet XX, at også praksis kan være noe «man bare gjør», slik som bruk av adgangskort. Således kan det hevdes at det ikke alltid er en sammenheng mellom grunnleggende verdier og den faktiske atferden.

Det kan hevdes at man til en viss grad kan måle aspekter ved kultur. Dette krever dog en svært god kompetanse og metodikk. Likevel kan denne målingen være unøyaktig eller svikte ved å fange opp dypereliggende antakelser, og vi kan komme ut for intervjuobjekter som er lite samarbeidsvillige, eller misforstår spørsmål. Således er jeg også svært ydmyk til den statistiske målingen jeg selv har gjort.

5.3 Hva kan security-kultur-begrepet gi oss?

I det følgende vil jeg diskutere hva security-kulturbegrepet kan tilføre, og hvorvidt det er et begrep som er tilstrekkelig å ta i bruk i en security-kontekst.

5.3.1 Integrert forståelse

Det kommer tydelig fram blant informantene at det er behov for å knytte kulturbegrepet opp mot security-relaterte utfordringer, for å bygge en innsikt og forståelse. Videre er det en tydelig oppfatning at security-aspektet faller bort ved bruk av begrepet «sikkerhetskultur».

[7] Figur 3: Kulturens manifestasjon gjennom ulik dybde og nivå, s. 18 (Hofstede, 2010).

Her ser vi således problematikken ved at vi ikke har et tilsvarende norsk begrepssett, som dermed representerer en utfordring når det gjelder å adressere security-dimensjonen. Empirien peker på at det er et behov for et skille innen sikkerhetskultur, da safety og security følgelig representerer ulike utfordringer, og ulike måter å tenke og forholde seg til risiko på. Det kan hevdes at dersom man tydeliggjør et skille og begrepsfester security-kultur som sådan, vil man samtidig manifestere security-aspektet som noe viktig, og i seg selv rette en oppmerksomhet mot det.

Det empiriske materialet peker på et behov for større bevissthet og forståelse rundt security-utfordringer. Særlig fremheves viktigheten av en integrert forståelse og en helhetstankegang. Det trekkes fram eksempler på at man er gode på noen områder, gjerne på IKT-delen, mens man på den andre siden er dårlige på fysisk security. Dette avdekker behovet for en integrert forståelse, en holistisk tilnærming som forankres hos ledelsen. Fra studien av XX var det tydelig at et slikt engasjement ikke var på plass hos ledelsen. Da kan det vanskelig foregå en helhetlig tilnærming. En slik helhetstankegang kan sees opp mot van Nunen et al. (2018), hvor forfatterne argumenterer for et behov for å trekke linjer mellom de organisatoriske, menneskelige og teknologiske aspekter i en organisasjon. De påpeker:

> «It can be concluded that security research often lacks an integrative approach. After all, it are mainly the technological security aspects that receive attention. It is only in the last decade that the concept of security culture gains interest from researchers and business leaders, with a dominant position of information/cyber security (van Nunen et al., s. 3)

Det kom frem fra det ene intervjuet, at et selskap som Safetec arbeidet for, har en tidvis god bevissthet på security, men at det likevel mangler en integrert tilnærming i virksomheten[8]. Informanten peker på at det er investert i mye utstyr, og at det er en TV-skjerm som viser ulike overvåkningsbilder med et tidsintervall. Dersom noen ringer på ved porten, slipper personen inn vedkommende uten å vente på at bildet kommer opp på skjermen, da det blir for lenge å vente.

Den menneskelige faktor blir derfor av betydning, og således kan det tenkes at det oppstår målkonflikter mellom det sosialt aksepterte, og security-mål. Det kan hevdes at det oppfattes som lite sosialt akseptert og ineffektivt å vente til bildet kommer på skjermen. Dermed kan

[8] Se s. 55-56

det antas at de tekniske barrierene er på plass, men at den menneskelige faktoren spiller inn og hindrer tiltakene i å fungere tilstrekkelig. Man kan argumentere for at det er sentralt å rette oppmerksomheten til hvorfor man skal bry seg om disse tiltakene som er der. Hvorfor er det viktig å se hvem som faktisk er på den TV-skjermen, og hvorfor er disse tiltakene der?

5.3.2 «Det man ikke vet»

Som det kommer fram av empirien, trenger vi kanskje å se hendelser i Norge for å skjønne hvorfor det er relevant å «tenke security» også i Norge. Dog kan dette synes å være et svært reaktivt tankesett, i henhold til hva Hollnagel kaller Safety I. Likevel ser vi at det i de senere år har blitt mer søkelys på security, noe undersøkelsen for XX og Safetecs engasjement således viser.

Det kan tenkes at det er vanskelig å forstå det man ikke vet noe om. I empirien blir begrepet «kreativt bekymret» anvendt av den ene informanten, som trekker fram at poenget ikke er å fange opp sorte svaner, for du vet ikke hva som kan skje. Det man derimot kan gjøre, er å innta en ydmyk posisjon i forhold til det man ikke vet, være på «let» og ikke sette seg ned og tro at «her er alt bombesikkert» ettersom man har investert tilstrekkelig med ressurser i en port og et avansert IKT-system. Det kan hevdes at ved å innta et slikt Safety II-perspektiv i arbeidet med security, vil man være pro-aktiv på let etter signaler og fange opp hva som rører seg.

Imidlertid kan det påpekes at mulige aktører som ønsker å utføre angrep, ikke vil gi slike «signaler» (Jore, 2017). På den ene siden er det av stor betydning å kjenne til trusselbildet i samfunnet, og således erverve seg en realistisk forestilling av hvordan det globale sikkerhetsklimaet ser ut. Samtidig er det også slik at security-hendelser er komplekse, uforutsette og kan være vanskelig å forutse, såkalte sorte svaner (Taleb, 2010). Videre kan slike hendelser innta ulike uttrykk og karakteristikker, slik som sammensatte eller hybride trusler, og de kan også være såpass skjult at de ikke oppdages (Nasjonal sikkerhetsmyndighet, 2017). Dermed kan man stille seg spørsmålet om hvorvidt man kan være bevisst, eller mindful, på noe man ikke vet om. Å forstå og være bevisst safety-hendelser kan hevdes å være mer lettfattelig og enklere å ha en bevissthet om, da slike hendelser gjerne er iboende i organisasjonen og skjer oftere enn alvorlige hendelser knyttet til security. Det er dermed også en større forståelse om hvorfor tiltak og oppmerksomhet rettet mot HMS- og safety-utfordringer er viktig. Vi er ofte hendelsesstyrte i vår omgang med risiko, dersom det skjer

noe nært på oss eller som har innvirkning på våre liv, vil vi gjerne komme tettere på, og forsøke å favne om situasjonen. Da vi ikke har hatt flere større angrep i ulike industrier her i Norge, kan det også tenkes at forståelsen rundt security er lavere, enn for safety hvor vi har hatt ulike tilfeller i de senere år.

5.3.3 Skal alle vite?

At det empiriske materialet peker på behov for større forståelse og bevissthet rundt security kan på mange måter synes paradoksalt, all den tid det kan hevdes at ikke alle skal ha en bevissthet eller kunnskap i en organisasjons arbeid med security. Det er således klare utfordringer ved å benytte kulturbegrepet i en security-kontekst. Er det ønskelig at alle i en organisasjon er klar over organisasjonens tiltak rundt security, og er det ønskelig at alle har en security-awareness med seg? Jore (2017) har følgelig stilt spørsmål ved hva mindfulness betyr i en security-kontekst. Handler det om å være mistenksomme ovenfor sine organisatoriske omgivelser, kolleger, og bygge en kultur av mistillit? Dette er et spørsmål som viktig å adressere, da bevissthet ovenfor security er noe annet enn bevissthet ovenfor utilsiktede hendelser. Dersom man skal få til en sunn organisasjonskultur som arbeider konsekvent og helhetlig med security, fordrer dette en tillitsfull og helhetlig kultur, all den tid kulturbegrepet handler om *delte* egenskaper, slik som antakelser, holdninger og praksis. Det hevdes at ikke alle security-tiltak og planer bør deles med alle, og følgelig kan det være problematisk å ha en felles kultur på området.

I intervju med representanter fra FM-selskapet XX ble det pekt på at mange av de ansatte er såkalte ressurssvake mennesker med økonomiske problemer, mange med tvunget lønnstrekk og således kanskje lett påvirkbare personer. Det ble følgelig pekt på at XX kunne være et svakt punkt i et eventuelt anslag mot en av kundene, hvor XX har tilgjengelig informasjon om alle kundenes anlegg, og følgelig dårligere security-tiltak enn det som gjelder hos bedriftene selv. Dersom de ansatte i XX har innblikk i security-regimene til kundene de arbeider hos, kan det tenkes at dette utgjør en særlig sårbarhet dersom noen skulle ønske å skade selskapene. Noen av selskapene er svært store konsern, hvor eventuell skade kan være katastrofal, både med tanke på menneskeliv, og materiell og økonomisk tap. Således er områdene «bevissthet» og «kompetanse» områder hvor det må trekkes en svært hårfin linje, hvor man må ha en viss forståelse for hvilken atferd som er akseptabel, samtidig som for mye bevissthet kan virke mot sin hensikt.

Security-begrepet, og security-kultur spesielt, oppfattes av flere informanter som et umodent felt. Safety og HMS har således et større fokus i vårt samfunn, og det kan hevdes at dette er mer håndgripelig og forståelig for folk flest. Security-dimensjonen kan oppfattes som en mer fjern og distansert tanke. Det kan tenkes at dette også kommer av vår manglende evne til å håndtere en tilsiktet hendelse, som den vanlige mannen i gata. Dog ser man gjerne en tendens til at selskaper retter oppmerksomhet mot særlig IKT-delen av security, da det gjerne er gjennom teknologien vi vil se flere anslag de kommende år. Følgelig blir det viktig, fra et organisatorisk styringsperspektiv, å ta inn over seg de dynamiske aspekter og endringene i samfunnet, både blant aktører, men også sikkerhetspolitiske områder. Internasjonale spenninger og det sosiale klimaet i samfunnet spiller inn, og det vil være essensielt at sentrale aktører erverver forståelse for dette bildet.

6. Konklusjon

Vi ser fra den kvantitative undersøkelsen av XX, at intensjoner, visjoner og mål rundt security har en lavere score enn den faktiske praksis for security. Dette kan sees som følge av lavt engasjement hos ledelsen vedrørende relevansen av security-tiltak, i tillegg til høye krav og fysiske barrierer blant kundene hvor XXs ansatte leverer tjenester. Motsatt resultat gjelder for safety, hvor intensjon er høy og etterlevelse lavere. Det argumenteres at selv om praksisen scorer relativt høyt på security, kan det likevel mangle forståelse for hvorfor tiltakene er tilstede.

Security-kultur er et nytt og umodent begrep, samtidig som det er komplekst og omfatter mange av aktivitetene som foregår i en organisasjon. Det framkommer av denne studien at det er nødvendig med en tydelig begrepsavklaring på norsk, eventuelt anvendelse av security og safety som såkalte hjelpeord i norsk språkbruk.

Det var en antakelse at sammenhengen, eller et eventuelt gap mellom intensjoner og praksis rundt security, ville kunne si noe om security-kulturen i organisasjonen. Denne antakelsen står jeg ved, da jeg mener kjernen av kultur ligger i dette spennet. Security-kultur kan forstås som de grunnleggende antakelser, ideer og intensjoner som deles blant medlemmer av en organisasjon som påvirker atferd, og som følgelig kan ha en påvirkning på security-tilstanden i organisasjonen. Når det gjelder å måle et gap mellom det som kommuniseres ut og det som viser seg i faktisk atferd, er jeg ydmyk når det gjelder målingen av dette.

Security-kultur oppfattes fra Safetecs ståsted som en kombinasjon av ulike faktorer som benyttes ved kartlegging av kultur. Det hevdes likevel at disse faktorene, som også benyttes ved å kartlegge safety-aspektet i virksomheter, ikke nødvendigvis er fullgode når det gjelder å kartlegge kulturdimensjonen ved security. Jeg argumenterer for at det er flere aspekter ved kultur som er utfordrende å måle ved spørreundersøkelser og intervju, ettersom flere grunnleggende antakelser er tatt for gitt av medlemmer i organisasjonen som sådan. Security-kultur er i stor grad *alt* en organisasjon foretar seg, og derfor er det også svært utfordrende å måle kultur. Samtidig kan det tenkes at ved en god metodikk og kompetanse innen feltet, kan noen lykkes bedre med en slik måling. Kultur kan til en viss grad kartlegges, men det er utfordrende å få nøyaktige resultater, ettersom vi har å gjøre med dyptliggende og til dels skjulte fenomener. Det krever at man stiller høye metodiske krav rundt dette. Det er behov for

videre studier innen måling av security-kultur, hvorvidt dette lar seg måle, samt hvilke faktorer som er sentrale innen kartlegging av kultur.

Mangel på forståelse og bevissthet blant FM-selskapets ledelse, taler til fordel for å knytte kultur-begrepet opp mot security. Det er et funn i studien at det mangler bevissthet for hvorfor security-tiltak og oppmerksomhet rundt security er relevant. Jeg hevder at det på et sentralt nivå blant ledelse og signifikante personer er viktig med en integrert forståelse av trusselbildet og sentrale aspekt knyttet til risikostyring av security, og således sette inn helhetlige tiltak rundt de ulike security-domener. Imidlertid er jeg skeptisk til om det er formålstjenlig med en felles informasjonsdeling når det gjelder security, da ikke alle skal vite alt rundt hva som gjøres på security-fronten i en virksomhet. I tillegg kan det synes problematisk om en felles bevissthet rundt security kan legge føringer for en mistillitskultur hvor man er mistenksomme ovenfor kolleger (Jore, 2017). Følgelig må det trekkes en møysommelig linje mellom hvordan man arbeider med en eventuell kultur rundt security. Det kan hevdes at det er behov for et kulturbegrep for økt forståelse blant sentrale beslutningstakere i organisasjoner. Imidlertid er det ikke gitt at alle bør ha en like stor rolle når det gjelder arbeid med security. Videre forskning rundt dette er nødvendig, og især hvorvidt kulturbegrepet kan og bør inngå i en security-kontekst. Feltet er umodent, og det er behov for nærmere kunnskapsutvikling på området.

Kultur i en security-kontekst er en dynamisk prosess som endrer seg i takt med organisasjonen, dens medlemmer og det internasjonale sikkerhetsklimaet. Det er således ikke noe statisk innad i en virksomhet. Det påvirkes således av trusselbildet i det lokale, nasjonale og internasjonale samfunn, all den tid risiko kan sies å være allestedsnærværende og global i sin natur. Således må også tilnærmingen vi har til security, og sikkerhet som sådan, være dynamisk og holistisk i sin tilnærming.

Litteraturliste

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

Aven, T. & Renn, O. *Risk Management and Governance. Concepts, Guidelines and Applications.* London: Springer

Antonsen, S. (2009). Safety Culture - Theory, Method and Improvement. Farnham: Ashgate

Bjerke, E. (2010). Her er årsaken til Deepwater Horizon-ulykken. *Dagens Næringsliv.* Hentet den 14.06.2018 https://www.dn.no/nyheter/energi/2010/09/08/her-er-arsaken-til-deepwater-horizonulykken

Blaikie, N. (2010) *Designing social research.* USA: Polity Press

Brinkmann, S., Tanggaard, L. (2012). *Kvalitative metoder*. Oslo: Gyldendal akademisk.

Clarke, J., Hall, S., Jefferson, T. & Roberts, B. (1975). Subcultures, cultures and class. I Gelder, K. (Red), *The Subculture Reader.* New York: Routledge

Engen, O. A., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E., Pettersen, K. A. (2016) *Perspektiver på samfunnssikkerhet.* Oslo: Cappelen Damm Akademisk.

Forsvarsdepartementet (2016). Samhandling for sikkerhet - beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid. (NOU 2016: 19). Hentet den 13.03.2018 fra https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou201620160019000dddpdfs.pdf

Guldenmund, F. W. (2010) (Mis)understanding Safety Culture and Its Relationship to Safety Management. I Cox, A. (Red), *Risk Analysis,* Vol. 30, Nr. 10. Hentet den 13.05.2018 fra https://onlinelibrary.wiley.com/doi/full/10.1111/j.1539-6924.2010.01452.x

Haukelid (2001). Oljekultur og sikkerhetskultur. Arbeidsnotat, Universitetet i Oslo. Hentet den 10.05.2018 fra https://www.duo.uio.no/bitstream/handle/10852/17818/1/haukelid.pdf

Hale, A. R. (2010). Culture`s confusions. I Boustras, G. (Red), *Safety Science*. Hentet den 28.04.2018 fra http://158.132.155.107/posh97/private/culture/culture-confusion-Editorial.pdf

Hellevik, O. (1999). Forskningsmetode i sosiologi og statsvitenskap. Oslo: Universitetsforlaget

Hofstede, G. (2010). Cultures and organizations: Software of the mind. New York: McGraw-Hill

Hollnagel, E. (2012). *A tale of two safeties*. Hentet den 18.01.2018 fra http://www.resilienthealthcare.net/A_tale_of_two_safeties.pdf

Hopkins, A. (2006). *Studying organisational cultures and their effects on safety*. I Boustras, G. (Red), *Safety Science.* Hentet den 10.05.2018 fra https://www-sciencedirect-com.ezproxy.uis.no/science/article/pii/S0925753506000567

Jore, S. (2017). *The Conceptual and Scientific Demarcation of Security in Contrast to Safety.* I European Journal for Security Research. Springer International Publishing.

Jore, S. (2017) *Security culture - a sufficient explanation for a terrorist attack?* I Walls, L., Revie, M. & Bedford, T. (Red.), Risk, Reliability and Safety: Innovating Theory and Practice. London: Taylor & Francis Group

Justis- og beredskapsdepartementet. *IKT-sikkerhet – et felles ansvar*. (Meld. St. 38, 2016-2017). Hentet den 08.03.2018 fra https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf

Justis- og beredskapsdepartementet. Risiko i et trygt samfunn. Samfunnssikkerhet. (Meld. St. 10, 2016-2017). Hentet den 30.02.2018 fra https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/sec1

Justis- og politidepartementet (2006). *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner. (*NOU 2006: 6). Hentet den 13.03.2018 fra https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf

Kvale, S. & Brinkman, S. (2012). *Det kvalitative forskningsintervju*. Oslo: Gyldendal Akademisk.

Lindøe, P. H., Kringen, J. & Braut, G. S. (2015). Risiko og tilsyn. Risikostyring og rettslig regulering. Oslo: Univesitetsforlaget

Malcolmson, J. (2009). *What is security culture? Does it differ in content from general organisational culture?*

Moe, S., Framstad, A. P. (2017). Maersk varlser milliardregning etter dataangrep. *E24* https://e24.no/naeringsliv/a-p-moeller-maersk/maersk-angrepet-kostet-200-300-millioner-dollar/24119103

Morgan, D. L. (2014). *Integrating Qualitative & Qualitative methods. A pragmatic approach.* London: SAGE Publications, Inc.

Nasjonal sikkerhetsmyndighet. (2017). *Risiko 2017. Risiko og sårbarheter i en ny tid.* Hentet den 13.03.2018 fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf

Oplenskedal, A. (2015). Sikkerhetskulturens betydning i bore- og brønnplanlegging. Masteroppgave ved Universitetet i Stavanger. Hentet den 10.06.2018 fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/2375850/Masteroppgave.pdf?sequence=3&isAllowed=y

Patè-Cornell, E. (1993). *Learning from the Piper Alpha Accident: A Postmortem Analysis of Technical and Organizational Factors.* Hentet den 26.06.2018 fra http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.366.3612&rep=rep1&type=pdf

Petroleumstilsynet (2013) *Piper Alpha: Marerittet.* Hentet den 26.06.2018 fra http://www.ptil.no/artikler-i-sikkerhet-status-og-signaler-2012-2013/piper-alpha-marerittet-article9136-1094.html

Reniers, G., Cremer, K. & Buytaert, J. (2011). *Continuously and simultaneously optimizing an organization's safety and security culture and climate: the Improvement Diamond for Excellence Achievement and Leadership in Safety & Security (IDEAL S&S model)*. I Journal of Cleaner Production, 19.

Ross, A., Willson, V. L. (2017). *Basic and advanced statistical tests.* Hentet den 09.06.2018 fra https://link.springer.com/content/pdf/10.1007%2F978-94-6351-086-8.pdf

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

Ringdal, K. (2001) *Enhet og mangfold.* Bergen: fagbokforlaget

Roer, K. (2015). *Build a security culture.* Cambridgeshire: IT Governance Publishing

Rollenhagen, C. (1997). *Sambanden människa, teknik och organisation - en introduktion.* Lund: Utbildningshuset, studentlitteratur

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

Standard Norge (2012). NS 5830. *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger*.

Taleb, N. N. (2010). The black swan. The impact of the highly improbable. New York: Random House Publishing Group

Van Nunen, K., Sas, M., Reniers, G., Vierendeels, G., Koen, P. & Hardyns, W. (2018) An integrative conceptual framework for psysical security culture in organisations. I *Journal of Integrated Security Science.* Vol 2, Nr. 1. Hentet den 24.06.2018 fra https://journals.library.tudelft.nl/index.php/jiss/article/view/1986

Vivold, T. (2015) *Resilience Engineering – Nøkkelen til bygging av god sikringskultur innen petroleumsvirksomheten?*Masteroppgave, Universitetet i Stavanger. Hentet den 12.02.2018 fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/2367003/Vivoll_Tine.pdf?sequence=1&isAllowed=y

Young, W., Leveson, N. G. (2014). An integrated approach to safety and security based on system theory. Communications of the ACM, Vol. 57, Nr. 2. Hentet den 25.06.2018 fra

http://web.a.ebscohost.com.ezproxy.uis.no/ehost/pdfviewer/pdfviewer?vid=1&sid=044198d6-9d81-4048-80c8-1fc47c9a292c%40sessionmgr4010

Østensjø, C. & Larsen, C. I. (2015). *Operatørselskapene i petroleumssektoren sitt syn på sikringskultur – bruk eller ikke bruk av begrepet sikringskultur.* Masteroppgave, Universitet i Stavanger. Hentet den 27.04.2018 fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/298602/Master.pdf?sequence=4&isAllowed=y

Vedlegg 1

Informert samtykke om deltakelse i forskningsprosjektet

Dette er et informasjonsskriv om et forskningsarbeid ved Universitetet i Stavanger med følgene tema:

"I hvilken grad er det samsvar mellom intensjoner og praksis i en organisasjons security-kultur"?

Bakgrunn og formål

Formålet med denne studien er å kartlegge og skape mer kunnskap på området innen security/sikringskultur, og derav hvorvidt det kan foreligge et gap mellom en organisasjons intensjoner og den faktiske praksis når det gjelder security mot intenderte uønskede hendelser. Prosjektet er et masterprosjekt som fullføres sommeren 2018. Forskningsprosjektet er et samarbeidsprosjekt med Safetec Nordic og skal etter planen avsluttes 13.07.2018

På bakgrunn av at deres virksomhet har vært/er en kunde hos Safetec Nordic, har det blitt inngått en avtale om å intervjue noen få representanter fra selskapet. Utvalget har blitt valgt med skjønn på bakgrunn av nøkkelinformanter som kan tenkes å ha relevant innsikt i prosjektets tema.

Hva innebærer deltakelse i studien?

Deltakelsen innebærer aktiv deltakelse i intervju, med varighet på ca. 1 time. Spørsmålene vil omhandle virksomhetens praksis når det gjelder tiltak vedrørende security, og virksomhetens intensjoner som blir kommunisert som forpliktelser til omgivelsene.

Hva skjer med informasjonen om deg?

Alle personopplysninger vil bli behandlet konfidensielt. Personinformasjon og virksomhetens navn vil anonymiseres i masteroppgaven. Det vil kun være student, sensor og veileder som vil ha tilgang til full personinformasjon. Opplysningene vil bli registrert ved hjelp av lydopptak, som like etterpå transkriberes. Disse vil slettes så snart sensur foreligger på masteroppgaven.

Frivillig deltakelse

Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn.

Mange takk for deltakelse i mitt forskningsprosjekt.

Samtykke til deltakelse i studien

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

---

(Signert av prosjektdeltaker, dato)

- Jeg samtykker til å delta i intervju.

- Jeg samtykker til at opplysninger om meg kan innhentes fra universitets veileder eller sensor i masteroppgaven.

Vedlegg 2

Intervjuguide

Kort om informanten (Navn, stilling, arbeidserfaring, arbeidsoppgaver)

Security-kultur som begrep

Hvordan forstår du begrepet security-kultur?

Hva er security-kultur i forhold til safety-kultur?

I hvilken grad mener du at begrepet sikkerhetskultur fanger opp security-utfordringer?

Ser dere noen utfordringer når det gjelder å benytte kulturbegrepet i en security-kontekst?

Felles forståelse og bevissthet om sikring

Vil du si at det foreligger felles holdninger og antakelser i XX om hva som er viktige verdier når det gjelder security/sikring?

I hvilken grad er det kommunisert ut informasjon til ansatte om hvilke aktører som kan tenkes å utgjøre en trussel?

Hvordan foregår opplæring og bevisstgjøring blant de ansatte når det gjelder security-utfordringer?

Kultur

Har dere aktive tiltak for kulturbygging i deres virksomhet?

Har dere lik eller ulik tilnærming til kulturbygging når det gjelder henholdsvis safety eller security-trusler?

Organisasjonens intensjoner

Hvilke visjoner har dere – er dere obs på disse?

Hvilke strategiske målsetninger har XX når det gjelder security?

Har dere ”quotes” eller formulerte visjoner som dere kommuniserer til organisasjonens omgivelser, som del av XX´s forpliktelse på security-arbeid?

I hvilken grad er virksomhetens intensjon/målsetninger kjent for personalet?

Mener du at det i deres organisasjon er samsvar mellom ord og handling?

Organisasjonens praksis

Hva gjør dere for å ivareta sikkerhet mot intenderte hendelser?

Hender det at dere må ofre sikkerhet til fordel for noe annet?

Hender det at dere opplever målkonflikter mellom security- og safety-tiltak?

I hvilken grad mener du at prosedyrer og retningslinjer blir fulgt i XX?

Mener du at virksomhetens intensjoner samsvarer med virksomhetens praksis når det gjelder security?

Hvor godt vil du si at XXs interesser er beskyttet?

Hvorvidt vil du si at tiltakene som finnes, også blir benyttet?

Hvor ofte vil du si at ledelsen oppfordrer de ansatte til å fokusere på sikkerhet?

I hvilken grad vil du si at XX er forberedt på uønskede intenderte hendelser?

Hvilke tanker gjør du deg om at XX kan benyttes indirekte for å ramme andre mål?

Oppsummering

Hvis du kunne bestemt, hva ville du gjort med tanke på security-arbeid..?

Hva vil du si er viktige nøkkelelementer i en god sikringskultur?

Har du andre tanker og mome nter som du mener kan ha relevans for problemstillingen?

Takk for deltakelse

Vedlegg 3

Informert samtykke om deltakelse i forskningsprosjektet

Dette er et informasjonsskriv om et forskningsarbeid ved Universitetet i Stavanger med følgene tema:

"I hvilken grad er det sasvar mellom intensjoner og praksis i en organisasjons security-kultur?

Bakgrunn og formål

Formålet med denne studien er å kartlegge og skape mer kunnskap på området innen sikringskultur, og derav hvorvidt det kan foreligge et gap mellom en organisasjons intensjoner og den faktiske praksis når det gjelder sikring mot intenderte uønskede hendelser. Prosjektet er et masterprosjekt som fullføres sommeren 2018. Forskningsprosjektet er et samarbeidsprosjekt med Safetec Nordic og skal etter planen avsluttes 13.07.2018

På bakgrunn av at Safetec har utviklet undersøkelsen som er utført for FM-selskapet, vil det være ønskelig å få dypere innsikt i hvordan utvalgte representanter fra Safetec tenker om security, og om indeksen intended versus done. Utvalget har blitt valgt med skjønn på bakgrunn av nøkkelinformanter som kan tenkes å ha relevant innsikt i prosjektets tema.

Hva innebærer deltakelse i studien?

Deltakelsen innebærer aktiv deltakelse i intervju, med varighet på ca. 1 time. Spørsmålene vil omhandle virksomhetens praksis når det gjelder sikringstiltak, og virksomhetens intensjoner som blir kommunisert som forpliktelser til omgivelsene.

Hva skjer med informasjonen om deg?

Alle personopplysninger vil bli behandlet konfidensielt. Personinformasjon og virksomhetens navn vil anonymiseres i masteroppgaven. Det vil kun være student, sensor og veileder som vil ha tilgang til full personinformasjon. Opplysningene vil bli registrert ved hjelp av lydopptak, som senere transkriberes på datamaskin. Opplysningene vil slettes så snart sensur foreligger på masteroppgaven.

Frivillig deltakelse

Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn.

Mange takk for deltakelse i mitt forskningsprosjekt.

Samtykke til deltakelse i studien

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

---

(Signert av prosjektdeltaker, dato)

- Jeg samtykker til å delta i intervju.

- Jeg samtykker til at opplysninger om meg kan innhentes fra universitets veileder eller sensor i masteroppgaven.

Vedlegg 4

Intervjuguide

Kort om informanten (Navn, stilling, arbeidserfaring, arbeidsoppgaver)

Sikringskultur

Hvordan forstår du begrepet sikringskultur?

Hva er security i forhold til safety?

Hva er sikringskultur i forhold til sikkerhetskultur?

I hvilken grad mener du at begrepet sikkerhetskultur fanger opp sikringsutfordringer?

Ser dere noen utfordringer når det gjelder å benytte kulturbegrepet i en sikringskontekst?

I hvilken grad mener du at man er forberedt på uønskede villede hendelser i Norge?

Felles forståelse og bevissthet om sikring

I hvilken grad prioriteres sikringsfeltet idag, sammenlignet med tidligere?

Opplever du ulikheter blant industrier/sektorer når det gjelder oppmerksomheten for sikring/security?

Kan man ha en forståelse for det man ”ikke vet?” (”man vet ikke det man ikke vet”)

Kultur

Hvordan kan man best bidra til kulturbygging på security innad i en organisajson?

I hvilken grad mener du at kultur er styrende for fravær av uønskede hendelser?

Er det mulig å måle en organisasjons sikringskultur?

Styring

Hva tenker du om samordningen innen security mellom ulike sektorer (myndigheter, ulike nivåer etc.)? Er den god nok?

Er noen industrier/sektorer bedre rustet for å håndtere security-hendelser (sabotasje eller terror)?

I hvilken grad tror du at effektivitet eller andre interesser kan komme i konflikt med hensynet til security?

Organisasjonens intensjoner

Opplever du at noen industrier har tydelige strategier og mål på det som går på security?
Hvordan blir dette eventuelt uttrykt?
Tror du det er en sammenheng mellom den faktiske beredskapen for security, og det som kommuniseres av strategier, formål og "fest-taler" – (safety first, 0-visjon etc.).

Praksis

I hvilken grad opplever du eller tror at sikringsrisiko blir fulgt opp med relevante tiltak?
Opplever du at det rapporteres ved avvik og ulike hendelser av uønsket karakter?
I hvilken grad mener du at prosedyrer, tiltak og retningslinjer blir fulgt og benyttet?
Hvordan bør ledelser arbeide for å innarbeide og etterleve, etter ditt ståsted, god security-praksis?
Hvilke rutiner og atferd ser du for deg en organisasjon bør ha for å være forberedt på tilsiktede hendelser, slik som sabotasje eller IKT-angrep?

Oppsummering

Hvis du kunne bestemt, hva ville du gjort i forbindelse med security-arbeid?
Hva vil du si er viktige nøkkelelementer i en god sikringskultur?
Har du andre tanker og momenter som du mener kan ha relevans for problemstillingen?
Takk for deltakelse