DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram: Master i risikostyring og sikkerhetsledelse	Vårsemesteret 2023 Åpen / ~~Konfidensiell~~
Forfatter: Baste Miljeteig Ramsdal	
Veileder: Førsteamanuensis ved UiS, Christian Henrik Alexander Kuran	
Tittel: «Et nytt perspektiv» - En casestudie av hvordan safety-teori kan øke informasjonssikkerheten i komplekse organisasjoner. Engelsk tittel: - "A New Perspective" - A case study on how Safety theory can increase cyber security in complex organizations.	
Studiepoeng: 30	
Informasjonssikkerhet, Safety, Systemteori, Cyber Security, Sikkerhetskultur, Sikkerhetsstyring, Komplekse organisasjoner	Sidetall: 69 + vedlegg/annet: 83 Stavanger, 26.mai 2023

Sammendrag

Store organisasjoner er i dag uløselig knyttet til informasjonsteknologien og digitaliseringen av samfunnet, økonomien og egen drift. Teknologien endrer seg svært raskt og fører til økt kompleksitet innad i organisasjonene. En mer krevende sikkerhetssituasjon gjør organisasjoner som sitter på store mengder data, til høyaktuelle mål for dataangrep utført av eksterne aktører, men også utilsiktede hendelser. Informasjonssikkerhet har aldri vært viktigere enn nå, men likevel opplever man vellykkede dataangrep mot infrastruktur, økonomiske verdier, samt tyveri av sensitive data.

Dette åpner for å tenke nytt rundt organisering og tilnærming til informasjonssikkerhet, og har ledet til problemstillingen:

«Hvordan organisere sikkerhetsarbeidet for å øke informasjonssikkerheten i Tolletaten?»

For å svare ut problemstillingen er det gjennomført en casestudie av Tolletaten med Equinor som sammenligningsgrunnlag. Equinor som sammenligningsgrunnlag er begrenset til at deres virksomhet og problemstillinger til en viss grad gjenspeilte Tolletatens. Det er innhentet data fra Equinor gjennom intervjuer, men det er ikke en komparativ studie.

Studien har undersøkt sammenhengen mellom valgt organisering, sikkerhetskultur og informasjonssikkerhetsarbeid i Tolletaten. Det er gjennomført seks dybdeintervjuer med interne og eksterne informanter som har sikkerhet som sitt fagfelt, samt en fokusgruppe med fire ansatte som berøres av sikkerhetsspørsmål. I tillegg er det gjennomgått styringsdokumenter for sikkerhet og organisering.

I studien er det anvendt teori og perspektiver fra Safety-feltet. Anvendelse av Safety-perspektiver på tradisjonelle Security-utfordringer som informasjonssikkerhet, representerer en ny tilnærming. Studien utfordrer en oppfatning om at Safety og Security er adskilte områder og håndteres på hver sin måte.

Funnene i studien peker på flere organisatoriske forhold som skaper sårbarheter i komplekse organisasjoner og deres arbeid med informasjonssikkerhet. Dette gjelder særlig informasjonsflyt, betydningen av intern organisering og kulturelle faktorer. Sikkerhetsarbeidet svekkes også av

interesse- og ressurskonflikter, svak internkommunikasjon og mangel på en helhetlig og systemisk tilnærming.

Oppgaven kommer avslutningsvis med konkrete anbefalinger til hvordan øke informasjonssikkerheten. Anbefalingene inkluderer blant annet bruk av et systemisk perspektiv som ser organisasjonens sikkerhetsarbeid som en helhetlig prosess. Økt desentralisering av sikkerhetsfunksjoner er viktig for å gi flere deler av organisasjonen et eierskap til sikkerheten og input i design av nye rutiner. Etablering av gode feedback-kanaler vil gi et mer oppdatert og korrekt risikobilde. Sammen med en sikkerhetsbevisst toppledelse og en løs organisasjonsstruktur vil organisasjonene øke den totale informasjonssikkerheten.

Abstract:

Large organizations today are closely tied to information technology space and the expanding digitalization of both the public and private sector. The technology changes rapidly and increases organizational complexity. A significantly more challenging security situation makes organizations who possess large quantities of sensitive data, high value targets for hostile actors, but also vulnerable to internal organizational risks. Information security is more important than ever, and large resources are spent on cyber security. Still, we see successful attacks on critical infrastructure, ransomware attacks, data breaches and theft of large amounts of economic data.

This encourages new thinking and new approaches to information security. This has led to the research question:
"How to organize security to increase information security in the Norwegian customs?"

To answer this question, I have done a case study of the Norwegian customs, with Equinor as a partial comparison. The study has looked at the connection between how the organizations have chosen to organize, and its safety culture and information security work. Ten informants have been interviewed, of whom six are internal and external experts on IT-security and security issues. The remaining four are customs employees and have participated in a focus group.

This study has applied theory and perspectives from Safety, in particular systemic thinking and a focus on work processes and mental models. Applying perspectives from Safety onto traditional Security-issues, like information security, represents a new way of thinking. The study challenges the somewhat established perception that security-issues is a separate area, should be handled thereafter.

The findings point to several organizational factors which creates vulnerabilities. Most apparent are problems related to the flow of information, internal organization, and organizational culture. Security is also challenged by conflicting interests, weak internal communication and the lack of a systemic and holistic approach to security.

The study lists specific advice on tackling these issues. Among these is a systemic approach with a focus on processes, increased organizational flexibility and more decentralization of security functions. Combined with effective feedback channels and increased awareness in the top management it is possible to increase information security in complex organizations.

Forord

Denne masteroppgaven er siste del av mastergraden i Risikostyring og sikkerhetsledelse tatt ved Universitetet i Stavanger. Den representerer også det som har vært en til tider svært krevende, men unik og givende reise. En reise hvor jeg som masterstudent, ved siden av full jobb og familie har fått anledning til å lære utrolig mye spennende og nyttig, som jeg helt klart vil få bruk for senere. Engasjerte og kunnskapsrike forelesere som brenner for faget sitt, har gitt meg ekstra driv til å jobbe videre med sikkerhetsfaget og økt appetitt på samfunnssikkerhet!

Jeg vil takke mine medstudenter for god feedback, diskusjoner og råd i prosessen. Takk til informantene som deltok i intervjuene i denne oppgaven - Deres perspektiver og erfaringer er høyt verdsatt.

En spesiell takk går til min fantastiske veileder ved UiS, Christian Henrik Alexander Kuran, som med sitt glødende engasjement, omfattende fagkunnskap og vilje til å svare på spørsmål, motiverte meg til å gjøre en ekstra innsats for å løfte oppgaven. Tusen takk Christian!

Den største takken går likevel til min kjære kone, Maria. Uten din gode hjelp, avlastning, støtte og oppmuntrende ord på sene kvelder i flere år, kunne jeg ikke ha gjennomført masteren. På mange måter er dette vår oppgave. Nå skal vi endelig få tilbringe mer tid sammen igjen – jeg gleder meg!

Stavanger, mai 2023

Baste Miljeteig Ramsdal

Tabell- og figuroversikt:

Innhold

1. Innledning

1.1 Bakgrunn for problemstilling:

Digitaliseringen av samfunnet og virksomheter fører til at stadig flere områder og ansatte eksponeres for digitale trusler. Mengden av informasjon som samles og behandles blir raskt mye større og bidrar til å komplisere sikkerhetsstyringen. NSM definerer sikkerhetsstyring som «*Sikkerhetsstyring er styringen av alle aktiviteter en virksomhet gjør for å sikre en god forebyggende sikkerhet»* (NSM, 2023). Da en slik definisjon omfatter alle aktiviteter, er illustrerer dette at informasjonssikkerhet er en naturlig del av den helhetlige sikkerhetsstyringen.

Informasjonssikkerhet blir av Datatilsynet definert som;

«Informasjonssikkerhet dreier seg om å håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger» (Datatilsynet, 2018).

Å ivareta informasjonssikkerheten krever stadig mer av både samfunnet, virksomheten og de ansatte. Som et resultat av dette blir flere og flere ressurser overført til fagområdet informasjonssikkerhet i et forsøk på å møte den økende graden av digitale trusler (NSM, 2023)

Informasjonssikkerhet som en del av sikkerhetsstyringen i virksomheter og organisasjoner får derfor en mer og mer sentral rolle, noe som også kan påvirke plasseringen og ansvaret i organisasjonen. Hvem som styrer hva og har ansvar for at gjeldende lover og regler blir fulgt, samt at informasjonen ikke kommer på avveie blir derfor også stadig viktigere. Med mer sentral organisatorisk plassering og mer ansvar følger det også gjerne mer ressurser og ansvar.

Organisatoriske enheter som har sikkerhetsarbeid som fagfelt vokser, men begrepet "sikkerhet" favner ofte vidt. Det har derfor blitt vanlig å skille mellom fagfeltet Safety og Security, hvor førstnevnte gjerne omhandler "tradisjonell" HMS med fokus på å unngå utilsiktede ulykker etc., mens sistnevnte har fokus på trusler og angrep som gjennomføres med intensjon (Jore, 2017).

Et slikt begreps- og forståelsesskille fører til at ansvaret for de ulike fagfeltene innen sikkerhet ofte deles organisatorisk i virksomhetene. Informasjonssikkerhet plasseres vanligvis under avdelinger med ansvar for IT-security (Information security/Cyber Security), og er således ofte organisert adskilt fra enheter som har ansvar for Safety-området, slik som Tolletaten har gjort med sin organisering, illustrert i figur 8 (Tolletaten, 2020).

En slik fordeling av fagområder kan virke intuitivt, men begge opererer med sikkerhetsstyring i samme virksomhet. De to ulike fagfeltene opererer gjerne med ulik risikoforståelse- og tilnærming, samt kan ha ulik metodikk knyttet til å avverge uønskede hendelser og trusler.

1.2 Problemstilling og forskningsspørsmål:

Ettersom digitaliseringen av samfunnet er så gjennomgripende og påvirker de fleste virksomheter, både ressursmessig og organisatorisk er det relevant å se på hvordan sikkerhetsstyringen er organisert. Dette gjelder spesielt i store virksomheter som innehar ansvar for kritiske samfunnsfunksjoner, da oppgavene kan være mange, komplekse og konsekvensene ved uønskede hendelser store.

Dette forskningsprosjektet skal gjennom en casestudie besvare problemstillingen:

«Hvordan organisere sikkerhetsarbeidet for å øke informasjonssikkerheten i Tolletaten?»

For å svare på problemstillingen stiller jeg følgende tre forskningsspørsmål:

1) Hvilke teoretiske rammeverk bygger dagens organisering av sikkerheten på?
2) Hvordan fungerer rammeverket i praksis?
3) Er det andre teoretiske rammeverk som kan benyttes?

1.3 Oppgavens oppbygning:

Oppgaven er delt opp i seks deler. Første del, innledningen, inneholder problemstilling, forskningsspørsmål og bakgrunn for å velge Tolletaten som case. I del to redegjøres det for valg av metode, design og tilnærming. I del tre presenteres relevant teori for forskingsprosjektet. I fjerde del presenteres funn gjort i oppgavens empiridel. Deretter følger diskusjon av funn opp mot teori og forskningsspørsmål og problemstilling vil besvares. I oppgavens sjette og siste del følger konklusjonen.

Det er et klart ønske fra min side at oppgaven bidrar til økt sikkerhet, så helt til slutt presenterer jeg noen konkrete anbefalinger.

1.4 Valg av Tolletaten som case:

Tolletaten er en stor norsk statlig etat underlagt Finansdepartementet. Tolletatens oppgave er å legge til rette for korrekt og effektiv vareførsel inn og ut av landet, og samtidig sørge for å beskytte Norge mot ulovlig inn- og utførsel av varer. Samfunnsoppdraget til Tolletaten er altså stort og omfattende, og Tolletaten forvalter regelverket på vegne av mange andre offentlige aktører, slik som Skatteetaten, Mattilsynet, DSB, Miljødirektoratet, Politiet osv.

Tolletaten representerer en etat med et viktig samfunnsoppdrag om å beskytte befolkningen mot ulovlige og farlige varer samt sørge for et velfungerende samfunn og næringsliv.

Videre har Tolletaten en kritisk samfunnsfunksjon, da den bidrar til en velfungerende forsyningskjede inn og ut av landet.

Tolletaten er valgt som case da samfunnsoppdraget som innkrever, beskytter og utøver av flere myndigheters regelverk, innebærer at Tolletaten besitter store mengder sensitive og verdifulle data, slik som personopplysninger, lisenser, bedriftshemmeligheter, kontrolldata og analyser. I tillegg er mye av Tolletatens arbeid av en slik art at den berøres av Safety- og Security, slik som operativt arbeid og beskyttelse av lokaler og personell. Å utøve et slikt samfunnsoppdrag kan kreve mye av en organisasjon, særlig når man skal balansere effektivitet, representere statens verdigrunnlag og økonomiske betingelser, og samtidig ta nødvendige grep for å sikre informasjon og personell.

Hvordan en stor norsk etat med ca. 1500 ansatte tilnærmer seg en slik utfordring er av generell interesse, da Tolletaten representerer en aktør med makt og innflytelse på flere områder, samt ansvar for innkreving av avgifter som finansierer velferdsstaten. Videre har Tolletaten stor potensiell påvirkning på befolkningens liv og helse gjennom arbeidet med nasjonal sikkerhet, samt et stort ansvar for å også ivareta personopplysninger og sensitive data. Tolletatens er tett knyttet til andre regelverkseiere som Forsvaret, Politi, Skatteetaten gjennom håndhevelse av deres regelverk, samt tett samarbeid. Denne rollen gjør Tolletaten til et potensielt høyt prioritert mål for ondsinnede aktører, men også en etat som må ivareta tillitten til befolkningen ved å selv jobbe for å beskytte data.

1.5 Equinor som sammenligningsgrunnlag:

Tolletaten er studiens eneste case, og oppgaven er slik sett ikke en komparativ studie. Mer informasjon rundt casestudiet presenteres i punkt 2.2.

Equinor ASA er et svært stort internasjonalt energiselskap med ca. 21 000 ansatte fordelt på 30 land, hvor den norske stat har en eierandel i selskapet på 67%. Med en produksjon på to millioner fat oljeekvivalenter er selskapet et av verdens største operatører innenfor olje og gass, samt en betydelig aktør innenfor fornybar energi slik som havvind.

Som en svært stor organisasjon med flere tusen ansatte fordelt over mange ulike land, hvor mange av dem jobber i høyrisikomiljøer offshore, er sikkerhet et sentralt element i hverdagen til hele selskapet, deres underleverandører og de ansatte. Når Equinor i tillegg sitter på svært sensitiv informasjon i form av forretningshemmeligheter, persondata, svært store økonomiske verdier er selskapet utsatt både for security- og safety-risikoer.

Equinors egen tilnærming til området sikkerhet er oppgitt å være en «proaktiv kultur hvor sikkerhet og sikring er integrert i alt vi gjør». Selskapet jobber etter nullvisjonen, altså null skader på mennesker, miljø og eiendeler. Selskapets ledelse innen sikkerhet og sikring har innstillingen om at alle ulykker kan forebygges. Konserndirektør for Sikkerhet, sikring og bærekraft, Jannicke Nilsson, oppgir videre at «*vi ønsker å ta mest mulig læring rundt hendelsene*» (Equinor.com, 2023)

Denne kombinasjonen av det å være en stor, kompleks organisasjon som jobber i et krevende dynamisk miljø, og som har valgt en proaktiv og omfattende tilnærming til sikkerhetsarbeid, gjør organisasjonen interessant som et sammenligningsgrunnlag når det kommer til sikkerhetsarbeid, også i forhold til Tolletaten med tanke på kompleksitet og ansvar.

2 Metode:

I dette kapittelet vil jeg redegjøre for mitt valg av metode, forskningsdesign samt etiske overveielser som jeg måtte ta stilling til. Jeg vil videre forklare hvorfor jeg har tatt de metodiske valgene jeg har tatt og planen for oppgaven.

2.1 Valg av metode og problemstilling:

Valg av problemstilling ble tatt på bakgrunn av et ønske å oppnå økt forståelse av temaene. Problemstilling kan forstås som *«spørsmål som blir stilt med et bestemt formål, og på en så presis måte at det lar seg belyse gjennom bruk av samfunnsvitenskapelig metoder»* (Halvorsen, 2008, s. 35)

Problemstillingen ønsket å undersøke forholdet mellom valgt organisering og sikkerhetsstyring innen informasjonssikkerhet. Denne problemstillingen var eksplorativ, og da måtte jeg komme tett på temaene og de som kjenner fenomenet best og selv sitter med egne erfaringer og perspektiv. At problemstillingen legger føringer for valg av metode er i tråd med Johannesen mfl. (2010) som skriver at; *«det er undersøkelsens problemstilling som styrer valg av metode, og som avgjør hvor vellykket forskningsprosjektet er, fordi den angir de spørsmålene som undersøkelsen forventes å gi et svar på»* (Johannesen mfl., 2010, s. 59)

Det var også praktiske fordeler ved å velge kvalitativ metode. Siden datainnsamlingen skulle foregå gjennom intervjuer med informanter var det viktig med fleksibilitet. I henhold til Thagaard, (2018) er en av fordelene med kvalitativ metode at den gir forskeren økt fleksibilitet og mulighet for å justere kursen underveis (Thagaard, 2018).

Med dette som utgangspunkt valgte jeg å benytte kvalitativ metode, da (..) *«kvalitativ metode er særlig hensiktsmessig hvis vi skal undersøke fenomener vi ikke kjenner særlig godt, og som det er forsket lite på»* (Johannesen mfl., 2010, s. 32). Min subjektive opplevelse av at å benytte safety på securityområder var lite forsket på, sammenfalt slik sett bra med valg av kvalitativ metode.

2.2 Valg av case som forskningsdesign

Oppgavens problemstilling er utforskende, noe som var av betydning for mitt valg av forskingsdesign. Problemstillingen ønsket å se nærmere på hvordan arbeidet med sikkerhetsstyring, og særlig arbeidet med informasjonssikkerhet foregår i Tolletaten.

Valget falt da på å benytte et casedesign. *«Case-studier kan defineres som intensive undersøkelser av et fåtall analyseenheter» (Thagaard, 2018, s. 51).* Et casedesign kjennetegnes ved at man henter inn mye informasjon fra få enheter som man analyserer (Johannesen mfl., 2010). Fordelen med å benytte casedesign i denne oppgaven var at jeg kunne studere organisasjonen Tolletaten som på et overordnet nivå, men likevel benytte metoder som intervjuer for å komme tett på kilder som kunne bidra med en dypere kunnskap om temaene og høre deres perspektiver på flere nivå i organisasjonen.

Ved å benytte to eller flere caser kan man utføre en sammenligning av ulike organisasjoner og se etter likheter. Denne vinklingen og bruk av flere caser blir gjerne omtalt som en komparativ case-studie (Thagaard, 2018). Denne oppgaven har imidlertid kun ett case, Tolletaten, og er ikke en komparativ studie. At Equinor er inkludert er med hensyn til utfordringer med å innhente nok data fra Tolletaten alene.

2.2.1 Etiske refleksjoner og dilemma:

Det etiske aspektet er viktig innen forskning, særlig gjelder dette forskning som berører enkeltmennesker direkte og hvor forskningen kan få konsekvenser for deltakerne eller menneskene som er involvert i prosjektet (Johannesen mfl., 2010). Med et forskningsprosjekt som skulle se på organiseringen av en virksomhet hvor mennesker jobber og innhenting av data gjennom intervjuer direkte med mennesker, ble det tidlig klart at her måtte jeg som forsker være bevisst på den etiske komponenten.

De forskningsetiske retningslinjene til «Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora (NESH)» var aktuelle for forskningsprosjektet. Disse vektlegger blant annet *«informantens rett til selvbestemmelse og autonomi, forskers plikt til å respektere informantens privatliv og forskerens ansvar for å unngå skade»* (Johannesen mfl., 2010, ss. 91-92)

Da virksomheten jeg undersøkte var en stor og aktør med mye ansvar og fullmakter i samfunnet ble jeg tidlig klar over etiske utfordringer og dilemmaer som kunne dukke opp i forskningsprosjektet, både relatert til informantene, men også rollen til virksomheten.

Datainnsamlingen ble bestemt gjennomført via intervju med informanter, noe som gjorde at jeg måtte sørge for å bevare deres personvern og skjerme dem fra eventuelle negative reaksjoner.

Det første steget i denne prosessen var å sjekke om jeg var pliktig til å melde forskningsprosjektet til Norsk senter for forskningsdata (NSD). Da prosjektet skulle samle inn personopplysninger om informantene i form av navn, stilling, kjønn og bakgrunn var det klart at jeg måtte melde prosjektet og ha en databehandlingsplan (NSD). Dette kravet er avgjørende både for å bevare personvern hos informantene og deres privatliv (Johannesen mfl., 2010)

Videre var det et dilemma når det kom til vurderingen av funn i forskningsprosjektet og publisering av disse, opp mot å begrense eksponeringen av sårbarheter som kunne bli avdekket. En uforbeholden publisering av negative funn ville i helt spesielle tilfeller, kunne svekke tilliten til virksomheten og gjøre trusselaktører klar over nye sårbarheter og svakheter i virksomhetens organisering.

Når man innhenter data gjennom intervjuer er det viktig at man tar hensyn til informantens rett til selvbestemmelse og at de deltar av egen fri vilje (Johannesen mfl., 2010, s. 91). For å være sikker på at informantene var klar over hva de deltok i og hvordan dataene deres ville bli brukt ble det utformet et samtykkeskjema som ble utdelt og signert av alle informantene som deltok i intervjuene. Som en del av prosessen med å samle inn data ønsket jeg å la informantene få muligheten til å gå gjennom sine egne bidrag og være trygg på at jeg som forsker ikke hadde endret dataene til ugunst for informanten.

2.3. Datainnsamling:

2.3.1 Forskerens rolle:

Jeg er selv ansatt i Tolletaten og har etter ti år i organisasjonen god kjennskap til personer og enheter. Selv om dette umiddelbart kan virke som en fordel, så kan det å gjennomføre studier i egen organisasjon gjøre det krevende å lage gode og relevante spørsmål til en intervjuguide eller være mindre kritisk til forhold som er delvis kjent fra før (Thagaard, 2018)

Ettersom jeg var bevisst på min rolle som ansatt i organisasjonen valgte jeg en problemstilling som krevde at jeg måtte søke perspektiv og kunnskap utenfor mitt umiddelbare nettverk og arbeidsområde. Ved å hente informanter fra andre deler av virksomheten og fra eksterne aktører ønsket jeg å distansere meg i en slik grad at spørsmålene ble utformet og stilt slik at de var relevant for forskingsprosjektet, ettersom jeg ikke utelukkende kunne ta utgangspunkt i egen kunnskap. En kombinasjon av å studere kjente og ukjente forhold innenfor egen organisasjon er én måte å oppnå nye perspektiver og få tak i relevante data (Thagaard, 2019).

Som ansatt i Tolletaten hadde jeg også et godt utgangspunkt for å starte rekruttering av kunnskapsrike informanter med antatt relevante betraktninger rundt problemstillingen. Disse rekrutterte videre etter snøballmetoden, noe som kan ha påvirket hvilke interne informanter som deltok i forskningsprosjektet. For å unngå skjevhet i utvalgene, ble f.eks. fokusgruppen strategisk valgt på bakgrunn av at de i mindre grad enn andre jobbet med spesifikt med informasjonssikkerhet.

Jeg valgte derfor å presentere meg selv og prosjektet skriftlig og muntlig ovenfor informantene, og påpekte at det var forskingsprosjektet som var i fokus og ikke meg, som deres kollega eller en ansatt. En slik presentasjon bidrar til å avklare hvem forskeren er og hva som er hensikten med forskningsprosjektet og etablere tillitt (Johannesen mfl., 2010).

2.3.2 Fokusgrupper:

Det ble tidlig besluttet å benytte fokusgrupper som én av måtene innhente data på. Fokusgrupper kan beskrives som en *«liten gruppe av mennesker, som har visse trekk og som bidrar med kvalitative data i en begrenset diskusjon for å forstå et tema eller område av interesse»* (Kruger & Casey, 2015, s. 6).

Forskningsprosjektet ser både på virksomhetens organisering og mål. Dette er områder som fokusgrupper kan være medvirkende til å belyse. Fokusgrupper er gode metoder for innhenting av data både når det gjelder organisasjonsutvikling og kartlegging av behov (som f.eks. for å nå målet om økt sikkerhet). Grunnen til at fokusgrupper kan være spesielt egnet i slike tilfeller er at de (..) *«tillater at folk diskuterer utfordringer, tanker og perspektiver og sammenligner sine egne opplevelser med andres»* (Kruger & Casey, 2015, s. 13)

Datainnsamlingen gjennom fokusgrupper skjer ved at man skaper et trygt og selvutleverende miljø hvor deltakerne i gruppen kan fortelle om sine erfaringer, perspektiver og tanker rundt temaet som forskningsprosjektet handler om (Kruger & Casey, 2015). Som en del av forskningsprosjektet var det av interesse å se nærmere på hva ulike personer tenker om kultur, verdier, utfordringer og generelle refleksjoner rundt f.eks. sikkerhetskultur, organisering og hva som ble oppfattet som hensiktsmessig og eventuelle utfordringer med informasjonssikkerhet. Bruk av fokusgrupper for å finne denne type informasjon, samt oppmuntre til forslag mm. er i tråd med anbefalingene til Kruger & Casey (2015).

Det ble innledningsvis valgt å ha tre fokusgrupper med fem deltakere i hver fokusgruppe. Fordelene med slike mini-grupper er hver deltaker får mer tid til å fortelle sin historie, det kan være enklere å komme til ordet og man kan diskutere vanskelige temaer som gjerne krever at man avsetter litt ekstra tid og oppmerksomhet (Johannesen mfl., 2010) Det var også et ressursaspekt i valg av fokusgrupper, da det var besparende i form av mindre reising og færre individuelle avtaler på ulike lokasjoner i landet.

2.3.3: Valg av informanter og fokusgruppenes sammensetning

Informantene ble valgt strategisk med tanke på hva som ble ansett som hensiktsmessig for å undersøke tematikken i problemstillingen. Johannesen mfl. (2010, s. 105) skriver at *« hensikten med kvalitative undersøkelser er å få mest mulig kunnskap (fyldige beskrivelser), og ikke foreta statistiske generaliseringer»*. Informantene ble derfor rekruttert med bakgrunn i deres kjennskap til temaene som tas opp i problemstillingen samt deres plassering i organisasjonen.

Videre ble det vektlagt bakgrunn- og antall år i virksomheten, samt deres arbeidsoppgaver, som alle berøres av ulike former for sikkerhet. Denne kombinasjonen ble ansett for å gi et godt datagrunnlag.

Kruger & Casey (2015) argumenterer for å være oppmerksom på maktstrukturer i organisasjonen og unngå et skjevt maktforhold i fokusgruppen. Med bakgrunn i deres anbefaling valgte jeg å ikke blande linjeledere og deres ansatte i samme fokusgruppe. Hensikten med dette var å unngå eventuell selvsensur under samtalene.

2.3.4: Rekruttering av informanter til fokusgruppene:

Etter at jeg hadde bestemt meg for profilen til informantene undersøkte jeg organisasjonen og fant ansatte som passet i henhold til valgkriteriene. Disse ble kontakt og orientert om forskningsprosjektet og hvorvidt de var positive til å bli invitert inn i prosjektet, når samtykkeskjema og informasjonsskriv var på plass. I kontakt med de første informantene pekte de på andre personer som kunne være av interesse. Denne måten å rekruttere informanter på er gjerne kjent som «snøballmetoden» da antall aktuelle informanter øker etter hvert som den ruller, som følge av at stadig flere peker på andre personer, som gjerne ligner dem selv (Kruger & Casey, 2015), (Thagaard, 2018).

En utfordring med snøballmetoden er at de første personene peker på andre innen sitt eget nettverk eller noen som de vet er positive til å delta i prosjektet (Thagaard, 2018). Et slikt utvalg av informanter ofte har høyere utdanning og gjerne er mer positive til forsking og har høyere mestringsfølelse, hvilket gjør at det oppstå en skjevhet som fører til at informasjon om negative forhold ikke kommer like tydelig frem. (Thagaard, 2018, s. 58).

For å prøve å motvirke en slik potensiell skjevhet valgte jeg å blande deltakere med både med og uten høyere utdannelse i fokusgruppe 1, bestående av ansatte.

Denne gruppen inkluderte heller ikke deltakere med IT eller sikkerhetsbakgrunn, da disse kunne risikere å «eie» samtalen i kraft av sin kompetanse.

2.3.5: Valg av intervjuteknikk og intervjuguide:

Målet med intervjuene var å få dybdekunnskap om temaene. Valg av intervjuteknikk var også preget av dette. Det brukes i hovedsak to intervjuteknikker; strukturerte og semistrukturerte intervju. Førstnevnte er preget av at det gjerne finnes klare svaralternativ og relativt enkel struktur mens sistnevnte er kjennetegnet ved at spørsmålene er mer åpne og intervjueren lar informanten snakke mer fritt. Det ble ansett som hensiktsmessig å benytte semistrukturerte intervjuer for å la informantene reflektere og snakke åpent. En fordel ved å benytte semistrukturerte intervjuer er at, selv om temaene i hovedsak er kjent, så er det større fleksibilitet til å justere spørsmålene underveis, samt muligheten til «grave» litt ekstra i form av oppfølgingsspørsmål hvis informantene kommer med refleksjoner og tanker som ikke var tenkt ut på forhånd (Thagaard, 2018).

Intervjuguiden ble utformet med åpningsspørsmål, hovedspørsmål og avslutningsspørsmål, da denne strukturen gjør det enkelt for deltakerne samt moderator å følge med på spørsmålsrekken. Spørsmålene ble forsøkt å holde enkle og å unngå dobbeltspørsmål og ja/nei spørsmål, da dette ville motvirket hensikten med å la informanten komme med tilleggsinformasjon. (Kruger & Casey, 2015).

2.3.6: Endringer i antall informanter, fokusgrupper og intervjustruktur.

Grunnet mindre tilgang til informanter enn forventet ble det i løpet av datainnhetningsprosessen nødvendig å redusere antall fokusgrupper fra tre til én, som bestod av fire ansatte. Den planlagte fokusgruppen bestående av eksperter utgikk da det ikke lot seg gjøre å samle så mange fageksperter samtidig pga. virksomhetens ressursbehov.

For å kompensere for dette og utvide datagrunnlaget ble det derfor gjennomført flere enkeltintervjuer enn først tiltenkt. Endringen til flere enkeltintervjuer beveget også intervjustrukturen i en mer ustrukturert retning, da informanten nå var alene og friere kunne fortelle om sine erfaringer og betraktninger. En mer åpen og uformell struktur på intervjuene gir forskeren mulighet til å få kjennskap til områder og temaer som ikke var tenkt ut i forkant (Thagaard, 2018). Det ble også nødvendig å hente inn informanter utenfor virksomheten. Disse ble hentet inn via eget nettverk og snøballmetoden.

2.3.7: Valg av informanter og deres relevans for forskingsprosjektet

Det er fire utvalg i forskningsprosjektet. Utvalgene består av én fokusgruppe med fire internt ansatte, uten formell utdanning innen sikkerhet, men som omgås sikkerhetsrelaterte problemstillinger i sitt daglige virke. Videre er det gjort intervjuer med fire informasjonssikkerhetsrådgiver, hvorav to ansatte og to eksterne konsulenter. I tillegg er det gjort intervju av to sikringsrådgivere i Equinor. Til sammen er det ti informanter som har deltatt i studien. Informantene og deres relevans for prosjektet er beskrevet i Tabell 1.

Utvalg	Informant og kode	Beskrivelse
Fokusgruppe med fire ansatte	Ansatt 1 (A1) Ansatt 2 (A2) Ansatt 3 (A3) Ansatt 4 (A4)	Fire tjenestemenn- og kvinner fra Tolletaten med både operativ og administrativ bakgrunn. Informantene har mellom tre og 35 års arbeidserfaring i Tolletaten. Arbeidserfaring med både digital sikkerhet og fysisk sikkerhet Tre har yrkesutdanning fra Tolletaten og én har høyere utdanning.
Interne IT-eksperter	Intern IT 1 (IT-1) Intern IT 2 (IT-2)	Begge er IT-ansatte i Tolletaten og har mer enn fem års erfaring med informasjonssikkerhetsarbeid. De er tett på utviklingen og har god kunnskap om fagfeltet.
IT-Konsulenter	Konsulent 1 (K1) Konsulent 2 (K2)	Begge jobber i konsulentbyrå og har fra fem til over 20års erfaring innen informasjonssikkerhet. En jobber som informasjonssikkerhetsrådgiver og en jobber for tiden som sikkerhetsarkitekt.
Sikringsrådgivere Equinor	Senior Security Advisor (EQ1) & Senior Consultant, Sikring og Beredskap (EQ2)	Sikringsrådgiverne ansatt i Equinor. Inntil 20 års erfaring med Security, Safety og beredskapsarbeid, både on- og offshore.

Tabell 1: *«Beskrivelse av informantene som deltok i studien»*

Informantene i fokusgruppen (A1-A4), som bestod av ansatte er ble valgt på bakgrunn av sin kjennskap til Tolletaten som organisasjonen og kan dele fra arbeidstakers ståsted. Et innblikk i hvordan sikkerhetsarbeid fungerer og oppleves på de lavere nivåene i organisasjonen ble ansett som relevant for å få et annet perspektiv enn et rent sikkerhetsteoretisk ett.

De to interne IT-ekspertene (IT1, IT2) ble valgt grunnet deres inngående kjennskap til sikkerhetsorganiseringen i Tolletaten og hvordan de opplever dagens organisering, samt deres tanker rundt anvendelse av teori og praksis med Tolletaten som case.

De to informasjonssikkerhetskonsulentene (K1, K2) representerer et utvalg som har et noe annet perspektiv, da de har kjennskap til flere typer virksomheter og problemstillinger som kanskje ikke

Tolletaten er berørt av. Det ble derfor ansett som hensiktsmessig å få input fra eksterne aktører for å heve blikket utover Tolletaten og få et sammenligningsgrunnlag.

De to siste informantene (EQ1 og EQ2) er sikringsrådgivere fra Equinor. De besitter lang og inngående kjennskap til sikkerhetsarbeid- og teori, samt praktisk anvendelse i en stor, kompleks og høyprofilert organisasjon som opererer i et risikofylt miljø. Deres innsikt og erfaringer er interessant, særlig siden Equinor også besitter store fysiske og digitale verdier. Ettersom Equinor også er en stor og kompleks organisasjon, men mange oppgaver og tett kobling til resten av samfunnet, så ville det være interessant å se selskapet i sammenheng med en offentlig etat, slik som Tolletaten.

3. Teori:

I denne delen vil oppgaves teoretiske fundament beskrives. Teorien her vil bli brukt til å besvare oppgavens problemstilling.

3.1 Lovfestet sikkerhetsregelverk

For å kunne ta stilling til Tolletatens sikkerhetsarbeid, er det relevant å se på dens forpliktelser etter lovverket som regulerer deler av dette. I denne sammenhengen vil jeg se nærmere på noen deler av «Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter» (internkontrollforskriften) og Lov og nasjonal sikkerhet (sikkerhetsloven)

3.1.1 Plikt til internkontroll og sikring av informasjon (informasjonssikkerhet)

Plikten til internkontroll og sikring av verdier og informasjon er hjemlet i Internkontrollforskriften: *«Den som er ansvarlig for virksomheten skal sørge for at det innføres og utøves internkontroll i virksomheten og at dette gjøres i samarbeid med arbeidstakerne og deres representanter»* (Internkontrollforskriften, u.d.).

Videre står det at *«Arbeidstakerne skal medvirke ved innføring og utøvelse av internkontroll»* (ibid.). I kommentarene til internkontrollforskriften er presisert at «Det er helt sentralt at internkontroll integreres i overordnet styring og planlegging av virksomheten.» (interkontrollforskriftens kommentarer til §4)

I sikkerhetsloven, som blant annet gjelder for statlige organer (sikkerhetsloven §1-2 1.ledd) er informasjonssikkerhet omtalt i §5-1a. Her står at;

«Virksomheten skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdig informasjon, slik at informasjonen ikke blir kjent for uvedkommende» (Sikkerhetsloven, 2019)

På bakgrunn av dette kan man kan hevde at det fremgår at sikkerhetsarbeid er et lederansvar knyttet til den enkelte virksomheten, men at alle de ansatte skal være involvert og har plikt til å medvirke til sikkerhetsarbeidet. Sikkerhetsarbeid- og styring er altså en sentral del av organisasjonen. I tillegg er det klart at menneskene i organisasjonen har en nøkkelrolle i denne sammenhengen. En slik gjennomgripende tilnærming i hele organisasjonen har ført til at flere teoretikere snakker om en organisasjonskultur, herunder også en sikkerhetskultur.

3.2 Sikkerhets- og organisasjonskultur

Når man ser på sikkerhetskultur i store offentlige virksomheter, slik som Tolletaten kan det være hensiktsmessig å se på både struktur og kultur i organisasjonen.

3.2.1 Organisasjonsstruktur

Store offentlige organisasjoner har gjerne en det man oppfatter som en «natur», eller en spesiell organisasjonsstruktur- og kultur. Slike organisasjoner kan f.eks. ha en byråkratisk organisasjonsform. Christensen mfl, (2021) skriver at «*byråkratiske organiasasjoner er preget av hierarki, arbeidsdeling og rutiner, men også av samordning som opptrer sammen med spesialisering. Hierarki innebærer over- og underordning mellom ulike vertikale nivåer i organisasjonen»* (Christensen mfl, 2021, s. 39).

I et byråkratisk hierarki er det gjerne tydelig arbeidsfordeling med regler for hvem som gjør hva og når, samt mange rutiner og prosedyrer som regulerer arbeidsoppgavene. Slike regulereringer kan også innebære *hvordan* oppgavene skal utføres. Foruten en vertikal fordeling av ansvarsområder kan det også eksistere en horisontal struktur i organisasjonen. Det horisontale nivået i hierarkiet er ofte delt opp i ulike enheter og avdelinger, som utfører visse typer arbeidsoppgaver basert på spesialisering på et fagområde eller et funksjonsprinsipp (Christensen mfl, 2021).

Oppgave- og problemløsning etter et slikt prinsipp kan være ekstra vanskelig dersom man skal løse problemer som berører flere områder og nivåer i organisasjonen, samt når det er uklart hvem

som har ansvar for å løse problemet. *«Særlig for gjenstridige problemer («wicked issues»), hvor problemene ikke kan løses innenfor ett departementsområde eller på ett forvaltningsnivå, men krever samhandling på tvers, skaper slike organisasjonsformer problemer»* (Christensen mfl, 2021, s. 41).

3.2.2 Organisasjonskultur

Organisasjonskultur kan beskrives som: *«de uformelle normene og verdiene som vokser fram og har betydning for livet i virksomheten til formelle organisasjoner»* (Christensen mfl, 2021, s. 56).

Ut fra denne beskrivelsen så er ikke organiasjonskultur noe statisk, men noe «levende» og dynamisk som vokser frem over tid og former organisasjonen. Utvikling av normer og verdier kan skje over lang tid og kan gradvis utvikle seg fra formelle organiasjoner til det Christensen mfl, (2021) referer til som instutisjoner. Medlemer, som ansatte og ledere i slike instutisjoner utvikler og internaliserer ofte verdiene og normene organiasajonen har. En slik internalisering kan bidra til mindre støy og spenning i organisasjoner da medlemmene opplever å ha felles mål og en sterk fellesskapsfølelse. Christensen mfl, (2021) peker imidlertid på at en slik organisasjon kan være mer kompleks og mindre fleksibel og risikere å låses til et mønster, noe som ikke alltid trenger å være optimalt.

Reason viser også til adferd og gruppens felles verdier i sin definisjon av organisasjonskultur, som han definerer slik; *"Shared values (what is important) and beliefs (how things work) that interact with an organizations structures and control system to produce behavioural norms (the way we do things around here)".* (Reason, 1997, s. 192)

Organisasjonskultur og betydningen av det kulturelle perspektivet innenfor sikkerhetstenkning er noe som har fått mer fokus de siste tiårene. Engen mfl., (2021) viser til rapporten fra 22. Juli-kommisjonen som påpekte at: «*kulturen bidro til at ledere i for liten grad erkjente risikoene man stod ovenfor, og dominerende holdninger og verdier begrenset deres og forvaltningens evne til gjennomføring og samhandling»* (NOU 2012:14, (Engen mfl, 2021, s. 174). Koblingen av organisasjonskultur til terrorangrepene 22.juli viser at det organisasjonskulturen kan ha direkte påvirkning på sikkerhetskulturen.

3.2.3 Sikkerhetskultur

Et mye brukt begrep innen sikkerhet er begrepet «sikkerhetskultur». Det finnes ikke en omforent definisjon av sikkerhetskultur, men sikkerhetsteoretikeren James Reason, gjengir en definisjon, opprinnelig gitt av UK Health and Safety Commission fra 1993, som lyder slik:

"The safety culture of an organization is the product of individual and group values, attitudes, competencies, and patterns of behavior that determine the commitment to, and the style and proficiency of, an organization's health and safety programmes. Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety, and by confidence in the efficacy of preventive measure" (Reason, 1997, s. 194).

Reason presenterer fire deler som må være på plass for å ha en velfungerende sikkerhetskultur. De fire delene er en rapporterende kultur, en rettferdig kultur, en fleksibel kultur og en lærende kultur. Resultatet av disse omtaler som en «informert kultur» (Reason, 1997).

Grunnlaget for å etablere en god rapporteringskultur er at det oppleves som trygt, enkelt og hensiktsmessig å melde om feil og avvik. En organisasjon som oppfordrer til rapportering av egne og andres feil er imidlertid avhengig av stor tillitt mellom ledelsen og de ansatte, slik at medlemmene i organisasjonen har tro på at de får en rettferdig behandling hvis de rapporterer feil (Reason, 1997). Medlemmene i organisasjonen føler ofte stor lojalitet til hverandre og har trolig få eller ingen insentiv til å rapportere kollegaer. Reason (1997) peker på at det å ikke skape problemer for seg selv eller andre er i seg selv et sterkt insentiv til å *ikke* rapportere.

Et tydelig skille mellom handlinger som begås med intensjon og som straffes, og feilhandlinger som er uten skyld er viktige for å ivareta denne tillitten. Dette skillet mellom intensjon eller ikke gjerne ikke svart-hvitt. Mangelfull opplæring, feil verktøy, dårlige prosedyrer for risikable situasjoner, kan medføre at medlemmene bevisst bryter reglene for å håndtere jobben, uten at de har til hensikt å skade. Dette kan tyde på at feilene systemiske i natur (Reason 1997).

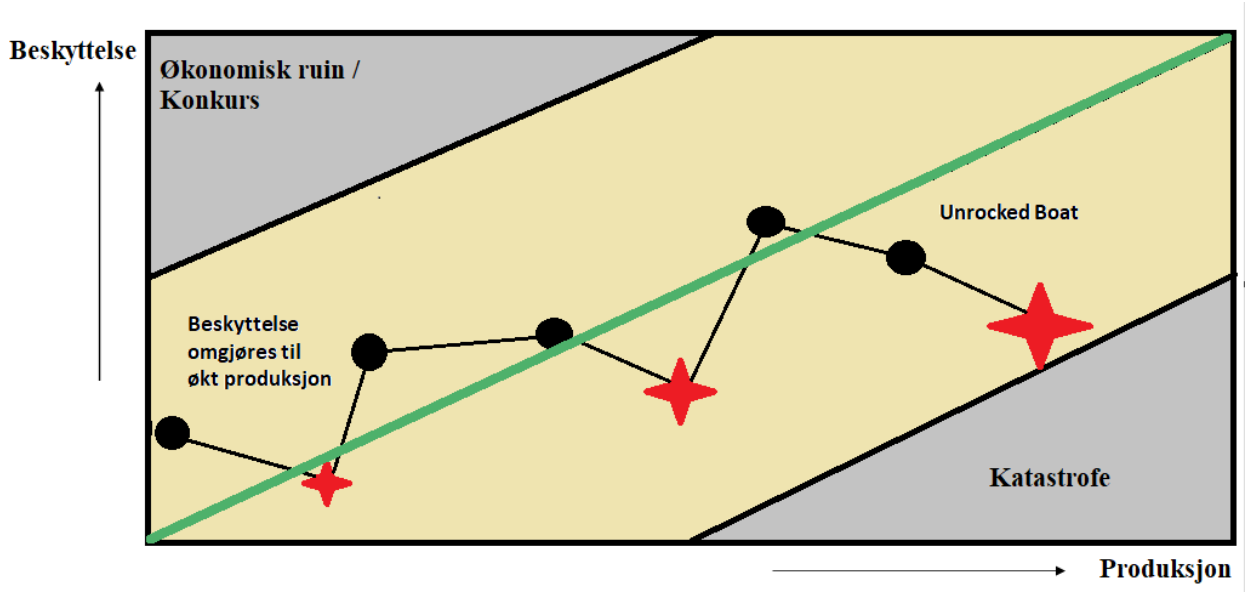
Reason har sett på hvordan feil og avvik behandles, og anbefaler at aktøren som behandler avviksmeldingene ikke samtidig har muligheten til å sanksjonere. Konfidensialitet i rapporteringen er også en forutsetning for å etablere og opprettholde tillitten. Andre forskere, som O`Leary & Chapell, peker likevel på at full anonymitet potensielt kan svekke rapportene da avviksbehandleren

ikke har mulighet til å utrede detaljer eller se nærmere på f.eks. en påstand om at feil er gjort (Reason, 1997).

Den tredje delen er at organisasjonen har en fleksibel kultur. En fleksibel kultur er kjennetegnet av at den har evne til å omstille til nye situasjoner seg og benytter seg av variasjon, samt læring av tidligere og lignende hendelser (Reason 1997). Medlemmer i organisasjonen utveksler erfaringer gjennom det Weick (1987) kaller «War stories», altså fortellinger om uønskede situasjoner som har oppstått og hvordan de har blitt håndtert. På denne måten kan flere personer i organisasjonen tilpasse seg situasjonen og håndtere lignende hendelser hvis de dukker opp senere. Denne fleksibiliteten henger tett sammen med den siste delen, som er en lærende kultur, hvor organisasjonen er opptatt av å observere, forstå og tar grep for å utbedre problemer (Reason, 1997).

3.2.4 Balansen mellom sikkerhet og produksjon

Det å ta tak i problemene, og ikke minst holde en god balanse mellom produksjon og sikkerhet er en av de mest krevende øvelsene for organisasjoner (Reason, 1997).



Figur 1: Basert på; «The Unrocked Boat» (Reason, 1997 s.5).

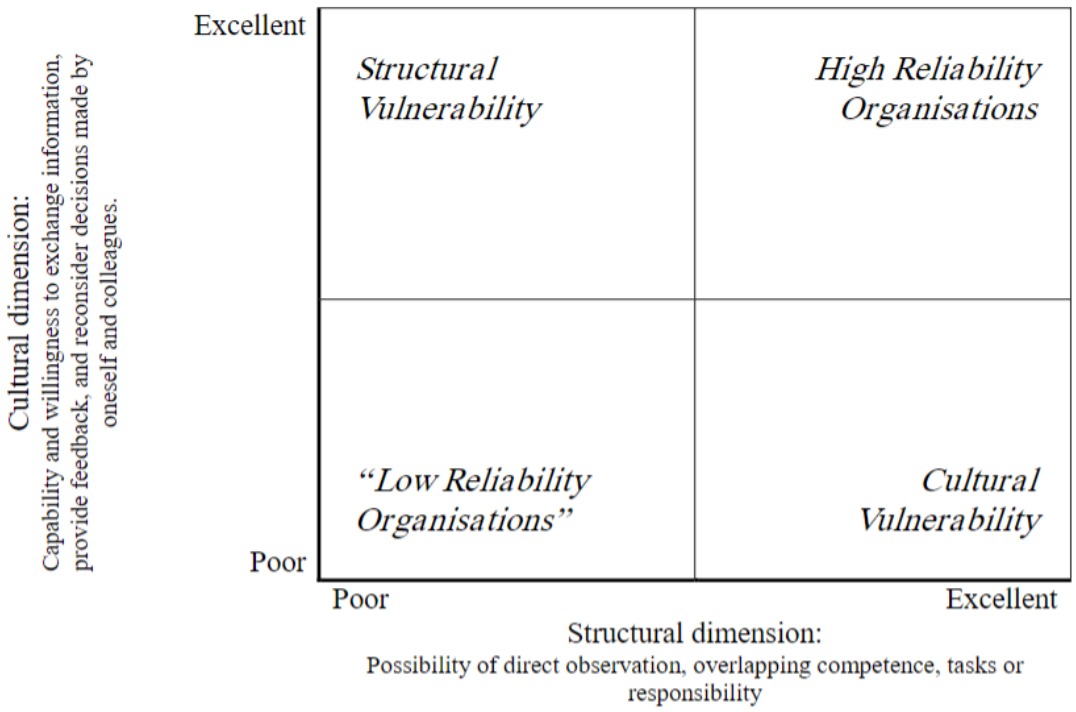
Modellen "The Unrocked Boat" av Reason viser hvordan en organisasjon må navigere mellom sikkerhet og produksjon. Jo nærmere den grønne linjen i figur 1, jo bedre er balansen mellom produksjon og sikkerhet. For mye sikkerhet vil redusere produksjonen og medføre ekstrakostnader og føre til konkurs. For lite sikkerhet vil føre til ulykker eller katastrofer og potensielt konkurs.

Reasons poeng er å illustrere hvordan mindre ulykker og uhell (illustrert i rødt) fører til økt sikkerhet som reduserer antall ulykker. Når ulykkene så er fraværende, vil organisasjonen igjen redusere sikkerheten for å øke produksjonen/profitten. Dette mønsteret gjentar seg, og man får en gradvis erodering av sikkerhetsnivået som til slutt fører til en katastrofe (Reason, 1997).

3.3 High Reliability Organizations (HRO)

Til tross for at store komplekse organisasjoner i stadig større grad anvender ny teknologi og opererer i et risikofylt miljø, så er har flere av dem en tilnærmet feilfri historikk når det kommer til store ulykker/alvorlige hendelser (Rosness mfl, 2004). De mest komplekse av disse organisasjonene, slik som atomkraftverk og hangarskip blir omtalt som High Relibility Organizations (HRO), eller høypålitelige organisasjoner. HRO-forskere, som LaPorte & Consolini (1991) observerte i sine studier av komplekse organisasjoner at man kunne benytte en organisasjonsform som bidro til å forhindre ulykker, samt oppdage og hindre feil i å utvikle seg. Denne måten å forebygge feil på er blitt betegnet som «organisatorisk redundans» (Rosness mfl, 2004, s. 30). Organisatorisk redundans har ifølge Rosness (2004) en strukturell og kulturell dimensjon, illustrert i figur 2. Den strukturelle/instrumentelle dimensjonen er basert på at ansatte/operatørene har mulighet for å observere hverandres arbeid og har delvis overlappende kompetanse, slik at de forstår oppgavene andre gjør og er i stand til å kjenne igjen feil og avvik som oppstår (Rosness mfl, 2004).

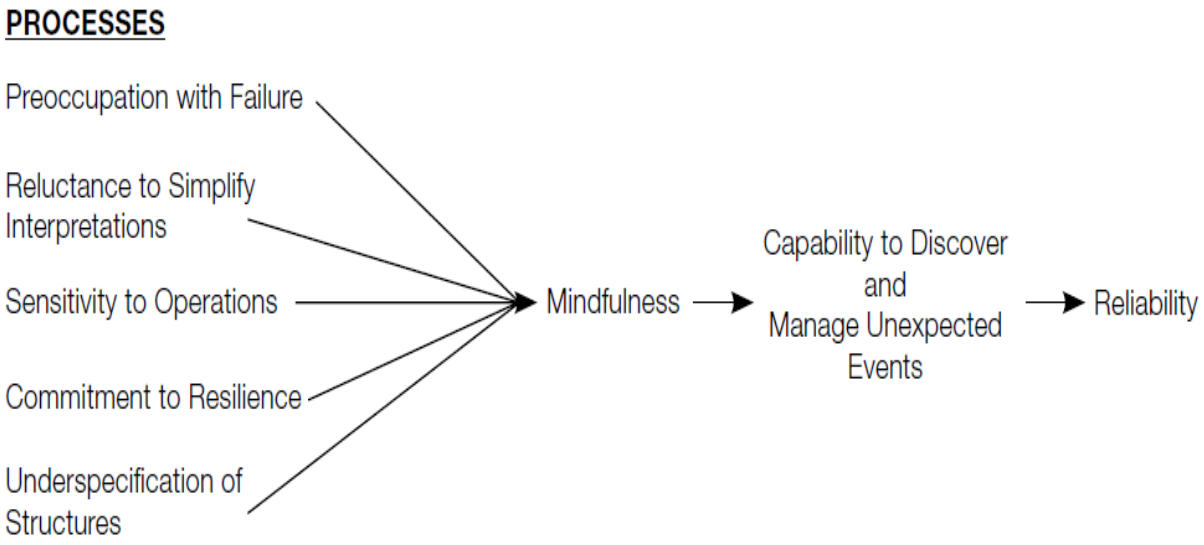
Den kulturelle dimensjonen tar for seg kulturen i organisasjonen og argumenterer for en kultur som er laget for å dele informasjon, erfaring og stille spørsmålstegn, samt trå inn og avverge potensielt farlige handlinger. Til tross for at man rapporterte andres feil og kunne overta oppgaver, så var kulturen preget av tillitt, god kommunikasjon og et felles ønske om å jobbe for sikkerhet, uten at man implementerte strenge føringer på hvordan arbeidet skulle gjøres (Rosness mfl, 2004, s. 30) (Laporte & Consolini, 1991). Kulturens betydning innen sikkerhet er også blitt fremhevet av Reason (1997) ifm. hans fokus på viktigheten av en sikkerhetskultur som legger til rette for rapportering og læring.



Figur 2: To dimensjoner ved organisatorisk redundans (Rosness mfl, 2004, s. 31)

3.3.1 Sikkerhet som resultat av «kollektiv bevissthet / Collective Mindfulness»

Fokuset på sikkerhet og høy pålitelighet i HRO-er, illustrert i den todimensjonale modellen til Rosness, figur 2 (2004) er ifølge Weick, Sutcliffe, & Obstfeld (1999) et resultat av en kollektiv bevissthet («Mindfulness») som gjennomsyrer prosessene rundt pålitelighet i organisasjonen. Pålitelighet oppnås ved å ha en bevissthet rundt sikkerhet som fører til at man kontinuerlig jobber med- og håndterer variasjoner i arbeidet. HRO-er fokuserer på avvik og håndtering av uforutsette problemer, da et pålitelig system må håndtere det uforventede, som standardiserte prosedyrer ikke fanger opp (Weick, Sutcliffe, & Obstfeld, 1999, s. 35).



Figur 3: Struktur av bevissthet for å oppnå høy pålitelighet (Weick, Sutcliffe, & Obstfeld, 1999, s. 37)

Weick, Sutcliffe, & Obstfeld (1999) peker på fem prosesser som sammen skaper en slik kollektivbevissthet, og er illustrert i figur 3. Den første er at HRO-er er opptatt av feil og avvik. Ettersom alvorlige avvik og ulykker sjeldent oppstår, er tilnærmingen til HRO-er å oppmuntre til rapportering av alle typer avvik og nesten-ulykker, samt behandle oppdagede feil som potensielle sårbarheter for hele systemet (Weick, Sutcliffe, & Obstfeld, 1999). Med en slik tilnærming til feil er det ikke noe som heter en isolert feil eller enkeltstående hendelse, men at feilene man finner kan stikke dypere og være mer kompliserte enn først antatt. (Weick, Sutcliffe, & Obstfeld, 1999, s. 39). Rapportering av egne og andres avvik, selv alvorlige tilfeller, oppmuntres da HRO-tilnærmingen her er at man bør lære av feilene fremfor at de kan gjenta seg i en annen sammenheng eller med andre personer, f.eks en nyansatt eller inkludering av en ny aktør. Videre er HRO-er bevisst på at det ved fravær av hendelser er lett å tenke at man har alt under kontroll og at etablerte rutiner er gode. En slik overdreven tro på egne rutiner kan redusere årvåkenheten og øke sjansen for ulykker (Weick, Sutcliffe, & Obstfeld, 1999).

Den andre prosessen som bidrar til kollektiv bevissthet, er at medlemmene i organisasjonen unngår å forenkle ting de observerer og slik legger merke til små ting som ellers kanskje ville gått uoppdaget. Uoppdagede feil som utvikle seg i det skjulte er en ting som Turner (1976) mener er en viktig årsak til at ulykker skjer. HRO-organisasjoner fremmer derfor et miljø med varierte

meninger i form av «menneskelig redundans», altså skepsis og kritikk av det bestående, hvilket skal motvirke konsensus og hybris i sikkerhetssammenheng (Weick, Sutcliffe, & Obstfeld, 1999).

Svært høy grad av situasjonsforståelse og årvåkenhet er også et kjennetegn på HRO-er. Denne prosessen omtales som «sensitivity to operations», og bygges internt i organisasjonen, først og fremst ved bruk av såkalt «historiefortelling» som er utveksling av informasjon og erfaringer fra tidligere situasjoner (Weick, Sutcliffe, & Obstfeld, 1999). Denne kunnskaps- og erfaringsdelingen fungerer slik som et mentalt oppslagsverk som personene i organisasjonen kan benytte for å identifisere feil eller gi mening til hvordan problemer kan løses (Weick, Sutcliffe, & Obstfeld, 1999).

Den fjerde prosessen er fokuset på resiliens. Resiliens blir definert av Wildavsky (1991, s.77) som *«evnen til å håndtere uforventede farer etter de ha manifestert seg»*, som også skiller mellom å være resillient og det å være forutseende, altså å forvente og forhindre uønskede hendelser (Wildavsky, 1991). Dette skillet mellom før og etter en hendelse har inntruffet er noe som skiller HRO-er fra andre organisasjoner med at de i større grad øver på å håndtere det uventede, fremfor den mer tradisjonelle tilnærmingen med å forhindre og avverge allerede kjente farer (Weick, Sutcliffe, & Obstfeld, 1999, s. 46). HRO-er erkjenner altså at de ikke kan avverge alle farer og ulykker, og prioriterer derfor både forebyggende tiltak og begrensende tiltak (Weick, Sutcliffe, & Obstfeld, 1999). Resiliens i HRO-er er ifølge Weick, Sutcliffe, & Obstfeld (1999) også relatert til deres naturlige skepsis med at de *«ikke tar for gitt at tidligere erfaringer alltid representerer et korrekt bilde når en ny fare oppstår»* (Weick, Sutcliffe, & Obstfeld, 1999, s. 47).

Den femte prosessen som bidrar til å skape kollektiv bevissthet i HRO-er er løse strukturer i organisasjonen. Den løse strukturen gjør at flere mindre deler av organisasjonen er involvert i helheten, noe (Weick, Sutcliffe, & Obstfeld, 1999, s. 48) referer til som *«Garbage Can»-systemet*. Denne måten å organisere på gir fordeler som det å motvirke hierarkiske strukturer til fordel for kompetanse og kunnskap (Weick, Sutcliffe, & Obstfeld, 1999). Ved å la flere nivåer i organisasjonen ta del i beslutninger, klarer HRO-er i større grad å dra nytte av et større spekter av løsninger og erfaringer som kan benyttes på nye problemer (Weick, Sutcliffe, & Obstfeld, 1999).

Selv om HRO-er kontinuerlig jobber for økt sikkerhet gjennom en felles bevissthet og prioriterer dette arbeidet, så er de også ofte underlagt krav om effektivisering, konkurransedyktighet og å finne balansen mellom kontroll og tillitt. HRO-er prøver derfor i stor grad å lære av andres feil og

skape analogier til egen organisasjon, slik at de selv slipper å eksponere egne systemer og eventuelle tap, fremfor å benytte en mer tradisjonell «øve og feile»-tilnærming (Weick, Sutcliffe, & Obstfeld, 1999, s. 54). HRO-er baserer mye av sin tilnærming til sikkerhet på en kollektiv bevissthet og et felles verdisett som medlemmene i organisasjoner bekjenner seg til.

Viktigheten av sikkerheten er altså i stor grad basert på en kulturell og sosial anerkjennelse. En moderne utvikling med økt kompleksitet og større grad av outsourcing representerer imidlertid også en utfordring for HRO-er (Weick, Sutcliffe, & Obstfeld, 1999). Outsourcing av tjenester og vedlikehold, samt at mer spisskompetanse ligger utenfor organisasjonen skaper flere potensielle sårbarheter (Weick, Sutcliffe, & Obstfeld, 1999). De viktige fem prosessene som skaper pålitelighet iht HRO-teorien, står da i fare for å «vannes ut» med mindre underleverandørene er like opptatt av feil og pålitelighet som kjøperen av tjenestene. Arbeidet med å bygge og vedlikeholde den kollektive bevisstheten rundt sikkerhet blir derfor stadig mer utfordrende, også for HRO-er.

3.4 Man-made Disasters / Informasjonssviktperspektivet

Et perspektiv som omhandler informasjonsflyten innad i organisasjoner og dens påvirkning på ulykker og uønskede hendelser er Barry Turner sin teori om «Man-made Disasters» (Turner, 1976). I henhold til dette perspektivet, gjerne kjent som informasjonsprosesseringsperspektivet, er forståelsen av tilgjengelig informasjon og viktigheten av å formidle denne innad i organisasjonen sentral (Rosness mfl, 2004). Fremfor å fokusere på kausale årsaksfaktorer rett forut hendelsen, så er Turner opptatt av prosessen som var forut for ulykken. Ulykken er altså en konsekvens av andre mindre hendelser/prosesser som har pågått, gjerne over lang tid, en periode Turner (1976) omtaler som «inkubasjonsfasen.

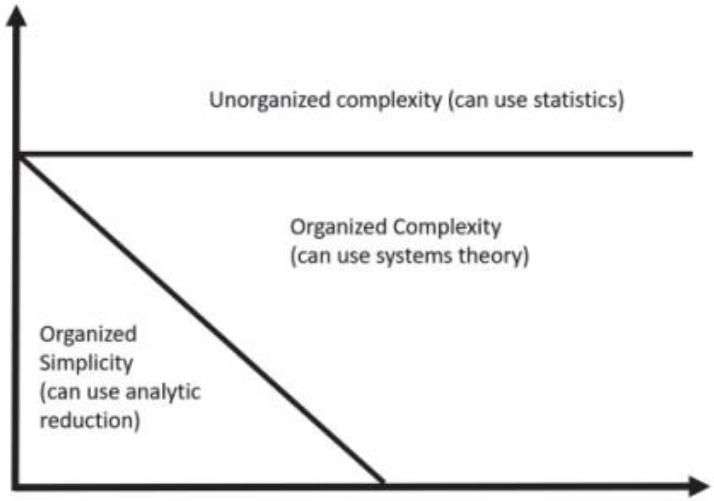
Turner hevder at i inkubasjonsfasen er avvikene enten skjult og ukjent for alle i organisasjonen eller så forstår man ikke sammenhengen og trusselen før ulykken er ute. Et moment som kan føre til at man ikke ser sammenhenger før en ulykke skjer, er at flere parter i ulike deler av en stor og kompleks organisasjon sitter på hver sin bit av informasjonspuslespillet. Dette bidrar til at de forstår risikoer og faresignaler ulikt basert på sin «versjon» av informasjon, som de ikke får delt med andre (Turner, 1976).

Andre organisatoriske årsaker som bidrar til dårlig informasjonsflyt kan være organisasjonens egen risikopersepsjon, altså deres egen oppfattelse av muligheten til at ulykker kan oppstå. Turner peker på rollen til organisasjonskultur og at det kan oppstå «blindsoner» dersom organisasjonen sitter på en forståelse av at alt er på stell (Turner, 1976). Gamle, ukjente eller uklare prosedyrer kan ifølge dette perspektivet ytterligere bidra til at ansatte i organisasjonen blir usikre på hvordan de skal forholde seg til informasjon og kan forverre en allerede dårlig informasjonsflyt (Rosness mfl, 2004), (Turner, 1976).

En av ulempene med store og komplekse organisasjoner at de genererer større mengder informasjon ifm. oppgaveløsning. Dette kan gjøre det vanskelig å skille ut hva som er relevant informasjon for å unngå ulykker, og forsterkes ytterligere av at enheter i organisasjonens struktur ha ulik risikoforståelse, sikkerhetskultur og ulikt rammeverk (Turner, 1976).

3.5 Systemteori

Med stadig flere systemer, deler og potensielt mange interaksjoner mener enkelte teoretikere at man i større grad bør se på helheten i systemet, fremfor enkeltdeler, altså ha et systemisk perspektiv. I henhold til tradisjonell systemteori kan man dele systemer inn i en typologi basert på organisering og kompleksitet med hver sine karakteristikker. Disse tre systemene er illustrert i figur 4 (Leveson, 2011).



Figur 4: «Systemtypologi» (Leveson, 2011, s. 62)

«Organized simplicity» er systemer som kan brytes ned i enkeltdeler og analyseres hver for seg, typisk for tradisjonell deduktiv metode. Komplekse systemer som mangler underliggende strukturer, men som kan analyseres gjennom statistisk metode omtaler Leveson som «unorganized complexity».

Det som gis mest oppmerksomhet er omtalt som «organized complexity», altså organisert kompleksitet. Denne typen system er (..) *«for stort og for komplekst til å brytes ned i enkeltdeler og for organisert til å undersøkes gjennom statistikk»* (Leveson, 2011, s. 63). Leveson argumenterer for at det er hensiktsmessig å bruke system- og hierarkisk teori for å analysere systemene som har organisert kompleksitet. Systemteori har en helhetlig tilnærming og hierarkisk teori ser nærmere på hvordan forholdet er mellom de ulike systemene, og hvordan deler, aktører og nivåer innad i systemet påvirker hverandre (Leveson, 2011).

Nivåene i hierarkiet får *utspringende egenskaper* («emergent properties») når de når et visst kompleksitetsnivå (Leveson, 2011).

Ettersom sikkerhet er en avledet egenskap av et system er det viktig å se på systemet for å analysere funksjonene, prosessene og kontrollmekanismene knyttet til sikkerheten. Kommunikasjon er her en forutsetning for å utøve god kontroll. Det må dessuten være et *mål* med kontrollen, som å opprettholde en funksjon. Videre er det nødvendig å ha kontroll på *handlinger*, slik at man kan påvirke situasjonen, og en modell som man jobber med og at man kan *observere* systemet for å sjekke om det fungerer slik det skal (Leveson, 2011).

Velfungerende system og evne til å beholde kontroll krever kontinuerlig og god tilbakemelding gjennom gode feedback loops. Tap av kontroll, ulykker og uønskede hendelser er iht. dette perspektivet resultater av dårlig kommunikasjon og systemer med svake feedback loops. For å analysere kommunikasjonsflyten og hvordan dette påvirker systemet som helhet, er det viktig å se utover enkeltdeler, og i et sosioteknisk system (Leveson, 2011).

3.5.1 STAMP: Systems-Theoretic Accident Model and Processes

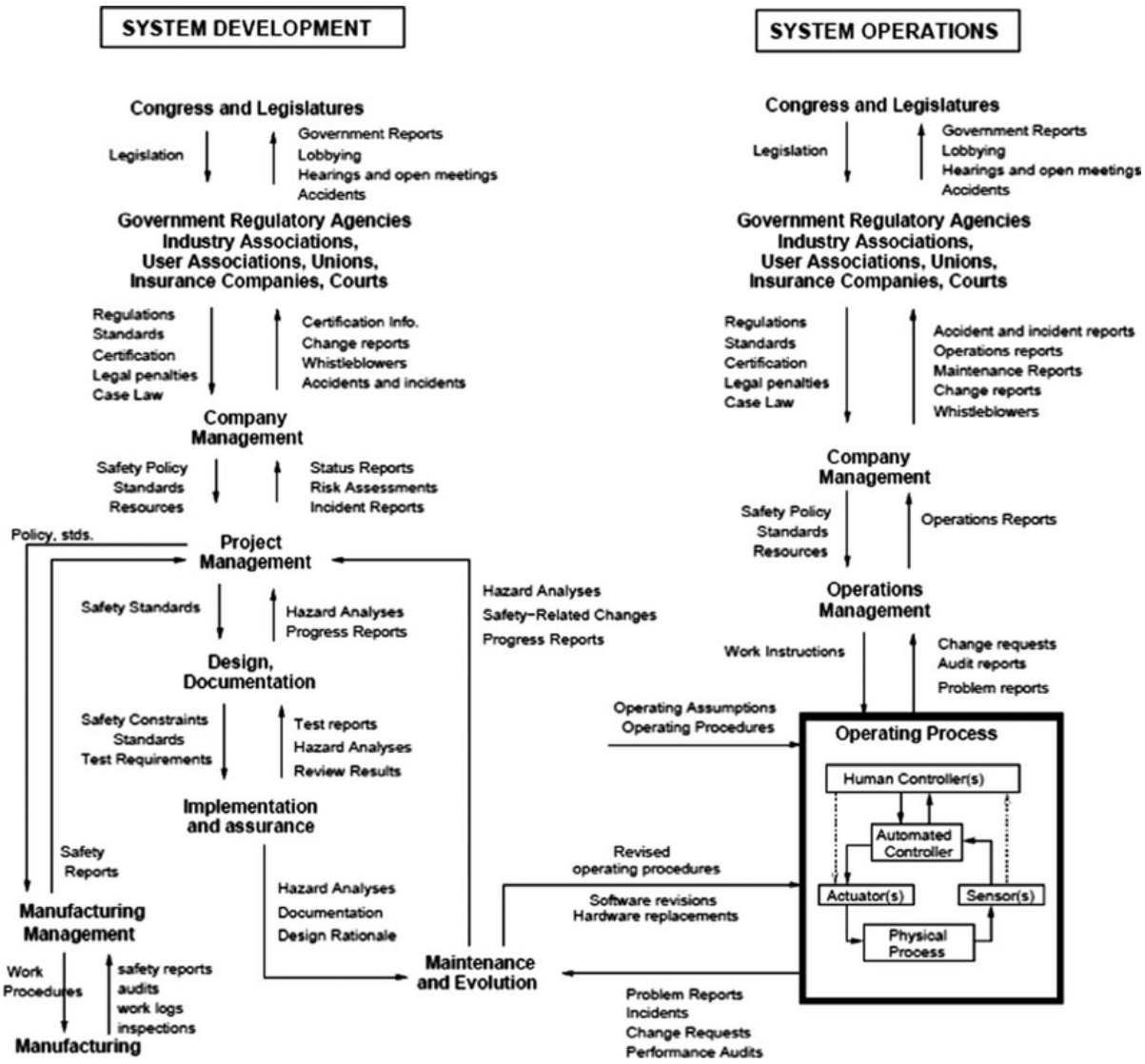
Leveson (2011) introduserer en ny ulykkesmodell basert på systemteori. Teorien forkortes STAMP og står for Systems- Theoretic Accident Model and Processes. Modellen har fokus på adferd som skal sørge for sikkerhetsbegrensningene og et systemblikk. Denne ulykkesmodellen

fokuserer på tre hovedmomenter som består sikkerhetsbegrensninger (contraints), hierarkiske kontrollstrukturer og prosessmodeller (Leveson, 2011).

Leveson definerer i forbindelse med denne modellen, en ulykke som: *«en ulykke er en ikke-planlagt og uønsket hendelse som fører til tap»* og presiserer at selv om metoden er safety-orientert, så kan *tap i denne sammenhengen også kan omfatte finansielle tap eller informasjonstap.* (Leveson, 2011, s. 75)

STAMP har fokus på at de utspringende egenskapene som følge av økt kompleksitet kontrolleres av sikkerhetsbegrensninger. Sikkerhet iht. STAMP blir da et spørsmål om kontroll, som kan håndteres av gode prosedyrer, menneskelig adferd, ledelse og styring, men også kulturelle og organisatoriske faktorer. Dette kontrollfokuset består også etter at en ulykke har skjedd. Iht. STAMP er det av særlig interesse hvorfor kontrollen over en sikkerhetsbegrensning sviktet, og at denne kontrollen kan ha flere ulike årsaker (Leveson, 2011).

Leveson argumenterer for en helhetlig tilnærming for å etablere og håndheve sikkerhetsbegrensningene. Det blir da nødvendig å se på sikkerhetsstyring i et sosioteknisk perspektiv og at alle de ulike nivåene engasjeres i å håndheve sikkerheten (Leveson, 2011). For at sikkerhetsarbeidet skal fungere optimalt i en slik modell bør ansvaret for de forskjellige system-sikkerhetsbegrensningene fordeles til ulike grupper og nivåer slik at man får effektiv styring basert på ressurser, kompetanse og kjennskap til sikkerhetsbegrensningene (Leveson, 2011) En annen av de sentrale delene i STAMP er hierarkiske kontrollstrukturer, noe hun illustrerer i sin sosiotekniske kontrollmodell.



Figur 5: Sosioteknisk modell av kontroll ifm. STAMP (Leveson, 2011, s. 82)

I en sosioteknisk modell, med flere aktører, nivåer og prosesser er det avgjørende at det foreligger god kommunikasjon. God kommunikasjon forutsetter et system med velfungerende feedback, slik at de ulike nivåene kan justere sikkerhetsbegrensningene etter hvert som situasjonen endrer seg (Leveson, 2011). Som figur 5 viser så er den sosiotekniske modellen til STAMP delt opp i to «søyler», en for systemutvikling og en for operasjoner (Leveson, 2011). Knytningen mellom de to søylene viser viktigheten av at feedback ikke bare må gå opp- og nedover i hver sin del, men også på tvers, slik at alle deler av det sosiotekniske systemet kommer med.

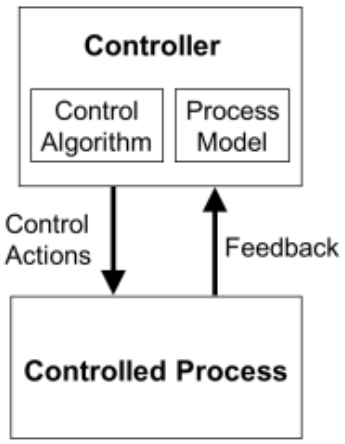
Feedback fra operasjonsdelen har konkret påvirkning på systemutvikling, slik at man kan forbedre eller justere underveis, og rammebetingelsene i utviklingssøylen påvirker hvordan operasjoner og

instrukser skal gjennomføres mm. Dette forutsetter imidlertid at det finnes mekanismer som gjør at informasjonen ikke stopper opp, men flyter godt mellom de to respektive søylene (Leveson, 2011). Mangel på slik feedback utgjør et betydelig sikkerhetsproblem, da manglende informasjon om feil, nødvendige justeringer, farer, reell status eller svake prosedyrer osv. fører til mangel på kontroll, slik at man mister kontrollen over sikkerhetsbegrensningene som må fungere for å hindre ulykker.

Selv om de implementerte prosedyrene og sikkerhetsrutinene er gode, så vil manglende kunnskap om hvorvidt de følges opp eller hvordan de fungerer i praksis, være av kritisk betydning om hvorvidt de faktisk bidrar til økt sikkerhet. Forsinkelser i systemet eller som følge av utvikling av formelt rammeverk fører til at systemet havner bakpå og ikke henger med i den teknologiske utviklingen. Utarbeidelse av internasjonale standarder (eksempelvis ISO-standarder eller felles rammeverk) kan ta lang tid, og kan i verste fall være utdatert når det er klart (Leveson, 2011)

Forsinkelser i systemet kan delvis motvirkes ved å delegere ansvar ned i de lavere nivåene, da disse menneskene her gjerne er tettere på prosessene. Skal delegering i det sosiotekniske systemet fungere, så poengter Leveson at det formuleres konkrete og klare målsetninger, samt at kommunikasjonen fungerer flyter godt mellom nivåene (Leveson, 2011).

Den siste delen i STAMP-modellen er det Leveson kaller «Prosessmodeller», altså en modell som en operatør eller et automatisert system kan forholde seg til, og som kan avleses og justeres fortløpende, etter feedback fra systemet. Leveson hevder at «*ulykker, spesielt dem som er en del av komplekse systemer, oppstår når det er avvik mellom prosessmodellen som benyttes av operatøren og prosessen som foregår*» (Leveson, 2011, s. 88)

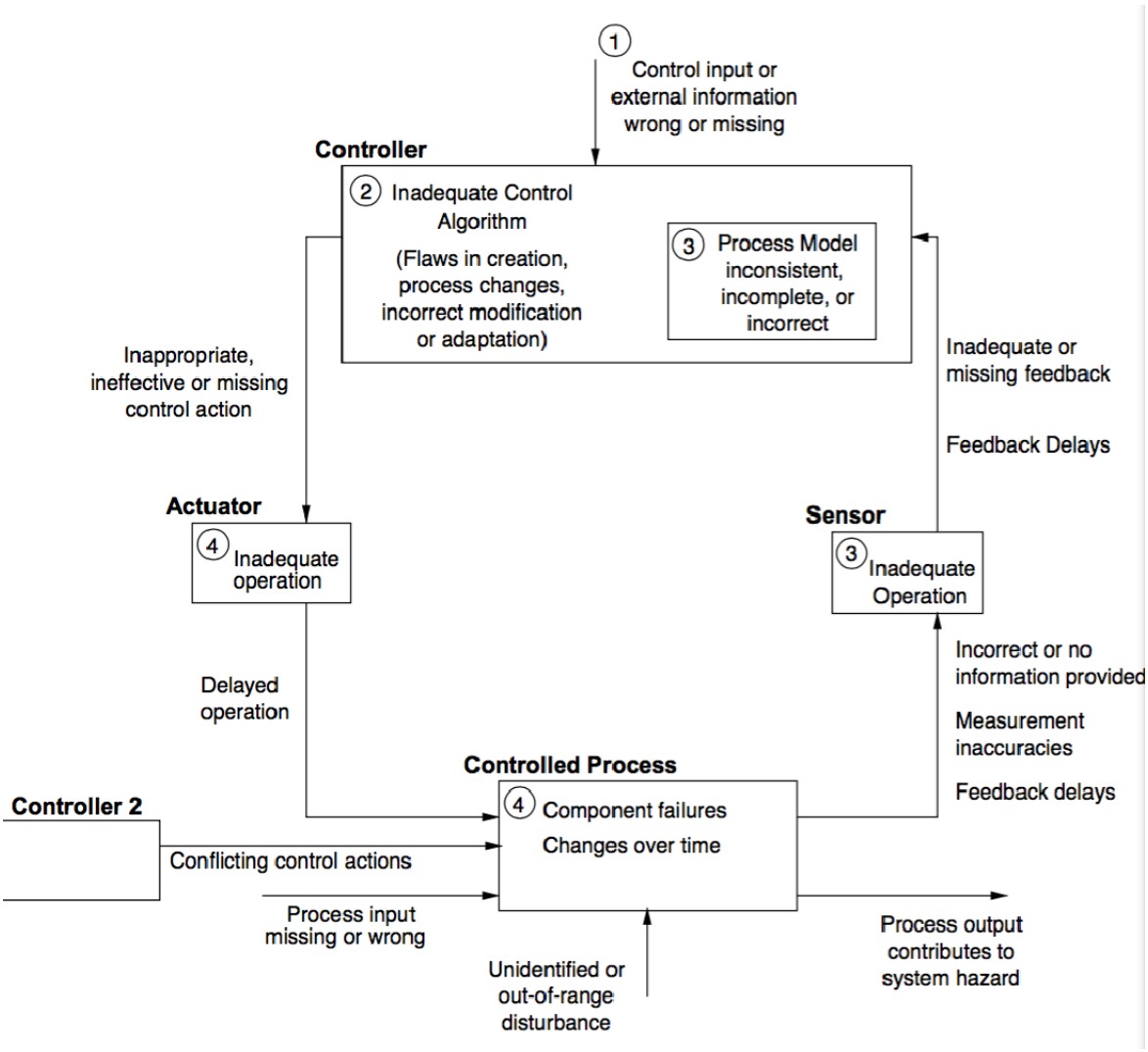


Figur 6: «Kontrollsløyfe (*Control Loop*)» (Leveson & Thomas, 2018, s. 23)

Kontrollsløyfen i figur 6 viser at feedback fra den kontrollerte prosessen er viktig for å velge riktig prosessmodell, som igjen er utslagsgivende for hvilke handlinger som operatøren velger (Leveson & Thomas, 2018). Feedback fra prosessen(e) som kontrolleres må nå alle deler av organisasjonen, slik at alle nivåer har riktig informasjon og kan ta korrekte beslutninger og kontrollhandlinger (Leveson, 2011). De ulike delene og nivåene av organisasjonen må involveres i sikkerhetsarbeidet, til tross for at de har ulike roller og er plassert på ulike nivå. Det er denne helhetlige tilnærmingen og delingen av informasjon som fremheves som kritisk for å ivareta sikkerheten iht. STAMP.

3.5.2 Kausalitet og årsaksforklaringer iht. STAMP

Det systemiske fokuset i STAMP gjør tilnærmingen relativt omfattende og detaljert, særlig gjelder dette når man ser på årsakssammenhenger i det sosiotekniske systemet. Leveson mener at årsakssammenhenger ofte blir forenklet og man ikke tar nok hensyn til at det er mange ulike bakenforliggende årsaker, samt interaksjoner som fører til ulykker (Leveson, 2011).



Figur 7: *«Klassifisering av kontrollfeil som fører til ulykker»* (Leveson, 2011, s. 93)

Figur 7 viser årsaker til kontrollfeil som fører til systemfarer. Informasjonen som ligger til grunn for å kontrollprosessene kan være mangelfulle eller fraværende helt fra start eller som grunnlag for design av selve systemet. Kontrollhandlingene som foretas, enten av maskiner eller mennesker blir da sårbar for systemiske feil (Leveson, 2011).

Flere aktører i prosessen kan så operere systemet ulikt og kan tilføre det ulik og motstridende kommandoer. Dette fører til feil kontroll samt forsinkelser i systemet, som igjen vil påvirke kontrollprosessen (som sørger for sikkerheten ivaretas) negativt og det kan oppstå en farlig eller uønsket situasjon i systemet som resultat. God feedback er da kritisk for å gjøre nødvendige endringer for å unngå ulykker. Skal dette fungere må det eksistere velfungerende feedbackkanaler, slik at informasjonen kommer effektivt og raskt frem til de som trenger den på andre nivåer i det

sosiotekniske systemet. Manglende feedback kan komme av en slik funksjon ikke er designet inn i systemet eller at informasjonsflyten er dårlig pga. dårlige kanaler eller relatert til sikkerhetskulturen i organisasjonen (Leveson, 2011) (Leveson & Thomas, 2018).

Kommunikasjon og klare roller er en forutsetning for å opprettholde god kontroll over sikkerhetsarbeidet. Flere aktører og manglende koordinasjon mellom disse, samt overlappende ansvarsområder kan føre til tvetydigheter og interaksjoner som har potensiale til å forstyrre sikkerhetsstyringen (Leveson, 2011).

Menneskers adferd og handlinger er påvirket av informasjonen som flyter rundt i systemet, men en annen viktig faktor er arbeidsmiljøet og konteksten mennesket jobber i. Et organisatorisk forhold som da kan påvirke kommunikasjonen er blant annet «*avstanden mellom nivåene og eksistensen av mange ulike avdelinger som skiller de ansatte og ledelsen*» (Leveson, 2011, s. 100).

Arbeidsmiljøet har også påvirkning på mennesket og menneskets rolle i ulykker (Reason, 1997). Mennesker og holdninger, på lik linje med teknologi, endrer seg over tid, noe som gjør det ekstra viktig at systemet er fleksibelt og kan justeres i takt med slike endringer og for å ivareta systemets sikkerhetsfunksjon (Leveson, 2011)

Leveson hevder at den sosiotekniske tilnærmingen gjør det mulig å se på hver enkelt del i systemet for å finne ut hvordan de påvirker helheten, og hvordan systemet som helhet har bidratt til at ulykken kunne skje. STAMP som analysemetode er hensiktsmessig i nye komplekse systemer med flere interaksjoner. Den ser også på menneskelige, organisatoriske og teknologiske faktorer, noe som ytterligere bidrar til et mer dekkende helhetsbilde (Leveson, 2011).

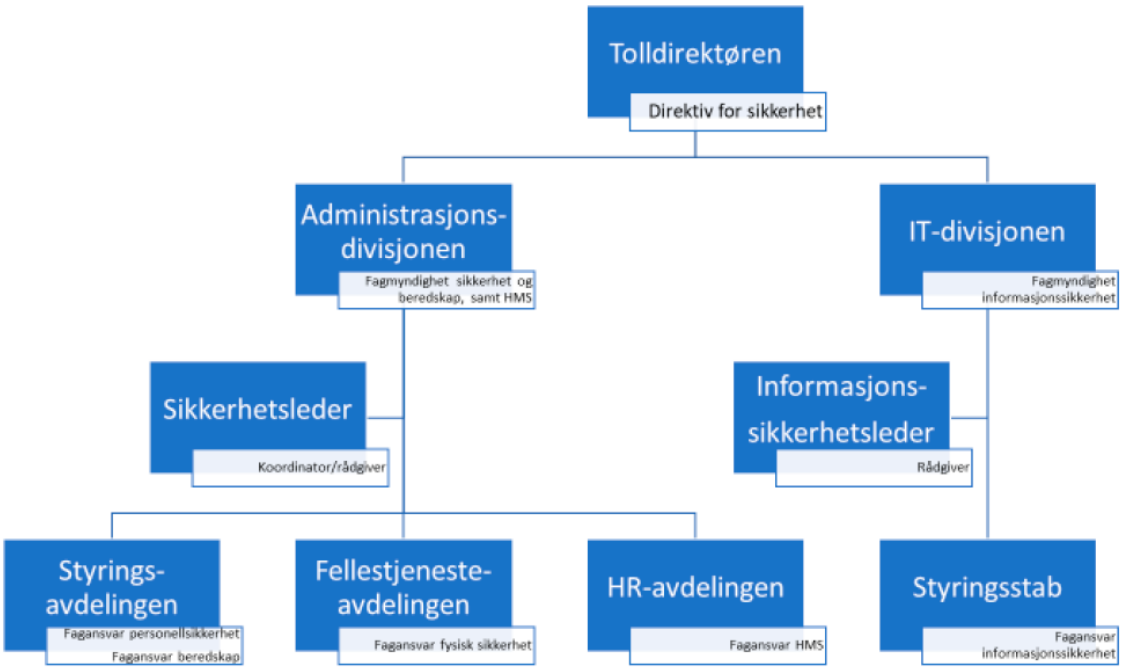
4. Empiri:

4.1 Beskrivelse av forskingsprosjektets empiri

Empirien er basert på kvalitative intervjuer av personer som har sikkerhet og informasjonssikkerhet som ekspertise eller som omgås sikkerhetsrelaterte problemstillinger i sitt daglige arbeid. Empirikapittelet er organisert slik at funnene presenteres tematisk.

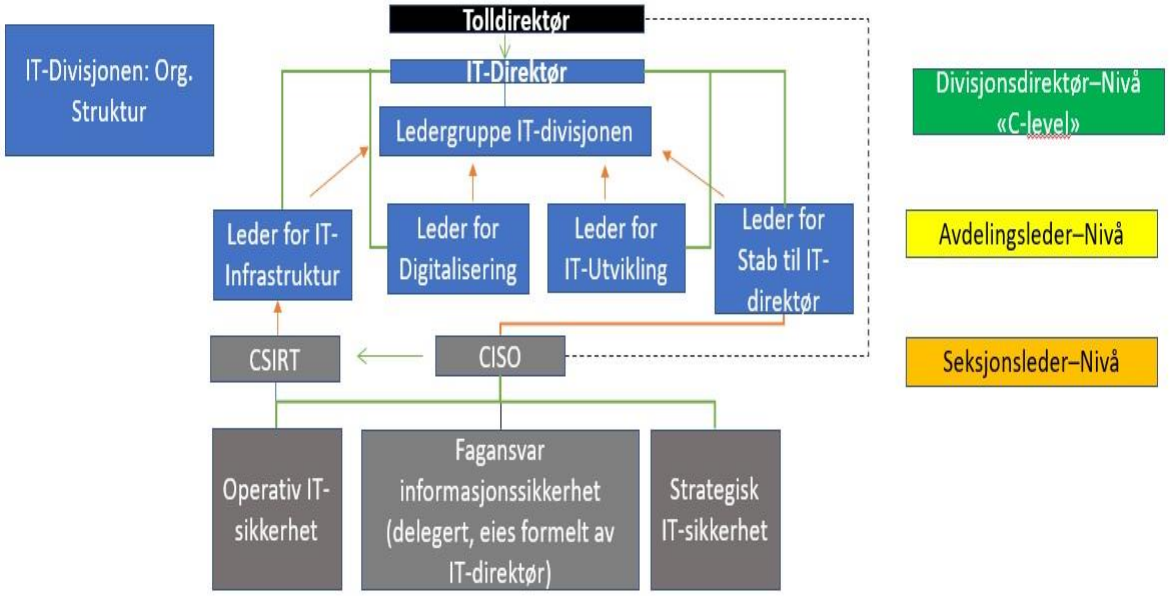
4.2 Organisering og samhandling

Tolletaten har i dag delt sikkerhetsstyringen i to ulike divisjoner i organisasjonen. Personellsikkerhet, fysisk sikring, beredskap og HMS er lagt til Administrasjonsdivisjonen, mens informasjonssikkerhet er lagt til IT-divisjonen. Organiseringen av Tolletatens sikkerhetsarbeid er vist i figur 8, som tydelig viser et skille mellom divisjonene og deres underliggende ansvarsområder. Man ser her at sikkerhetsleder og informasjonssikkerhetsleder er under to ulike divisjoner.



Figur 8: Organisasjonskart over Tolletatens sikkerhetsorganisering (Tolletaten, 2020)

Som man kan se ut fra figur 9, så har Tolletaten videre organisert informasjonssikkerhetsarbeidet i to blokker i IT-avdelingen, med CISO (informasjonssikkerhetsansvarlig) plassert i styringsstaben til divisjonsdirektøren under egen stabsleder, mens operasjonell sikkerhet (hendelseshåndtering og sikkerhetsarkitektur) ligger i infrastrukturavdelingen. Informasjonssikkerhetsarbeidet er altså delt, med strategisk ansvar hos CISO i styringsstab og operasjonelt ansvar i en annen avdeling (infrastrukturavdelingen)



Figur 9 Dagens Org.struktur i IT-divisjonens basert på informanten og Tolletatens org.kart (Tolletaten, Informant IT-2).

De grønne pilene i figur 9 representerer instruksjonsmyndighet eller ansvar. Man ser f.eks. at CISO til en viss grad kan instruere CSIRT-teamet, men har rød pil til sin egen leder i styringsstab. Det samme gjelder for CSIRT som rapporterer til sin respektive leder i infrastrukturavdelingen. De ulike avdelingslederne møtes i ledergruppen og rapporterer der til IT-direktøren. I dagens organisering er CISO altså ikke direkte involvert i beslutninger som tas i ledergrupper, men har som figuren viser, en stiplet linje til Tolldirektør. Dette er for å ha en «bakdør» til Tolldirektøren som er den eneste som kan instruere IT-direktør, dersom det trengs spesielle avklaringer.

4.2.1 Informasjonssikkerhetsansvarlig bør ha en tydelig rolle og myndighet:

Noe som opptar samtlige informanter med IT-bakgrunn, er viktigheten av klare roller og hvem som har myndighet når det kommer til spørsmål om informasjonssikkerheten i virksomheten. Flere av informantene viser til at det i dag er blitt vanligere å ha en egen informasjonssikkerhetsleder (CISO) i virksomheten, men at den organisatoriske plasseringen av rollen varierer.

K-2 understreker at han ofte ser det han mener er feil plassering av CISO. Han er veldig klar på at det er viktig med en høy organisatorisk plassering av CISO. *«CISO bør være på samme linje/nivå som IT-sjefen og CFO. Personen må ha en myndighet og autoritet i bedriften som gjør at den personen kan påvirke og ta avgjørelser som har noe å si for hele bedriften»*. Informanten forteller videre om en case hvor (…):«*Sikkerhetssjef/CISO var plassert under en administrasjonssjef som hadde administrative oppgaver, som f.eks. bygningsmasse, sitteplasser osv. altså rene administrative oppgaver. Dette kunne føre til en konflikt fordi når f.eks. CISO kom og sa at det var nødvendig med tiltak som kanskje gikk utover den administrative delen og måten de jobbet på, så kunne lederen bare si nei, og det var det»*. I henhold til informanten så en slik plassering føre til en interessekonflikt, som kunne være tegn på feil plassering.

Synligheten av CISO i virksomheten og myndigheten er noe som også informant K-1 tar opp. *«En plassering høyt oppe gir sikkerhet mer tyngde og en tydeligere stemme. Det vil også føre til at CISO alltid er til stede på møter og briefes, samt får muligheten til å gi brief. Det at ledelsen gir taletid til sikkerhetsarbeidet mener jeg er viktig. Sikkerhet kommer slik tydeligere frem enn om man sitter lengre ned i organisasjonen»*. K-2 understreker igjen at (…) *«det er viktig at CISO sitter i ledergruppen, det gjør han i alle selskaper i dag, da informasjonssikkerhet blir mer og mer viktig»*.

4.2.2 Svekket gjennomslagskraft ved feil plassering av CISO.

Informantene virker svært samstemt i at plasseringen av CISO er viktig i forbindelse med god styring og effektivt informasjonssikkerhetsarbeid. Selve plasseringen av CISO i Tolletaten er også noe som opptar de interne informantene. Skillet mellom strategisk og operativ del, og at CISO ikke er en del av ledergruppen er noe informant IT-1 mener er uheldig. Når CISO ikke er en del av ledergruppen mener noen av informantene at gjennomslagskraften blir svekket ved at han må søke godkjenning av nyskrevne policyer hos sine overordnede, og dermed er sårbar i et hierarkisk system: (…): «*det er litt spesielt at CISO er utenfor ledergruppen, med tanke på at CISO er den*

som på papiret har øverste myndighet med tanke på det som kommer til informasjonssikkerheten, utenom divisjonsdirektøren». «I dag så har CISO en leder mellom seg og lederen av IT-divisjonen. Det vil si at han har et ekstra ledd å gå igjennom, før han komme opp til nærmeste leder igjen som er den tar avgjørelser, som omfatter alt som har med direkte it-sikkerhet å gjøre. Det vil si at CISOs leder, og nærmeste leder der igjen, må da være bedre enn CISO på sikkerhet, for å vurdere om forslaget til en ny prosedyre er godt».

Informant IT-1 understreker igjen at han mener dagens plassering er feil og heller ser for seg en alternativ organisering: (…) «CISO burde jo egentlig vært en lederfunksjon. Gjennomslagskraften til en leder på nivå tre er mye større enn en mellomleder på nivå 4 eller 5» (IT-1). Andre virksomheter har jo en CSO, Chief Security Officer, en totalsikkerhetsleder med CISO under seg igjen. En CISO som har ansvar for både operative og strategiske sikkerhetstiltak. Altså CISO leder alt som har med IT og sikkerhet å gjøre»

K-2 er i motsetning til den interne informanten, IT-1 skeptisk til å ha én og samme enhet for både strategisk og operativ sikkerhet. *«IT-sjefen skal jo ha et operativt ansvar. En IT-sjef skal tenke operativt, altså hvordan bruker man informasjonsteknologi i bedriften og følge bedriftens mål, mens en CISO skal tenke hvordan man sikrer bedriftens verdier i den digitale verden og hvordan gjøre dette på best måte, og da på et overordnet nivå. De som gjør dette best er de som har én som tenker strategi, og så har de én som setter strategien ut i handling, altså operativ virksomhet» (K-2).*

4.2.3 Politisk styring og byråkratiske utfordringer

Arbeid med informasjonssikkerhet og fysisk sikring foregår ikke et vakuum i virksomhetene. Som del av en større organisasjon, og samfunnet generelt påvirkes sikkerhetsarbeidet av interne og eksterne faktorer som politikk og andre myndigheter.

IT-2 nevner at som i mange andre store statlige organisasjoner så kreves det evne til å manøvrere i byråkratiet. Til tross for at ansvaret for informasjonssikkerheten i Tolletaten er delegert til CISO, finnes det organisatoriske utfordringer. *«(…) det som går igjen er byråkratiet. Selv om CISO er gitt fagmyndighet på et område så er det ikke bare å utforme en instruks og smelle den i bordet. Man må ha med seg mange interessenter, man må snakke med alle som blir påvirket av den, sånn at den har en effekt. Ellers blir den en papirtiger, et fint dokument, men som ingen følger og forholder seg til. Den jobben, med å få andre interessert i dokumentet og forankre det, kan være*

nok være utfordrende for mange. Man må være frempå og by på seg selv og ta kontakt med de aktørene det gjelder» (IT-2).

Informanten i Equinor, EQ1 trekker også frem politisk styring og påvirkning om en utfordring. Informanten viser blant annet til at sikring av installasjoner i noen tilfeller har gått på bekostning av det han mener er lokalpolitiske interesser: (…) *«når man skulle sikre et anlegg her i Norge, så var enkelte mest opptatt av å ikke skade hjorten i området. Den lokale ordføreren ville derfor ikke ha piggtråd på toppen som et sikkerhetstiltak, så da skjedde det ikke!» (EQ1).*

Evnen til å implementere sikkerhetstiltak raskt og effektivt bør ifølge noen av informantene ikke hindres av politikk som går på tvers av fagmiljøene: (…) *«det er frustrerende at det ikke lyttes mer til fagmiljøene. De kommer med en anbefaling om en vei fremover og så kommer politikere, snakker litt ullent og overprøver anbefalingen. Det virker nesten som om det er viktigere å blidgjøre enkelte lenger inn i systemet … det er noe som bekymrer meg» (EQ1).*

Flere av informantene peker på strukturelle utfordringer på myndighetsnivå, og at dette fører til at beslutninger tar det informantene mener er unødvendig lang tid. Utfordringene knyttes til lav bemanning og liten fleksibilitet i hvem som kan ta avgjørelser på myndighetssiden.

Informant EQ2 viser til at de opplever at Equinor som organisasjon selv må ta ansvaret og gjøre tiltak internt mens de venter på myndighetene: (…) *«myndighetene bremser på en måte ting. Det tar for lang tid»*. EQ1 understreker at imidlertid at: (…) *«når myndighetene først er kommet på banen så blir det bra, men det kan oppstå uønskede tilfeller pga. ulike vaktordninger i departementene at man ikke får tak i f.eks. en jurist ifm. bistandsanmodning osv. Når du står i krisen, så trenger man hjelp der og da. Man kan ikke vente til mandag når det kommer en jurist på jobb*».

4.3 Informasjonsflyt internt i organisasjonen

Alle informantene mener det er en forutsetning for sikkerheten at informasjonsflyten fungerer. Enten de befinner seg på gulvet, IT-området eller jobber med informasjonssikkerhet direkte, så er gjengangeren at det er avgjørende å få informasjon. Enkelte av informantene peker på at det er viktig å kunne være i stand til å forstå det som blir formidlet og vite hvor man kan henvende seg for ytterligere informasjon.

4.3.1 Informasjonsflyten rundt informasjonssikkerhet

A3 opplever at informasjonsflyten rundt IT-sikkerhet fungerer, men påpeker at *«fagartikler kan være litt sånn stammespråk som neppe leses av mer enn et par stykker»,* men at andre ting som *«enkle påminnelser på intranettet er lettere å forstå, noe som jeg tror er viktig»*.

Informant A4 er enig i at *«påminnelser for vanlige ansatte utenfor IT-avd. er lurt»,* men poengterer at *«selv om informasjonen kommer ut på nettet, så er det jo opp til den enkelte å trykke på og lese artikkelen»* Informanten mener at det ikke er noen kontrollfunksjon her og at man ikke har noen garanti for at dette folk faktisk tar seg tid å lese seg opp.

Hele gruppen opplever at budskapet om at informasjonssikkerhet er veldig viktig, og er tydelig formidlet via digitale kanaler i organisasjonen, spesielt i form av jevnlige innlegg på intranettet. Det er imidlertid ulike rutiner lokalt når det gjelder behandling av data og A3 spekulerer i at hens avdeling kanskje har *«ekstra strenge rutiner siden vi har en sånn informasjonssikkerhetsfyr på avdelingen og han er veldig opptatt av sånne ting, og passer på at det gjøres skikkelig»*.

Informant A1 påpeker at *«kommunikasjonen fra CSIRT (Computer Security Incident Response Team) har gjort det lett å rapportere feil og å få nyttig informasjon, så det med IT funger fint»*.

4.3.2 Informasjonsflyten rundt Safety:

Dagens organisering innebærer at Safety-arbeidet i Tolletaten er organisert i Administrasjonsdivisjonen, adskilt fra de andre divisjonene. Seksjonen som er lokalisert i denne divisjonen har ansvar for personellsikkerhet, sikring av lokasjoner, hms og beredskap.

Flere av informantene i fokusgruppen gir uttrykk for at de opplever at det er lettere å få informasjon rundt informasjonssikkerhet enn det er for HMS, personellsikkerhet og brannøvelser. A4 opplever at forholdet mellom de ulike typene sikkerhetsinformasjon er ubalansert (…): *«jeg observerer bare det som kommer på intranettet, og det er jo mest IT. Jeg synes ikke det kommer noe fra den andre fronten, altså fra HMS og sånt»*.

Informant A1 etterlyser bedre deling av informasjon rundt brann- og sikkerhetsøvelser som foregår på andre lokasjoner, og påpeker at *«de som ikke er fysisk tilstede under øvelsen eller er en del av arbeidet …de står utenfor og at det er litt tilfeldig at man får vite om det. Det kom heller ingen rapport vi ansatte kunne lese og som vi andre kunne lære av. Ledere fikk sikkert den, men jeg så ingenting til den»*. Gruppen er enig i at det er viktig med øvelser og det å trekke lærdom av disse.

Informant A3, som har lang operativ erfaring og deltatt på flere treninger og øvelser, mener det i dag er en svakhet i sikkerhetsarbeidet at man ikke organiserer egne brannøvelser … *«vi gjennomfører som mange andre, øvelser iht. huseiers plan og ikke vårt eget opplegg, kanskje vi burde gjøre ha egne brannøvelser? Vi har kanskje spesielle behov eller situasjoner som kun vi burde øve på?»*

A1 deler oppfatningen om synligheten av safety-informasjon og personellsikkerhet er for dårlig. På spørsmål om hvor man skal melde avvik rundt safety eller personellsikkerhet, så er gruppen usikker. A2 viser til at *«det finnes sikkert på intranettet et sted, men jeg klarer ikke å huske hvor eller hvem som har ansvar for å ta tak i problemene»*. Flere av informantene tar opp igjen dette med hvor enkelt det er å melde informasjonssikkerhetsavvik. CSIRT og enkel rapportering blir positivt omtalt og A1 presiserer at *«å melde ting relatert til informasjonssikkerhet synes jeg er blitt lett, man bare sender det rett inn til de»*.

På spørsmål om informantene i fokusgruppen har gjort seg noen tanker rundt organiseringen av sikkerhetsarbeidet, svarer flere av dem at en todelt organisering av informasjonssikkerhet og fysisk/safety-sikkerhet var ukjent for dem.

Informant A1 opplever at det er informasjon og budskap rundt informasjonssikkerhet som dominerer og fungerer best… *«jeg synes jo definitivt at det er den IT-sikkerhetsdelen som er mest synlig»*. På spørsmål om tilgangen på informasjon fra den delen av virksomheten som har ansvar for Safety og sikring, så svarer A1 at *«Hvis jeg skal være helt ærlig så føler jeg at kan så lite om det, at jeg ikke har forutsetninger for å fange opp hvis det er dårlig informasjon. Jeg må bare stole på at det er tatt hånd om»*.

A3 spekulerer i om det kan være et resultat av at andre avdelinger og divisjoner tradisjonelt har vært mer utsatt enn de på kontor... *«Det kan jo hende, hvis det er snakk om grensedivisjonen, at det er mer fokus på HMS og sikkerhet der. Der er det snakk om trusler eller hva det måtte være, mot personer eller mot tolletaten. Det kan hende at de kommuniserer i andre kanaler enn akkurat på intranettet, men det vet jeg ikke»*. Informant A1 viser til at en offentlig ansatt på et kontor i nærheten ble drept på jobb og at dette førte naturlig nok til en revitalisert sikkerhetsdiskusjon *«Skulle en sånn episode eller lignende skje her, så føler jeg kanskje ikke hva jeg skulle gjort da, det er jo ikke noe vi har øvd på»*.

4.3.3 Fragmentering av miljøer krever bedre og tettere samhandling:

IT-1 forteller om utfordringer rundt informasjonsflyten grunnet dagens organisering. *«Informasjonsflyten på tvers av avdelinger og divisjoner som arbeider med sikkerhet er fragmentert, noe som har vanskeliggjort rolleavklaringer og informasjonsutveksling»*. IT-1 viser til organisering og informasjonsdeling og fremhever at *«siden Tolletaten har lagt fysisk sikring og personellsikkerhet til Administrasjonsdivisjonen og Informasjonssikkerhet til IT-divisjonen, så tok de ansatte selv initiativ til et felles sikkerhetsfora, kalt Tolletatens sikkerhetsråd (TSR) for å samarbeide tettere»*. Dette var begrunnet i et ønske om at fagpersoner innen flere typer sikkerhet kunne ha en *«uformell arena på lavt nivå der det ikke sitter en leder og følger med»*.

IT-1 fremhever også opprettelsen av spesialenheter på sikkerhetsområdet som et effektivt tiltak for både feedback og informasjon ut. *«En annen ting som ble gjort for å få til bedre informasjonsflyt og rapportering, var at man opprettet hendelsesteamet CSIRT, sånn at ansatte kunne melde informasjonssikkerhetshendelser eller skumle eposter eller hvis man selv hadde gjort en feil, som å trykke på en lenke eller noe sånt… man kunne nå melde dette direkte til et team som hadde dette som fagfelt uten at det måtte gå via lederen din». En enklere kanal og system for rapportering var ifølge informanten viktig for å få bedre feedback fra organisasjonen. Tolletaten fikk en enorm økning i feedback på informasjonssikkerhetsavvik ute i organisasjonen, noe som er viktig for å bedre sikkerheten»* (IT-1).

Informant IT-2 fremsnakker også sikkerhetsforaet TSR og viktigheten av god dialog og informasjonsflyt mellom enhetene som har ansvar for sikkerhet (…): *«nøkkelen er god samhandling mellom fagmiljøene, og TSR fungerer veldig godt her. Det er jevnlige møter med representanter for alle sikkerhetsområdene*»

IT-2 nevner også at IT-ansatte må ta mer ansvar i formidlingen av sikkerhetsinformasjon og engasjere seg mer i direkte personlig dialog.. *«vi må komme oss ut og gjøre det forståelig for folk, og ikke minst få folk til å forstå hvorfor det er viktig»*.

Informant K-1 nevner at informasjonsflyten rundt informasjonssikkerhet i mange bedrifter er preget av mye enveis-kommunikasjon fra toppen og fra IT-ansvarlige. *«Det går mye i awareness-kampanjer og sånt, hvor fokuset gjerne er at de ansatte skal få informasjon om hvordan unngå phising og den klassiske kontakt oss hvis du ser noe, men det er lite toveisdialog. Det er mye mer sånn til informasjon-aktig»*.

K-2 fremhever også viktigheten av å ha feedbackmekanismer på plass. *«Hvis en bedrift har gode feedbackmekanismer opp og ned så vil disse også fungere på sikkerhet. Noen har kanskje i tillegg tatt i bruk automatisk rapportering i Outlook. Hvis du får en mail og vil noen skal se på den så vil det bli loggført og så vil de som driver med operasjonell sikkerhet se på den».*

4.3.4 Delegering av sikkerhetsarbeid til lavere nivå i organisasjonen

Både informant K-1 og K-2 viser til at det nå er en ny trend som innebærer å ha sikkerhetsansvarlige i hver avdeling. Dette er personer som har fått litt ekstra opplæring innen sikkerhet og kan være en ressurs på sin avdeling for spørsmål og hjelp. Begge informantene bruker begrepet «security champions». K-2 viser til at bruken av «security champions» har flere fordeler, også for feedback og rapportering. «*Bruken av security champions gjør det lettere for de som skal ha ansvar for den operasjonelle sikkerheten, men også de som har ansvar for den strategiske (CISO) fordi sistnevnte forholder seg til et mindre antall folk. Security champions kan også brukes til å formidle informasjon nedover i organisasjonen, altså lokalt på sin avdeling».*

K-1 nevner også andre styringsfordeler ved å benytte security champions … *«det er viktig med desentralisert ledelse og muligheten for at folk med sikkerhetskunnskap er tett på prosessen som foregår i andre deler av organisasjonen, som f.eks. risikovurdering i utvikling»*

4.3.5 Leders rolle i formidling av sikkerhetsinformasjon- og opplæring.

På spørsmål om hvem som er ansvarlig for sikkerhetsinformasjon og hvordan kompetanseheving gjennomføres varierer informantenes svar noe.

Informant A1 peker på at skal opplæring innen sikkerhet fungere skikkelig, så er man avhengig at ledelsen setter av tid og ressurser til å jobbe med det (…): *«det er jo ledelsens ansvar å sørge for at vi har tid, klare retningslinjer som er up to date og i henhold til beste praksis»* (A1).

A2 viser til tidligere praksis med opplæring innen sikkerhet i arbeidslivet at *«før satt vi oss ned i et rom og fikk undervisning, mens nå er det jo sånn at alle må lese seg opp på alt selv. Det er jo en stor forandring for mange».*

Noen av informantene stiller spørsmålstegn ved leders mulighet til å følge opp hvorvidt de ansatte har tilegnet seg ny informasjon (…) *«Jeg tror det er et krav til leder om å sørge for at de ansatte er up to date, men spørsmålet er jo om leder har tid til den delen av jobben, eller har de for mye å gjøre? Det kan hende denne biten blir nedprioritert til fordel for noe annet?»* (A3).

A3 mener imidlertid at til tross for at det formelle ansvaret ligger hos leder, så kreves egeninnsats (…) *«man må forvente at de ansatte tar seg tid til å opparbeide seg kunnskap rundt informasjonssikkerhet»* og at «*nærmeste leder ikke skal gå rundt og informere hver enkelt ansatt»*.

Kompetansehevingen til de ansatte på informasjonssikkerhet og informasjon rundt dette fremstår for gruppen som er noe de i stor grad må ta ansvar for selv, og som leder ikke er en synlig del av.

4.4 Sikkerhetskultur

Alle informantene er enige i at sikkerhetstenkning bør være en naturlig del av arbeidshverdagen og at det derfor også er viktig med en god rapporteringskultur i hele organisasjonen.

4.4.1 Sikkerhets- og rapporteringskultur

Flere av informantene mente at det var viktig med en god rapporteringskultur sånn at det ble meldt inn avvik og at man lærte av disse for å bli bedre. Det fremkom imidlertid under intervjuene at ord som avvik og rapportering også kunne innebære en negativ assosiasjon som kunne hindre innmelding av avvik. Informantene pekte blant annet på håndteringen av avvik og at det var usikkerhet knyttet til type respons på det som ble meldt.

4.4.2 God avvikshåndtering og struktur er avgjørende for økt rapportering

Informant A4 delte en personlig historie om å melde avvik (…) *«etter å ha meldt avviket, ble det en samtale med leder og vi opplevde at leder var misfornøyd med episoden, og at vi fikk kritikk for hva vi hadde gjort i situasjonen, fremfor å spørre om bakgrunnen for at vi handlet som vi gjorde». «At det ble en negativ opplevelse handlet mye om måten det ble håndtert på, altså litt i etterkant. Vi oppfattet det som direkte kritikk, og i stedet for å høre «takk for at du meldte avviket sånn at vi kan lære av det», så ble dette kun en dårlig opplevelse. Vi følte vi satt igjen med svarteper. Jeg har ikke meldt noen avvik etter denne hendelsen» (A4).*

Informant A2 mener også at det er viktig å få frem intensjonen i å melde avvik, som f.eks. å lære av en episode. Med henvisning til A4s historie, *«Så i stedet for å angripe måten dere håndterte situasjonen, så kunne man sagt at, ja da må vi kanskje dra litte granne lærdom av akkurat denne episoden?»*.

Informant IT-1 understreker at tidligere systemer i Tolletaten ikke var tilrettelagt for å avviksrapportering. Begrep som avvik var ifølge flere informanter forbundet med svak håndtering og dårlige strukturer. IT-1 bemerket blant annet at «Avvik er *et sånt uttrykk jeg ikke liker å bruke*,

og det funger veldig dårlig i toll. Ekstremt dårlig. Det gamle avvikssystemet var strukturert slik at det var nærmeste leder som hadde ansvar for å håndtere og lukke avvik. Ta f.eks. et informasjonssikkerhetsavvik, hvor du har fått virus på PC`n din. Du sendte inn et avvik på dette her, for du hadde lyst å melde fra til noen. Din nærmeste leder får nå beskjed om at du har fått et virus på PCn, og så ville han jo gå til deg å si «hvorfor har du fått virus på PCn!? Dette ser jo så dårlig ut for vår avdeling!». (…)«Jeg mener at slike episoder kan ha bidratt til at det tidligere ble meldt inn svært få avvik».

Informant IT-2 trekker viser til tiltaket som ble gjort for å øke rapporteringen av informasjonssikkerhetsavvik. *«Opprettelsen av CSIRT og det å ledere ikke lenger hadde ansvar for å håndtere avvik kan ha vært en faktor i den store økningen av innmeldte avvik», og at «CSIRT har muliggjort å rapportere inn ting som ikke er avvik, slik som skummel epost eller noe som oppfattes som unormalt". CSIRT vurderer da selv om det er et avvik eller ikke».*

«Ved å legge om avviksrapportering til et team, fremfor at alt går til CISO, så får man også bedre redundans i form av mer kunnskap og mer effektiv behandling da flere enn én person håndterer det».

4.4.3 Tillitt som faktor i informasjonssikkerhetsarbeid

IT-1 understreker at tilnærmingen til hvem som har ansvaret for feil er flyttet vekk fra bruker og over på systemnivå. «*Hvis du har fått virus på PCn din, så er det organisasjonen som har tillatt/tilrettelagt for at det kunne skje. Det vil si at det alltid er Tolletaten som har gjort noe feil. Hvis ikke det bevisste handlinger fra den ansatte da. Hvis du selvrapporter det inn, så skal du ikke bli straffet for det. Det er prinsippet».*

Dette skiftet fra individ til systemnivå bidro også til at de ansatte fikk mer tillitt til rapporteringssystemet og at de ble mer sikker på å få en rettferdig behandling dersom de meldte inn feil. *«Den enorme økningen i antall henvendelser angående informasjonssikkerhetsavvik CSIRT fikk, sier kanskje litt om viktigheten av tillitt og trygghet i at det håndteres anonymt og av en profesjonell funksjon».*

Anonym rapportering er også noe som K-2 argumenterer for, selv i phising- og sikkerhetsøvelser. *«Vi sørger for at de personene som har gjort noe galt i øvelser, aldri kan identifiseres. Det vi har*

gjort i enkelttilfeller er at vi har tatt direkte kontakt med disse selv, uten at ledelsen er klar over det».

K-2 understreker igjen at tillitsfaktoren er vel så viktig som økt kunnskap i arbeidet med informasjonssikkerhet. Her brukes Sec-Leads eller Security champions igjen som eksempel. *«Gutta på gulvet snakker med gutta på gulvet» og de må ikke alltid oppover i systemet. Det er en person du føler deg trygg på å snakke med. En du kan gå inn og si «jeg gjorde noe dumt, eller hva skal jeg gjøre her?». Sånne ting er viktig for å bygge en bedre rapporteringskultur, men også en utdanningskultur, altså at man sprer det gode budskap. Rapporteringen vil også kunne gå begge veier, altså også fra champions nede i organisasjonen og oppover til f.eks. IT-sikkerhet eller CISO».*

4.4.4 Noen typer informasjonssikkerhetsavvik rapporteres ikke

Avvik oppfattes av de involverte informasjonssikkerhetsekspertene som brudd på instruks eller regelverk. Det fremkommer imidlertid blant informantene i fokusgruppen at noen avvik oppfattes som mindre viktige og ikke rapporteres.

Informant A4, som jobber på kontor kobler avvik til det at folk forlater PCen uten å låse skjermen, og at dette skjer mange ganger daglig. (…): *«dette kunne man meldt daglig, men tror ikke det er noen som faktisk melder det. Jeg tror ikke folk tenker at det er så alvorlig så det kan være, men heller har en tanke om at neh, det er ikke så farlig»* (A4). Informant A3 nevner at akkurat dette med å låse skjermen er noe som fokuseres på i kampanjer som «sikker oktober» osv. og at dette er et positivt tiltak, da alle informantene i gruppen er enige om viktigheten av å låse skjermen og rydde viktige dokumenter fra pulten sin når de ikke er til stede.

De erkjenner likevel at dette er et område de mistenker at det ikke rapporteres på, hverken til leder eller via avvikssystemet. (…): «jeg ville neppe meldt det til videre, siden det er noe folk bare glemmer» (A2).

Informant A1 nevner at man skal kunne stole på kollegaene sine og at hen heller ville tatt det direkte med vedkommende hvis det skjedde mange ganger, fremfor å melde det inn. (…): *«det virker så mye styr for en liten ting, og så blir det som jeg sladrer eller tyster på en kollega ved å gå direkte til leder, med noe jeg heller kunne tatt direkte»* (A1).

Tillitt er også viktig for informant A3, som sier at fremfor å «ta noen for avvik» så burde fokuset være på forbedring. Flere av informantene fremstår også sterkt skeptisk til bruken av ordet avvik. *«Avvik er et veldig negativt ladet ord, så det må jeg være forsiktig med å rapportere inn, fordi det kan få katastrofale følger for han som rapporteres»(A3)…(…): «ja, det er et godt poeng, at man må tenke på konsekvensene for han som blir meldt (A1)»*.

Informant A3 og A4 lufter så ideen om at et annet ord enn avvik kunne vært hensiktsmessig i å oppnå bedre rapportering. *«det kan godt hende at et annet ord ville gjort det til noe mindre skummelt, f.eks. kalt det forbedringsmelding eller noe sånt. Ja, endret fokuset fra noe negativt til noe positivt. Da tror jeg terskelen for å melde inn hadde vært lavere»*

4.5 Informasjonssikkerhet

4.5.1. Økt kompleksitet og nye trusler

Alle informantene er samstemte i at verden blir mer digitalisert og kompleks, noe som krever en større bevissthet rundt egen rolle, men også rundt teknologi og nye digitale trusler. Informantene har noe ulik forståelse av hva som konstituerer de største truslene, men at informasjonssikkerhet er enda viktigere enn før er det felles enighet om.

4.5.1.1 Trusler rettet mot operativ teknologi (OT)

Informant K-1, som har jobbet mye med sikkerhet og har erfaring fra Forsvaret og IT, peker på økt digitalisering av OT (operativ teknologi) som et nytt sårbart område. (…): *«med OT tenker jeg på digitalisering av fiskefarmer, olje- og gassnæringen, havbruk, digitalisering av skip osv. Når disse kobles på nettet kan noen av disse systemene være utsatt for angrep som overbelaster dem. De er utsatt for å bli kjørt så høyt opp at de går i luften. I tillegg har man den geopolitiske situasjonen nå, med krig i Ukraina, påvirkningsoperasjoner, manipulering, fake news og ikke minst sabotasje. Det er nå et stort og komplekst trusselbilde» (K-1).*

Utfordringene med OT-systemer er også noe som opptar K-2. (…): *«vi ser nå er at bedriftene vil utnytte de dataene som produseres i et OT-miljø. Du får altså en tettere integrasjon mellom OT og IT, og da får du et større behov for å sikre OT-nettet ditt. Noen har en CISO på strategisk nivå som dekker begge deler, mens noen skiller på det operative, men da dukker det opp en utfordring med hvem som har ansvar for det i midten, dataene som skal føres frem og tilbake»*

Informant K-2 mener derfor det er viktig med en holistisk tilnærming, hvor man ser ting i sammenheng. (…): *«i bedriftene som har tatt dette helt ut, som virkelig har kontroll på det, de har en operativ sikkerhetsavdeling som støtter begge deler, altså som har ansvar både for IT og OT. For da evner de å se tingene i sin helhet. Dette er noe jeg også anbefaler, da man har et annet risikobilde på OT. Man kan ikke klikke på en link og få et virus, men på den andre siden så har du det at systemene i et OT-nett er ofte veldig mye eldre og svært sårbare ved påkobling» (K-2).*

4.5.1.2 Trusler og utfordringer med overgang til skyløsninger

Informant IT-1 peker på sin side på omstillinger og overgang til skyløsninger som en potensiell sikkerhetsutfordring. *«La oss ta en SaaS-tjeneste (security as a service). Her outsourcer vi alt av tjenesten til en ekstern leverandør, så vi mister egentlig hele kontrollen over alle disse sikkerhetsmekanismene som vi har i dag. I dag har vi anti-virus, brannmur og alle disse beskyttelsesmekanismene. De gir vi til en ekstern leverandør, og så endrer vi ansvarsområdet fra fysiske system til avtale- og regelverk. Er f.eks. disse nye databehandleravtalene og regelverkene godt nok beskrevet mtp. sikkerhet?»* (IT-1).

Videre peker informanten på potensielle utfordringer ved manglende omstillingsevne i organisasjonene, blant annet som følge av avganger og gjennomtrekk. (…) *«I store organisasjoner har man gjerne en jevn utskiftning av ansatte, f.eks. ledere som går av med pensjon om fem eller ti år, parallelt med ti år før det digitale skiftet skjer for fullt. Dette kan muligens føre til en passivitet og et ønske om å ikke skape de største omstillingsbølgene i sin avdeling før pensjon. Dette er jo også en potensiell stor risiko»* (IT-1).

4.5.2 Sikker utvikling («DevSecOps»)

4.5.2.1 Opplevd interessekonflikt mellom kreativitet og sikkerhet:

Et tema som går igjen blant informantene med IT-bakgrunn er utfordringen med å implementere informasjonssikkerhet i utviklingsprosessen. IT-utvikling- og IT-sikkerhet er ofte organisatorisk skilt ut fra CISO og informasjonssikkerhet. Kreativitet og frihet er verdier som informantene oppfatter som viktige i utviklermiljøene. Flere av informantene peker på kulturforskjeller og eierskap til utviklingsprosessen kan skape problemer med å etablere og opprettholde et velfungerende system for sikker utvikling.

K-2 viser til egen erfaring om at (…): *«i noen av utviklermiljøene finnes en holdning om at «utvikleren vet best, også når det gjelder sikkerhet. Derfor er det lite å hente i å jobbe med meg*

som sikkerhetskonsulent». Utfordringen er at man skal ikke tre sikkerhetstiltak nedover hodet til utviklerne, da dreper du kreativiteten deres. Du må gi de et sikkert miljø å utvikle koden i, samtidig som koden som går ut er i henhold til et gitt kvalitetsnivå»

K-1 har også erfaring med dårlig dialog mellom sikkerhetsavdelinger og IT-utvikling. (…) *«det er kanskje mangel på kompetanse eller forståelse for IT-sikkerhet på utvikling. Sikkerhetsseksjonen snakker gjerne ISO-27001 språk, om sikkerhetsprosesser og vurderinger, mens IT snakker agil metode, sikker utvikling, DevSecOps, ting skal være smidig og gå fort. Ofte snakker de ikke samme språk fra starten av» (K-1).*

Graden av sikker utvikling (DevSecOps) varierer ifølge informantene stort blant virksomhetene. (…): *«noen sier at nå skal vi bygge sikkerhet inn i alle ledd», «vi skal ha sjekk av koden, sjekk av biblioteket, og før vi tar release så skal vi gjennom følgende prosesser etc. Og så har du den andre enden av skalaen: hvor bedriftene har sikret seg så mye de kan, men utviklerne har mulighet for å release ting rett i operasjonen, uten at det går igjennom noen form for sikkerhetskontroll. Utviklerne har altså langt på vei lov å gjøre som de vil (K-2).*

4.5.2.2 Produksjonspress og sikker utvikling:

Informant K-1 peker også på utviklernes ønske om frihet, men understreker at det er et annet forhold som han ofte ser, hvilket er et produksjonspress på utviklingsfronten. *«Det er et press at utviklingen skal skje raskt, altså å få de nyutviklede systemene ut i produksjon. Jeg generaliserer, men utviklerne er opptatt av å løse problemer og få ting i produksjon. Når det da kommer sånne sikkerhetsfolk og spør «har vi tenkt på dettte, dette og dette?» så blir de samme sikkerhetsfolkene en hemsko for utviklingen» (K-1).*

En annen utfordring med utvikling som løftes frem ifm. forventninger og rask produksjon er utfordringen knyttet til rapportering av potensielle sårbarheter i utviklingen oppover i organisasjonen til beslutningstakere. (…): *«Hvordan kan jeg som direktør vite at de produktene som utvikles i mitt selskap er sikre? Det kan være hundrevis av utviklere og IT-utvikling er ikke noe jeg som direktør har innsikt i»* (K-1). *(…) «det å få aggregert opp informasjon om kritiske sårbarheter, om de er løst eller ikke, før det settes i produksjon mener jeg er veldig viktig. Her tror jeg det er et veldig stort gap i dag, på hva man vet om og hvordan det faktisk er»* (K-1).

4.5.2.3 Risikovurdering sentralt for sikker utvikling

Informantene med IT-bakgrunn trekker frem god risikovurdering som viktig i utviklingsfasen og for informasjonssikkerheten generelt, men at dette kan være vanskelig å få til, enten pga. manglende kompetanse, organisering, eller begge deler.

Informant IT-1 viser til et eksempel med en organisering med det han kaller «systemeiere», altså enheter og ansatte med totalansvar for applikasjoner og systemer. (…): *«regelverket sa at disse personene hadde ansvar for alt inni løsningen, inklusiv sikkerhet og risiko. Altså, disse personene skulle ikke bare være ansvarlig for å gjennomføre disse tingene, men de skulle også kunne alt, de skulle kunne risikovurdering 100%. Disse kan ikke være risikostyringseksperter i tillegg til alt det andre så det er nesten dømt til å mislykkes» (IT-1).*

K-1 viser også til at mangel på risikovurdering i utviklingsprosessen er et utbredt problem. (…): *«jeg har snakket med flere selskaper som driver med utvikling, og akkurat det der, med risikovurdering i utviklingsprosessen, det eksisterer nesten ikke»..(…): «jeg tror kanskje at det henger sammen med tanken om å få ting raskt i produksjon».*

K-2 peker på at samhandling mellom de ulike avdelingene, og inkludering av ledelsen er nødvendig for å implementere sikker utvikling, som også innebærer god risikovurdering. *«Nye sikkerhetsrutiner må komme fra CISO, med forankring i ledelsen. Operativ IT-leder og leder for systemutviklingsavdelingen setter seg sammen, og har kanskje fått et mandat fra CISO som sier gjør «utviklingen vår på en sikker måte». «Jeg pleier å si at de sikkerhetstiltak som skal innføres i en bedrift, de må være koblet opp mot et risikobilde, og da har du vanlig tradisjonell risikovurdering» (K-2).*

En strukturert tilnærming til risiko er noe informant K-1 fremhever som viktig i det helhetlige risikoarbeidet, sånn at det blir enklere for ledere å prioritere (…) *«dette er noe vi kan/må prioritere, dette kan vi ta til neste år» osv. Det er viktig å dytte det opp til ledelsen og vise at man er bevisst på risikoene, og at risikoen bæres av leder, ikke sikkerhetsansvarlig. Så er det opp til virksomhetene om de tar tak i den eller om de opplever risikoene som akseptable. Jeg opplever likevel at virksomheter bærer høyere risiko enn det som kanskje er lurt» (K-1).*

Arbeidet med å innføre sikker utvikling og forbedre prosessene rundt sikkerhet er noe flere av informantene mener er krevende og et område som gjerne blir nedprioritert inntil de oppstår en uønsket hendelse. (…) *«Når det gjelder å gå fra liten satsning på sikker utvikling til stor, så kan jeg love deg at flere bedrifter har en lang vei å gå, og noen ser ikke lyset før de har gått på en skikkelig smell, enten selv eller noen de jobber tett med»* (K-2).

4.5.3 Uønskede hendelser forekommer

Til tross for at samtlige informanter enten har økt sin egen eller jobber med å øke andres risikoforståelse, er det en kjensgjerning at det forekommer uønskede hendelser. Informantene med IT-bakgrunn forteller om digitale angrep og informantene med sikringsbakgrunn viser til alvorlige hendelser som terrorangrep og lignende. Felles for historiene til informantene er at de peker på at alvorlige hendelser i de fleste tilfeller fører til en eller annen form for endring.

4.5.3.1 Alvorlige hendelser fører til endringer

Flere organisasjoner, blant annet Equinor har opplevd svært dramatiske hendelser de siste ti årene. En av de mest profilerte var terrorangrepet mot (daværende Statoil) gassanlegget i In Amenas i Algerie.

EQ1 og EQ2, begge med inngående kjennskap til terrorangrepet og følgende det fikk for sikkerhetstenkningen, fremhever at (…): *«In Amenas-hendelsen endret selskapet fullstendig. Det har skjedd mange kvantesprang innen fokus på fysisk sikring og sikkerhet generelt, men jeg vil si at det er ofte hendelser som har vært triggere til at vi får de løftene innen sikkerhet (EQ1). (…): «Før var det mer silotenkning, men det er nok mindre nå, med tanke på hendelsene vi har vært igjennom. Vi har kommet nærmere hverandre og har flere informasjonsmøter på tvers. Vi har også jobbet med å koble flere enheter sammen med felles informasjon» (EQ2).*

«Det fikk også konkrete endringer ift. planverket vårt. Vi fokuserer nå på at et felles planverk må være sånn at det kan settes ut på lavest mulig nivå, og at det er desentralisert. Så om det smeller igjen, så skal han som er sjef på stedet, kunne iverksette de tiltak han mener er nødvendig, uten å få kritikk for å gå for hardt ut, inntil storsystemet/myndighetene kommer med føringer» (EQ1).

Informanten understreker også at det viktig å lytte til hele organisasjonen og få med alle ansatte når det gjelder sikkerhet og at alle i organisasjonen vet hva de skal gjøre. (…): *«tanken er at hvis det skjer noe, så er det ikke bare én sikringsansvarlig på et anlegg, men man har alle ansatte. Det er f.eks. ikke nok at bare ett vaktlag som deltok i en sikkerhetsøvelse vet hva de skal gjøre. Et skift*

består kanskje av fem-seks vaktlag og det er viktig at alle er med. Det må helt ut i enden av organisasjonen om vi skal lykkes» (EQ1).

Informantene fortsetter å vise til eksempler hvor det har oppstått en hendelse og deretter en endring i sikkerhetskulturen, enten ved å investere i nytt utstyr eller legge om planer. (…): *«Det har vært såpass mange hendelser, at flere bedrifter har blitt mer opptatt av informasjonssikkerhet. Særlig dette med security awareness er noe de blir mer opptatt av (K-2).*

4.5.3.2: Kostbart med sikkerhetstiltak, men også kostbart uten.

Flere av informantene peker på at det er svært store kostnader forbundet med å drastisk øke sikkerheten og det å opprettholde et økt sikkerhetsnivå. Kostnadene relatert til dette er både økonomiske og psykiske, og er ifølge informantene delvis styrt av eksterne forhold.

Informant EQ1 peker på at det er vanskelig å planlegge og styre når man må opprettholde et høyt sikringsnivå over lang tid. Planverk er ofte ikke dimensjonert for en langvarig økning i sikkerhetstiltak, som tærer både på personell og ressurser. (…): *«altså, det er jo krevende i det at det koster veldig mye penger. For store organisasjoner snakker man kanskje millioner i måneden med dagens situasjon. Man har kanskje lagt et planverk for 3-5 uker frem i tid, men når man ender opp med over 20 uker på forhøyet sikringsnivå merker man kostnadene. I tillegg så kan det jo hende at situasjonen blir enda verre, så det er skremmende på flere måter» (EQ1).*

«En annen ting er den menneskelige påkjenningen. Å stå på tærne over lang tid er belastende. Å hele tiden være årvåken og ikke slappe av. Det er krevende å ikke si til oss selv «nå har det ikke skjedd noe i det siste, så nå kan jeg slappe litt av» (EQ2).

Scenarioer man ikke har trent på kan også ifølge informant EQ1 gi utslag i form av frykt og bekymring, altså en menneskelig kostnad. (…): *«når droneobservasjonene begynte ute offshore, så var jo vi bekymret og folk begynte å bli redd. Vi var ikke trent i å håndtere dette selv, så vi måtte ta kontakt med myndighetene for å få utbedret det. Det var ganske skjellsettende, at det var vi først som var nødt til å dra inn og be om hjelp»* (EQ1).

K-2 forteller om en stor entreprenør i Stavangerområdet som i 2022 ble rammet av et alvorlig dataangrep og avkrevd flere millioner i løsepenger. Virksomheten hadde ikke investert tilstrekkelig i gode informasjonssikkerhetsløsninger i forkant av angrepet. *«En uttalelse i etterkant*

fra den rammede virksomheten var at (…):nå skulle de bygge den beste løsningen for informasjonssikkerhet som fantes. Problemet var at denne målsetningen kom i etterkant av angrepet, som kostet dem en god del penger …de merket det godt for å si det sånn» (K-2).

5 Diskusjon

I dette kapittelet drøftes funnene i studien opp mot teorien presentert i del 3. Diskusjonen er strukturert slik at forskningsspørsmål 1 – 3 drøftes og besvares hver for seg.

5.1 Forskingsspørsmål 1: «Hvilke teoretiske rammeverk bygger dagens organisering av sikkerheten på»?

Organiseringen av sikkerhetsstyringen nevnes av flere informanter som et område som blir stadig viktigere, men også et område som blir mer komplekst og mer krevende. Sikkerhetsstyringen berøres av en rekke ulike standarder og retningslinjer, samt reguleres av lovkrav som følge av blant annet sikkerhetsloven og internkontrollforskriften.

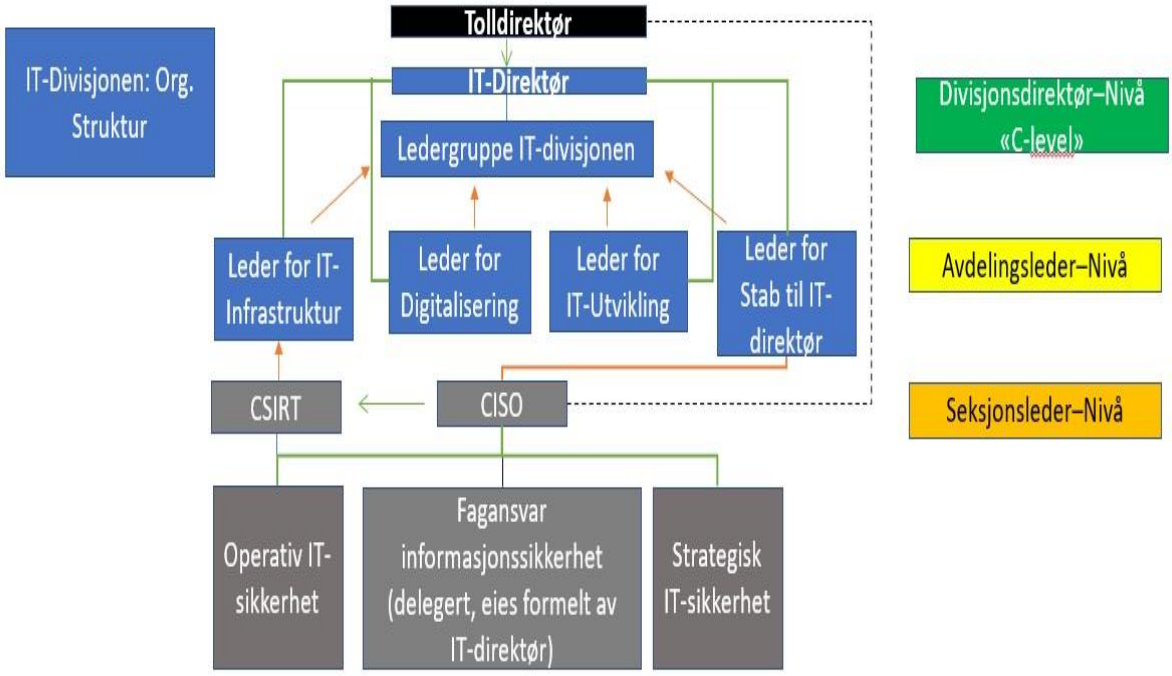
5.1.1 Standarder, retningslinjer og lover regulerer informasjonssikkerhetsarbeidet

Tolletaten baserer i likhet med mange store virksomheter sitt arbeid med informasjonssikkerhet blant annet på ISO-standard 27001 og 27005. Disse standardene gir anbefalinger rundt styring og risikovurdering, men er ingen fasit for god sikkerhet. De må implementeres i organisasjonen og tilpasses strukturelle og kulturelle forhold. Dette er illustrert i den *todimensjonale modellen over organisatorisk redundans* til Rosness (Rosness, 2004) (figur 2, i del 3.3) Det er altså ikke nok «å ha en god standard å følge», den må også fungere i den enkelte organisasjonen. Den må særlig legge til rette for god rapportering, en viktig forutsetning for en god sikkerhetskultur (Reason, 1997). En ISO-standard er likevel et godt utgangspunkt, noe informant IT-2 understreker i intervjuet. Den etablerer et styringssystem for informasjonssikkerhet og er et fundament som virksomheten kan bygge videre på. Standarder kan være en fordel når det kommer til samarbeid med andre aktører og som et felles krav til en minstestandard. Dette området endres raskt og hvis flere aktører har en lik forståelse av begreper og metodikk innen informasjonssikkerhet kan dette bidra til å en harmonisering på fagfeltet.

Å lene seg for sterkt på standarder kan likevel sies å presentere en risiko, da disse er generelle, samt at det tar gjerne lang tid å utvikle nye og tiden kan ha «løpt ifra neste versjon», noe som også påpekes av Leveson (2011).

5.1.2 CISO delegert ansvar, men ikke ansvarlig for informasjonssikkerhet

Det fremkom i intervjuene med de interne informantene, IT-1 og IT-2, samt «Direktiv for sikkerhet» (2020) at Tolletatens fagansvar for informasjonssikkerhet er lagt til IT-direktøren og derfra delegert til informasjonssikkerhetsansvarlig (CISO). Under informasjonssikkerhetsansvarlig befinner også operativ it-sikkerhet seg. Man har i henhold til denne strukturen delegert ansvar «ned i linjen» fra et høyere nivå hos IT-direktør. En slik delegering kan sies å være i tråd med Weick, Sutcliffe & Obstfelds (1999) teori HRO og en fleksibel organisasjon. Løsere strukturer er hensiktsmessig for å komme tettere på de mindre og lavere delene av organisasjonene, som gjerne krever mer fagkunnskap for å forstå og styre. Det bør imidlertid påpekes at Tolletaten har valgt å delegere, ikke overlate eierskapet for informasjonssikkerheten til CISO, så man kan til dels innvende at det fortsatt et tydelig hierarkisk preg over organisasjonens arbeid med informasjonssikkerhet. En hierarkisk struktur og det faktum at intern informant IT-1 opplyste om at CISO er plassert utenfor ledergruppen i IT-divisjonen (se figur 9 av nåværende struktur i IT-divisjonen) kan sies å støtte en slik påstand.



Figur 9: Dagens organisering av IT-divisjonen (Tolletaten, 2020)

Med delegert ansvar for informasjonssikkerhet, men likevel delvis utenfor viktige kanaler og beslutningsfora, slik som ledergruppen, er CISO og informasjonssikkerhetsområdet sårbart for tap

av kritisk informasjon, noe som blant annet Turner (1976), gjennom det såkalte informasjonsprosesseringsperspektivet hevder er en medvirkende årsak til uønskede hendelser. Hvis CISO ikke får anledning til å formidle risiko og korrigere antagelser, kan toppledere basere sine beslutninger på feil grunnlag innen informasjonssikkerheten.

Det hierarkiske aspektet er godt illustrert i Leveson (2011) sin sosiotekniske modell, som også fremhever feedback fra lavere nivå som viktig for å kunne justere kursen i organisasjonen. Til tross for at Tolletaten har valgt en slik organisering, har tolletaten likevel gitt CISO en sikkerhetsventil i form av en stiplet linje til tolldirektøren. Dette kan ses i lys av de bekymringene flere informanter, både interne og eksterne delte, om at ledere kunne stenge forslag fra CISO på et lavere nivå ute, dersom det var motstridende interesser. Tolletatens valgte løsning gir CISO muligheten til å «forbigå» sine ledere og gå rett til toppen og tolldirektør som har instruksjonsmyndighet over de øvre ledernivåene. Dette motvirker potensielt rigide strukturer, et grep som iht. Weick, Sutcliffe & Obstfelds (1999) teorier om høypålitelige organisasjoner (HRO) bidrar til økt sikkerhet i organisasjoner.

5.1.3 Safety og security er klart adskilt gjennom bruk av definisjoner

Tolletatens overordnede dokument for sikkerhetsstyring, «Direktiv for sikkerhet» (2020) er tydelig på skillet mellom Safety og Security. Direktivet viser til NOU: 2000 «Et sårbart samfunn» sine definisjoner på Safety og Security. Safety defineres her som *«Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter»* og Security som *«Sikkerhet mot uønskede hendelser som er resultat av overlegg og planlegging»*. (NOU: 2000:24).

Iht. direktiv for sikkerhet, er tolletatens forståelse av skillet som følger: *«Forskjellen mellom safety og security beror altså på om skaden er påført uten motiv (ikke villet) eller med motiv (villet)» … «I Tolletaten reguleres safety gjennom ledelsessystemet for helse, miljø og sikkerhet (HMS)»* (Direktiv for sikkerhet: s3, 2020). Tolletatens organisering med et tilsynelatende klart skille på fagområder og ansvarlig fagmyndighet, gir organisasjonen klare føringer om hvem som er ansvarlig for hva. Denne måten å organisere på er av informant K-2 en anbefalt tilnærming, og basert på prinsippet om såkalt «segregation of duties», eller «skille mellom oppgaver/plikter».

Likevel viser funn gjort gjennom fokusgruppe-intervjuene at ansatte ikke nødvendigvis er kjent med organiseringen, har nok kunnskap om avvikssystemet, og til dels etterspør mer informasjon om safety-relaterte saker. Dette kan indikere at kompleksiteten og mengden informasjon som flyter

rundt på sikkerhetsområdet ikke nødvendigvis når alle tiltenkte mottakere. At informasjon blir fortolket ulikt og forsvinner på veien i de ulike nivåene er noe Leveson (2011) og Turner (1976) begge omtaler som en risiko i komplekse organisasjoner. Utfordringen med å nå ut til den spisse enden med informasjon ble også nevnt av informant EQ1, på noe som ble oppfattet som krevende i en stor organisasjon som Equinor.

Når det gjelder fysisk sikring, personellsikkerhet og beredskap så er disse også lagt til seksjon for HMS og delegert til sikkerhetsansvarlig (Chief Security Officer). Direktiv for sikkerhet påpeker for øvrig at mens informasjonssikkerhet er lagt til IT-direktøren er «resten av *sikkerhetsområdet lagt under divisjonsdirektør for administrasjonsdivisjonen». (…) «For å sikre at Tolldirektøren kan forholde seg til sikkerhetsområdet helhetlig, er det tildelt et koordinerende ansvar for sikkerhetsområdet til divisjonsdirektør AD, som har ansvaret for det overordnede styringssystem for sikkerhet»* (Direktiv for sikkerhet: s4, 2020). Fagansvaret til administrasjonsdivisjonen favner altså også sikkerhetsområdene fysisk sikring og personellsikring, og er i likhet med tilnærmingen i IT-divisjonen, delegert, i dette tilfellet til CSO. Et koordinerende ansvar gjør det ekstra viktig at informasjonsflyten fungerer på horisontalt og vertikalt i organisasjonen. Til tross for delegering til lavere nivåer for å øke fleksibiliteten, fremhever enkelte av informantene at en fragmentering av sikkerhetsområdet tidligere kunne være krevende, og man etablerte det som da ble kjent som Tolletatens sikkerhetsråd (TSR), i dag omdøpt «Sikkerhetssamarbeid».

Beskrivelsen til informantene av utbyttet med TSR var at sikkerhetsmiljøene i Tolletaten oppnådde en bedre informasjonsflyt, deling av innrapporterte data, og anledning til å vurdere sikkerhetssaker sammen, før de eventuelt ble skalert opp til et høyere nivå. Resultatene var altså en økt fleksibilitet, bedre rapportering, fleksibelt fagmiljø og et miljø preget av gjensidig tillitt. En slik tilnærming og oppnåelsen av dette er alle anbefalte punkter i oppbyggingen og styrkingen av en sikkerhetskultur (Reason,1997). Med fokus på forbedring av sikkerhetskultur kan man hevde at TSR oppnådde sitt formål med å styrke sikkerhetssamarbeidet i Tolletaten.

5.2 Forskningsspørsmål 2: «Hvordan fungerer rammeverket i praksis?»

Med rammeverk som ISO27001 og etablert sikkerhetsstyring, ansvarsfordeling og begrepsavklaring på plass, hva er de praktiske konsekvensene for organisasjonen?

5.2.1 Standarder og rammeverk fanger ikke opp alle typer avvik

ISO-standarder for som 27001 legger f.eks. føringer for at avvik skal registreres og håndteres av virksomheten, med hensikt om å styrke informasjonssikkerheten. ISO-standarder er imidlertid akkurat det, en standard, og ikke et svar, noe som kan resultere i varierende resultater i ulike organisasjoner.

Utfordringen her, som ble illustrert i fokusgruppeintervjuet, var at det er flere typer avvik som blir underrapportert eller ikke rapportert i det hele tatt. Et eksempel på dette var å ikke låse skjermen når man forlot arbeidsplassen sin. Dette konstituerer ifølge IT-2 et avvik og brudd på informasjonssikkerheten, og skal etter reglene rapporteres, men deltakerne i fokusgruppen sa at de likevel ikke hadde rapportert slike tilfeller, til tross for de observerte det daglig.

Alle informantene var enig det var viktig å låse skjermen, men vurderte det som glemskhet og en «liten feil», og lite rapporteringsverdig, eller som informant A2 sa det, «(…): «jeg ville neppe meldt det til videre, *siden det er noe folk bare glemmer*», samt at (…): *«å gi beskjed om sånne små ting føles som å bidra til en tysterkultur»* (A1). Mangelfull rapportering kan gjøre at føre til at organisasjonen fortsetter driften basert på en antagelse om at alt er bra, når det egentlig ikke stemmer. En slik antagelse og mangel på korrigerende tiltak kan føre til at feil, selv små får utvikle seg og resultere i en uønsket hendelse (Turner, 1976).

Den feile antagelsen kan være at informasjonssikkerheten er god nok og «no news are good news». Dette med «små ting» som å glemme å låse skjermen kan likevel være tegn på et større skjult avvik på informasjonssikkerhetsområdet. Tanken om at man ser små feil, men går glipp av det egentlige problemet er sentralt i Turner sitt perspektiv på informasjonsflyt i hans teori om Man-Made disasters (Turner, 1976).

5.2.2 Organisasjonskultur som faktor i sikkerhetsarbeidet

Dersom standarder og styringssystemer ikke fungerer optimalt og avviksrapportering uteblir, så bør man vurdere å se nærmere på dette i en organisatorisk kontekst. Er denne delen av standarden eller kommuniseringen av formålet med den tilpasset den enkelte organisasjonen? Er det en organisasjonskultur til stede for å godta visse feil og rapportere andre, til tross for at de bryter med sikkerhetsinstrukser? Stadig flere forskere peker på at kultur ikke nødvendigvis bare er noe en organisasjon har, i form av konstruerte regler og instrukser som dikterer adferd, men at det er noe en organisasjon *er* (Engen mflr. 2021; Reason 1997). Med dette siktes det til at organisasjonskultur

kan være et *«komplekst system av symboler og meninger, bestående av historier, myter, ritualer og andre verdimessige uttrykk»* (Engen mflr. s.175).

Informantene i fokusgruppen viser til personlige historier rundt avvik og en tidligere uheldig praksis i å håndteringen av avvik. En historie med enkeltepisoder med f.eks. sterke sanksjoner kan ha bidratt til å etablere en organisasjonskultur hvor man ikke melder ifra i frykt for sanksjoner. En slik organisasjonskultur kan tenkes å videreføres til nye ansatte. Videreføringen kan komme av at *«organisasjonskulturen er noe som sitter i veggene, som de ansatte kan lære om og internalisere, - sosialiseres til etter en viss tid i organisasjonen»* (Christensen mflr. 2021 s.57). Man risikerer slik sett å bli «opplært» til å ikke melde ifra etter velmente råd fra erfarne kollegaer.

Flere av de eksterne informantene viser til at dersom virksomheter legger til rette for enklere og helt eller delvis anonym rapportering vil rapporteringen øke. Dette var også tilfellet med Tolletatens initiativ da de etablerte CSIRT og oppfordret de ansatte til å sende inn epost og spørsmål. De ansatte rapportere inn selv om de var usikre på om det var en hendelse eller ikke. Det at rapporteringen økte signifikant kan være en indikator på at de på gulvet tar sikkerheten på alvor og rapporterer dersom avviksrapportering «ufarliggjøres». Dette inntrykket deles også av intern informant IT-1, gitt de har tillitt til systemet og behandlingen de får.

5.2.3 Hva som er rapporteringsverdig påvirkes av dialog mellom nivåene

Oppfatningen blant ansatte at noe er mindre rapporteringsverdig kan muligens tilskrives at det kanskje ikke tydelig nok er kommunisert hvorvidt det finnes ulike grader av viktighet blant avvikstyper eller hvorfor det er viktig. Ser man på dokumentasjon, styringssystemer og intensjon til sikkerhetsansvarlige så er det viktig å rapportere alle typer avvik, alltid. En slik tilnærming fordrer imidlertid at de sikkerhetsansvarlige og ledere gis mulighet til å forklare bakgrunnen for dette standpunktet til de i den spisse enden. Informant IT-2 nevnte helt spesifikt i intervjuet at en dialog mellom nivåene var avgjørende for å forstå *hvorfor* man skulle rapportere. Også her vender forbedring i sikkerhetsarbeidet tilbake til Leveson (2011) sitt fokus på feedbackmekanismer og god informasjonsflyt i organisasjonen.

At ulike typer avvik og feil ikke nødvendigvis skyldes en intensjon om å begå regelbrudd er også noe som fremheves av Reason (1997). De interne informantene i fokusgruppen viser til at kollegaer som bryter rutinen om f.eks. å låse skjermen tilsynelatende gjør dette på bakgrunn av glemskhet og ikke har til hensikt å eksponere data eller legge til rette for sårbarheter. Reason (1997) betegner

dette som «glipper og glemskhet» (slips & lapses), og at disse ofte er relatert til å ta snarveier og ikke ta seg det ekstra bryet i å følge rutiner (som i å låse maskinen). *«Denne type snarveier, kan i et miljø som hverken sanksjonerer feil eller belønner korrekt adferd etablere uvaner» (Reason, 1997 s.73).* Dersom høyere nivåer eller sikkerhetsledelsen ikke i praksis belønner korrekt adferd, og heller ikke sanksjonerer (f.eks. i form av å ta et ekstra kurs) så kan dette oppfattes som kultur for likegyldighet. Denne kulturen kan, som vi har sett med rapportering, forplante seg i de lavere nivåene og etablere en felles organisasjonskultur hvor noe er viktig, mens andre ting er «unødvendig merarbeid».

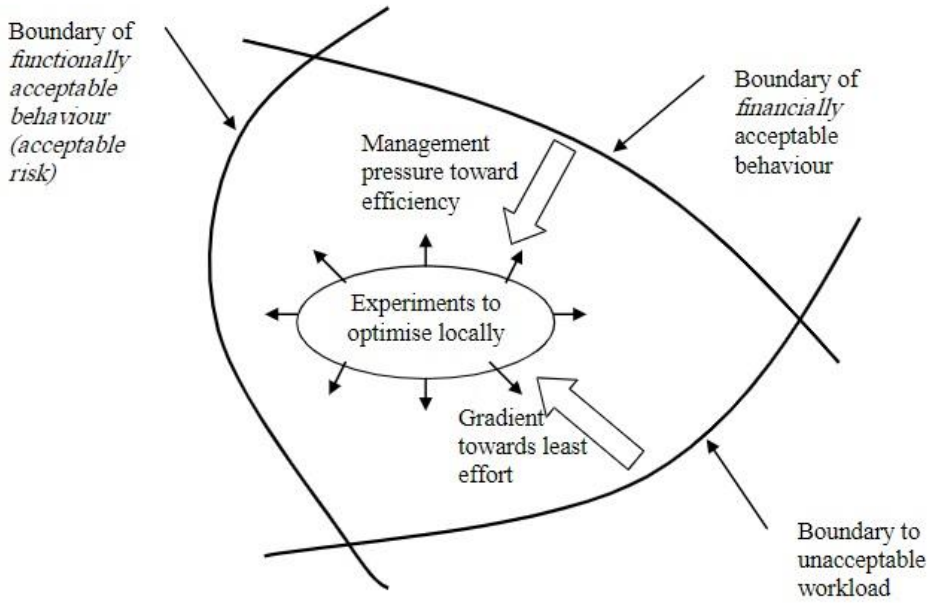
5.2.4 Konkurranse og interessekonflikter favoriserer produksjon over sikkerhet.

En utfordring med dagens risikostyring og rammeverk er at det tilsynelatende ikke adresserer i stor nok grad ulike interesser i organisasjoner, spesielt forholdet mellom produksjon og sikkerhet i utviklingsprosessen (DevSecOps). Dette kom tydelig frem i intervjuene med informant K-1 og K-2 som har utstrakt kontakt med eksterne virksomheter som driver med IT-utviklingsarbeid.

Tilbakemeldingene var at flere utviklermiljø hadde stor eller full frihet til å produsere og en forventning i å få ting i produksjon uten å skulle bli «forsinket» av sikkerhetsfolk og ISO-standarder. Å balansere mellom produksjon og sikkerhet er krevende for virksomheten. I tillegg er det å opprettholde et høyt sikkerhetsnivå også kostnadsdrivende, noe som ble bekreftet av informantene i Equinor. I en slik dragkamp kommer gjerne produksjon ut på topp (Reason, 1997). Til tross for at sikkerhet er viktig, så understreker Aven (2015) at det hele tiden er snakk om en balansegang: *«formålet med risikostyring er å sikre den riktige balansen mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap. Risikostyring er således ikke en ensidig prosess for å redusere risiko i samfunnet eller i bedriften»* (Aven, 2015. s. 14).

Ser man på eksempelet informant K-2 nevner, om entreprenøren i Stavanger som ble offer for et dataangrep, så kan man innvende at ledelsen i dette tilfellet bevisst tok en risiko ved å ikke etablere tilstrekkelige informasjonssikkerhetstiltak. I en konkurranseutsatt bransje med små marginer og tilsynelatende større avstand til digitale sårbarheter i den daglige driften, er det naturlig å tenke at produksjon og økonomisk utbytte presset sikkerhetsmarginen.

Ulike aktører innenfor samme virksomhet kan ha ulike prioriteringer og interessekonflikter. Dette er illustrert i Rasmussens (1997) «migrasjonsmodell». Modellen viser at så lenge aktørene oppholder seg innenfor rammene hvor de kan gjøre fortløpende justeringer og optimaliseringer så opererer man i et trygt miljø (Rosness mfl, 2004). Problemer kan oppstå når grensene flyttes som følge av at aktørene gjør tilpasninger som reduserer det trygge handlingsrommet.



Figur 10: *Migrasjonsmodell – (Rasmussen 1996, Rosness 2004)*

I dilemmaet mellom økt sikkerhet eller økt produksjon, slik det fremkom i intervjuene er det sannsynlig at det gjøres tilpasninger. Ledelsen kan f.eks. øke risikoen i andre deler av virksomheten for å balansere ut kostnadene som må tas på informasjonssikkerhet eller for å være konkurransedyktig. Dette kan gjøre at de ansatte vil bevege sin grense for det de oppfatter som en akseptabel arbeidsbelastning. Utfordringen er imidlertid at det er vanskelig for organisasjonen å vite når de nærmer seg en slik yttergrense, særlig hvis kommunikasjonen internt er mangelfull. En bedre dialog som bidrar til en synliggjøring av hvor grensene går og hvordan man skal forholde seg til dem, er tiltak som kan bidra til å unngå farer (Rosness mfl, 2004).

5.2.5 Store organisasjoner har høyere sårbarhet som følge av kompleksitet

I en organisasjon som Equinor, med mange tusen ansatte, stort antall avdelinger og underleverandører samt svært variert oppgaveportefølje er det nesten umulig å ha full oversikt. Equinor møter informasjonssikkerhetstrusler og sikringstrusler de også, men i kraft av sin størrelse er de potensielt ekstra sårbare.

Bakgrunnen for dette er at det er mange aktører internt som kan ha motstridende interesser. Dette kan være ulike avdelinger, fagmiljø, ledere eller underleverandører. Underleverandører konkurrerer om å vinne og fornye kontrakter, interne avdelinger får mer press om effektivisering og en ledelse som må navigere i et stadig mer uoversiktlig sikkerhetsbilde nasjonalt og internasjonalt. Man har f.eks. sikkerhetseksperter som er satt til å verne om virksomhetens verdier, en ledelse som skal drifte mest effektivt og avdelinger som skal skape verdier, levere et produkt av en gitt kvalitet osv. Ettersom ingen har ubegrensede ressurser, er også Equinor nødt å prioritere. Dersom man skal øke sikkerhetstiltakene som følge av krigen i Ukraina, cyberangrep og øke produksjonen for å imøtekomme energibehovet i Europa, må man omprioritere.

Denne omprioriteringen vanskeliggjøres ved at det er høy kompleksitet og potensielt store avstander mellom nivåer i organisasjonen. En direktør onshore har få forutsetninger for å forstå praktiske implikasjoner i den spisse enden ved å ikke prioritere utskifting av en komponent i felten pga. kostnader. Kommunikasjon mellom nivåene og de ulike avdelingene her er derfor avgjørende (Leveson, 2011). Skal man omdisponere midler fra en produksjonsavdeling og overføre dem til f.eks. informasjonssikkerhet, så må det være en tydelig dialog mellom ledelsen i Equinor og produksjonen for å hindre sårbarheter og justering av forventinger, slik at alle parter er innforstått med de endrede premissene.

Som informant EQ1 i Equinor var inne på, så forutsetter dette god bestillerkompetanse, altså at aktøren i den spisse enden ser, forstår og formidler risikoene opp i systemet, slik at sikkerhetsansvarlige kan viderebringe dette til ledelsen og iverksette passende tiltak. Det må derfor legges til rette for gode feedbackmekanismer og en organisasjonskultur som oppmuntrer rapportering og gir de ansatte en følelse av å bli hørt, for å fortsette med rapporteringen.

En annen utfordring med å være stor og ha en så samfunnskritisk rolle som Equinor har, er at det er mange interessenter inne i bildet, også utenfor virksomheten. Informantene EQ1 og EQ1 fra Equinor forteller om episoder hvor de har opplevd en «kamp om æren», eksemplifisert i

redningsaksjonen av cruiseskipet «Viking Sky» i 2019. «Viking Sky» fikk motorstans utenfor Hustadvika den 23.mars 2019 og skipet drev mot land, med stor fare for grunnstøting. På grunn av full storm i området var det ikke mulig å sette ut livbåter, så redningssentralen på Sola besluttet å evakuere skipet ved hjelp av helikoptre. Til tross for en dramatisk og svært komplisert redningsaksjon, resulterte det i en vellykket operasjon. En av informantene mente at det (…): *«aldri hadde vært mulig å gjennomføre redningsaksjonen uten Equinors evne til å stille med fire av seks helikoptre og refulingsanlegg, men Equinor ble ikke nevnt med ett ord»* (EQ1 og EQ2).

I dette tilfellet var de mest fremtredende aktørene mannskapet på Viking Sky, redningssentralen på Sola, helikopterpilotene, redningsmannskapene og ansvarlige myndigheter osv. Equinors organisatoriske evne til å raskt omstille seg og vilje til å omdisponere helikoptre fra sin egen SAR (Search and Rescue)-tjeneste er nevnt i mindre grad. Dette ble av flere i Equinor opplevd som en liten profesjonskamp mellom de involverte. Den som «vinner» kampen om æren, får gjerne en belønning i form av positiv omtale, økte ressurser eller politisk kapital til å bruke senere.

I tilfellet med Viking Sky, så kan man tenke seg til en situasjon hvor Equinors helikoptre var opptatt et annet sted eller redningsaksjonen var spesielt risikofylt for Equinors egne piloter og materiell. Hvem skulle da «vike» i en eventuell interessekonflikt, og hvordan skulle den bli løst – Ved at en aktør overprøvde vurderinger eller instruerte redningsmannskap eller Equinor? Resultatet av en slik interessekonflikt kunne blitt en katastrofe i form av et stort forlis. Denne type forventninger kan også dukke opp andre steder. Equinor har derfor fokusert på det de omtaler som «samvirkeprinsippet», at man har et tettere samarbeid med andre aktører for å dekke flere eventualiteter. Tett samarbeid, god risikoforståelse og årvåkenhet om at noe plutselig kan skje er alle typiske HRO-kjennetegn (Engen mfl, 2021). Årvåkenheten til Equinor en høy pris, men som vi så med tilfellet i dataangrepet i Stavanger, kan mangel på den samme årvåkenheten og mindre beskyttelse bli kostbart.

5.3 Forskningsspørsmål 3: «Er det andre teoretiske rammeverk som kan benyttes?»

Empirien i dette forskningsprosjektet har vist at til tross for rammeverk, styringssystemer og sikkerhetsdirektiver, så er det fortsatt store utfordringer med tanke på informasjonssikkerheten. Informantene forteller i intervjuene om tradisjonelle trusler, men også nye trusler, som dem mot OT (Operativ teknologi), økt kompleksitet og et mer alvorlig trusselbilde. I tillegg er det tilsynelatende ulike oppfatninger av hva som konstituerer et lite/alvorlig brudd på informasjonssikkerheten. Det er derfor interessant å spørre seg om alternative teorier/tilnærminger kan benyttes. Som grunnlag for drøftingen av dette forskingsspørsmålet vil jeg i hovedsak benytte meg av teoriene presentert i kapittel tre.

5.3.1 Safety-teori er relevant for [Information] Security.

Hvis vi vender tilbake til Tolletatens «Direktiv for sikkerhet», så skiller dette tydelig mellom safety og security. Skillet trekkes primært på intensjon, hvor en villet handling er en «security-handling», som f.eks. i «Information Security» og dem uten intensjon er safety-relatert (Tolletaten, 2020). Utfordringen med denne forståelsen er at et slikt skille ikke alltid er like klart. Flere forskere, blant annet Jore (2017) og Reason (1997) fremhever at handling med intensjon ikke automatisk er en alvorlig security-handling, men også kan ses på som safety-tilfeller.

Intervjuene viste at handlinger som å låse skjermen eller unnlate å rapportere feil, ikke ble valgt som en ondsinnet handling, til tross for et bevisst valg, spesielt i sistnevnte tilfelle. Dette konstituerer en sikkerhetstrussel og et brudd på sikkerhetsinstruksene, og er ifølge definisjonene et security-tilfelle, men som Jore (2017) skriver om organisatorisk sikkerhet: *"The literature on organizational safety has for several decades acknowledged that accidents are neither arbitrary nor random, but rather a result of lack of safety planning"* (Jore, 2017 s.161). Ser man på dette med et organisatorisk safety-perspektiv, så kan slike handlinger være som følge av f.eks. uklare prosedyrer, overregulering som fører til at folk tar snarveier og etablerer uvaner eller skaper dårlig oppslutning rundt rapporteringskultur og sikkerhet (Reason 1997).

Det kan være relevant å se til blant annet Reason (1997) for tanker rundt slike organisatoriske forhold, og Leveson (2011) mtp. en systemisk tilnærming til informasjonssikkerhetsområdet. Særlig relevant er den sosiotekniske modellen, da den godt illustrerer at det er mange aktører inne i bildet, hver med sitt «språk», agenda, ressurser, prioriteringer og hvordan de påvirker hverandre

(Leveson, 2011). Å dreie fokus i større grad over på systemiske årsaker til at sårbarheter i informasjonssikkerheten oppstår, vil gi flere perspektiver og løsninger på informasjonssikkerhetstruslene vi står ovenfor. Det vil derfor være hensiktsmessig å benytte teori og metodikk fra Safety på Security-feltet og informasjonssikkerhet (Information Security) spesielt.

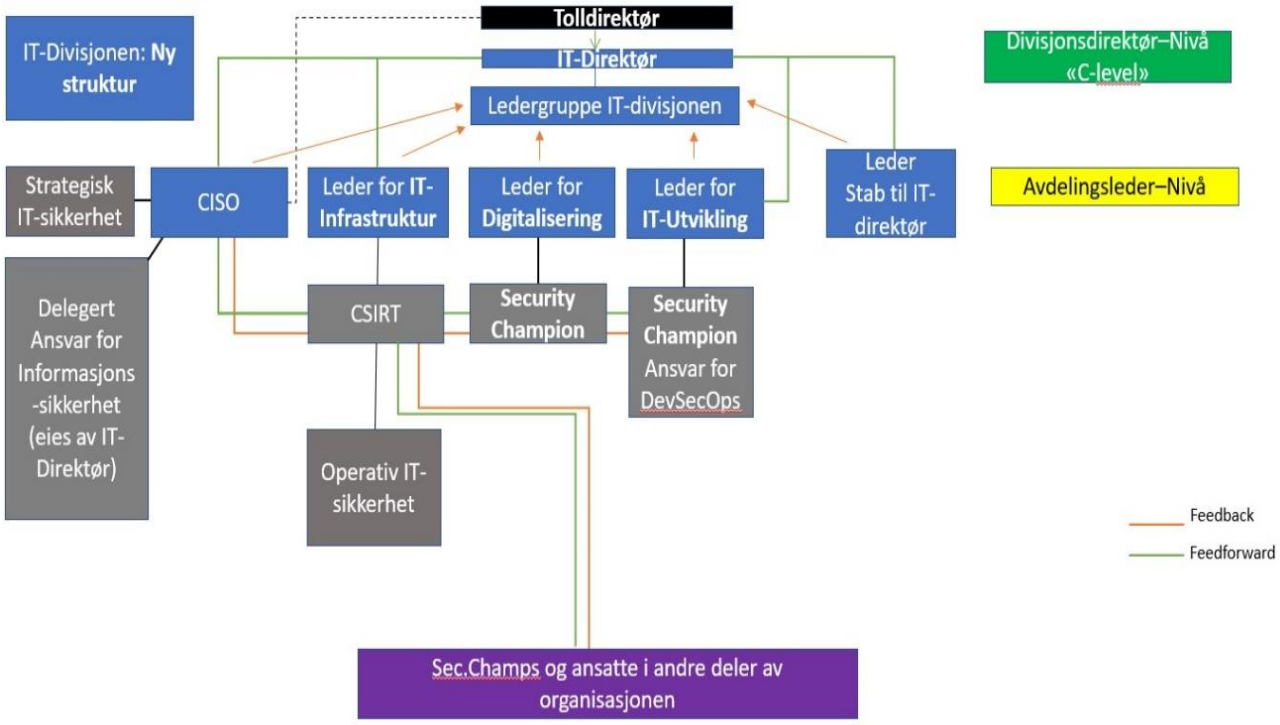
5.3.2 Preskriptiv tilnærming i informasjonsflyten bør revurderes

Intervjuene avdekket også at ansatte og personer i de lavere nivåene i Tolletaten i stor grad ble «informert» når det kommer til informasjon om sikkerhetstiltak, fremfor en løpende dialog. Mange av de forebyggende tiltakene ble formidlet på en klassisk preskriptiv måte, med en sikkerhetsledelse eller toppledelse som formidlet antatt relevant informasjon ned i organisasjonen. En slik ovenfra og ned – formidling gjør organisasjonen som sårbar for informasjonstap eller at det stopper opp, før det kommer helt ned (Turner 1976, Leveson 2011). En flatere struktur og det å engasjere flere deler av organisasjonen i sikkerhetsarbeidet er av Weick, Sutcliffe, & Obstfeld (1999) fremhevet som en av fordelene ved å tenke helhetlig rundt bevissthet om sikkerhet, noe som er sentralt i HRO-teorien.

En alternativ tilnærming for Tolletaten her vil derfor kunne være å flytte *formidlingen* av sikkerhetsinformasjons lavere i organisasjonen og få sikkerhetsinformasjon til å sirkulere internt på avdelingene og i fagmiljøene. Flere av informantene omtalte ordningen med Security Champions, som de mente hadde gitt god effekt hos mange. Å kunne snakke språket til målgruppen man skal utbedre sikkerhetsnivået hos er viktig. Informasjonsdeling mellom fagmiljøene og mellom ansatt-ledelse er kritisk, da man er avhengig av god informasjonsflyt. Dette er noe både Weick, Sutcliffe, & Obstfeld (1999) med HRO og Turner (1976) med sitt rundt informasjonsperspektiv fremhever. Begge disse safety-perspektivene, fokuserer i likhet med Levesons (2011) systemiske tilnærming, på viktigheten av feedback og fortløpende justering av kursen. Parallelt bør sentrale beslutningstakere for informasjonssikkerhet, slik som CISO flyttes opp til ledernivå, for å sikre at toppledelsen fortløpende har det siste av informasjon. Etablering av flere spesialiserte enheter, slik som Tolletatens CSIRT-enhet, og security champions på lavere nivå kan adressere noe av informasjonsflytutfordringen Turner (1976) hevder er bidragsytende til uønskede hendelser.

Figur 11 viser en alternativ organisering av IT-divisjonen i Tolletaten basert på teorien i denne oppgaven. CISO flyttes til avdelingsledernivå og inn i ledergruppen for å kunne ha jevnlig tilgang til beslutningstakere og sørge for at toppledelsen til enhver tid har det siste innen informasjonssikkerhetskunnskap. CISO svarer heller ikke lengre til leder i styringstab, men har selv ansvar for strategisk IT-sikkerhet og beholder overordnet ansvar for informasjonssikkerheten, til tross for at det er delegert. Operativ sikkerhet er i større grad skilt ut og rapporterer til CSIRT som videreformidler dette til CISO. For å sørge for sikker utvikling har utviklingsavdelingen selv ansvar for DevSecOps med sin egen dedikerte Security Champion på dette området.

Det er etablert flere kanaler for feedback og feedforward i den hensikt å legge til rette for en bedre informasjonsflyt opp og ned. Videre har hver avdeling, både i IT-divisjonen og i andre divisjoner fått sin Security Champion, som skal sørge for nærhet til sikkerhetsarbeidet på sin avdeling. Dette skal bidra til tillitt ved at hver avdeling har «sin egen person som snakker deres interesser».



Figur 11: Alternativ tilnærming basert på teori: *«Desentralisert informasjonsformidling og plassering av CISO i IT-divisjonen i Tolletaten»*

5.3.3 Høypålitelig tilnærming funger, men koster mye

Med stadig flere cyberangrep, nye trusselscenarioer og større sikkerhetsrisiko har noen store virksomheter valgt å fokusere ekstra mye på sikkerhet. Her vil jeg trekke frem Equinor som eksempel. Equinor representerer en bransje (olje- og gassnæringen) som har hatt høyt fokus på sikkerhet i flere tiår, og da særlig «tradisjonell» safety siden dette har vært fremtredende i industrien. Equinor har i likhet med tilfellene observert i studiene til Weick, Sutcliffe, & Obstfeld (1999) klart å holde antallet alvorlige hendelser og storulykker lavt, til tross for arbeid i et høyrisikomiljø.

5.3.3.1 Kollektiv bevissthet er krevende, men øker sikkerheten

I intervjuene med informantene fra Equinor, forteller de om Equinors helhetlige og kontinuerlige satsning på høy sikkerhet, inklusiv fysisk sikring og informasjonssikkerhet. Ett av nøkkelordene her er kontinuerlig. Etter utsagn fra informantene, ser hele organisasjonen på hva som kan være feil eller avvik og man rapporterer dette straks, til tross for at det tilsynelatende ikke er alvorlig der og da. Tidligere hendelser, slik som terrorangrepet mot Norge 22. Juli, viste at saken med den forsinkede stengningen av Grubbegata i Oslo potensielt bidro til katastrofen. Informanten fortalte at i Equinor ble det bestemt at: (…) *«Vi skulle ikke ha en Grubbegata-episode, og det ble derfor besluttet å gjøre noe med ting som skulle ha vært gjort, snarest»* (EQ1). Denne tilnærmingen om å ikke vente til noe alvorlig skjer i egen organisasjon, men heller se til andre og lære av dem er i tråd med HRO-teoriens fokus på kollektiv bevissthet og da spesielt rapportering av behandling av nesten-ulykker og potensielle sårbarheter før de manifesterer seg (Weick, Sutcliffe, & Obstfeld, 1999).

Equinors fokus på dette med kollektiv bevissthet adresserer også Turners (1976) bekymringer rundt at feil overses og får utvikle seg. Mengden av informasjon og kompleksiteten i systemer gjør det stadig viktigere å ha bedre oversikt og kontroll, men helst uten bruk av strenge prosedyrer, da slike kan føre til trangt handlingsrom og lede til brudd på regler, som igjen kan føre til ulykker (Reason, 1997). Utfordringen, som begge informantene fra Equinor påpeker, er at denne tilnærmingen er svært kostbar og vanskelig å opprettholde over tid, både i form av tilgjengelige ressurser og den menneskelige belastningen om å alltid være på vakt. Man kan altså argumentere for at dersom man har råd, tid og energi til å opprettholde et høyt sikkerhetsnivå, så vil en HRO-tilnærming adressere en del av sikkerhetsutfordringene nevnt av Turner (1976) og Reason (1997).

En mulighet for å kompensere for de høye kostnadene er å tenke enda større, altså utenfor organisasjonen. Ved å styrke samvirkeprinsippet og dele på kostnader med samarbeidspartnere vil man være i stand til å holde sikkerhetsnivået oppe lengre. Dette krever imidlertid gode ferdigheter i å manøvrere i byråkratiet og blant ulike interessenter, noe informantene også omtalte som en utfordring.

5.3.4. Informasjonssikkerhet og nye trusler

Funnene gjort i intervjuene med informantene med IT- og sikkerhetsbakgrunn har fellestrekket at digitaliseringen og sikkerhetssituasjonen øker kompleksiteten og utfordringen i organisasjonene. Selv «positive» og planlagte endringer som overgangen til skyløsninger innebærer utfordringer som kan være vanskelig å se for organisasjonene. Ledelsen kan ha fokus på kostnadsbesparelse og tilsynelatende mindre å holde oversikt på internt, mens ansatte innen personvern og informasjonssikkerhet kan ha bekymringer rundt teknologi og håndtering som foretas av andre.

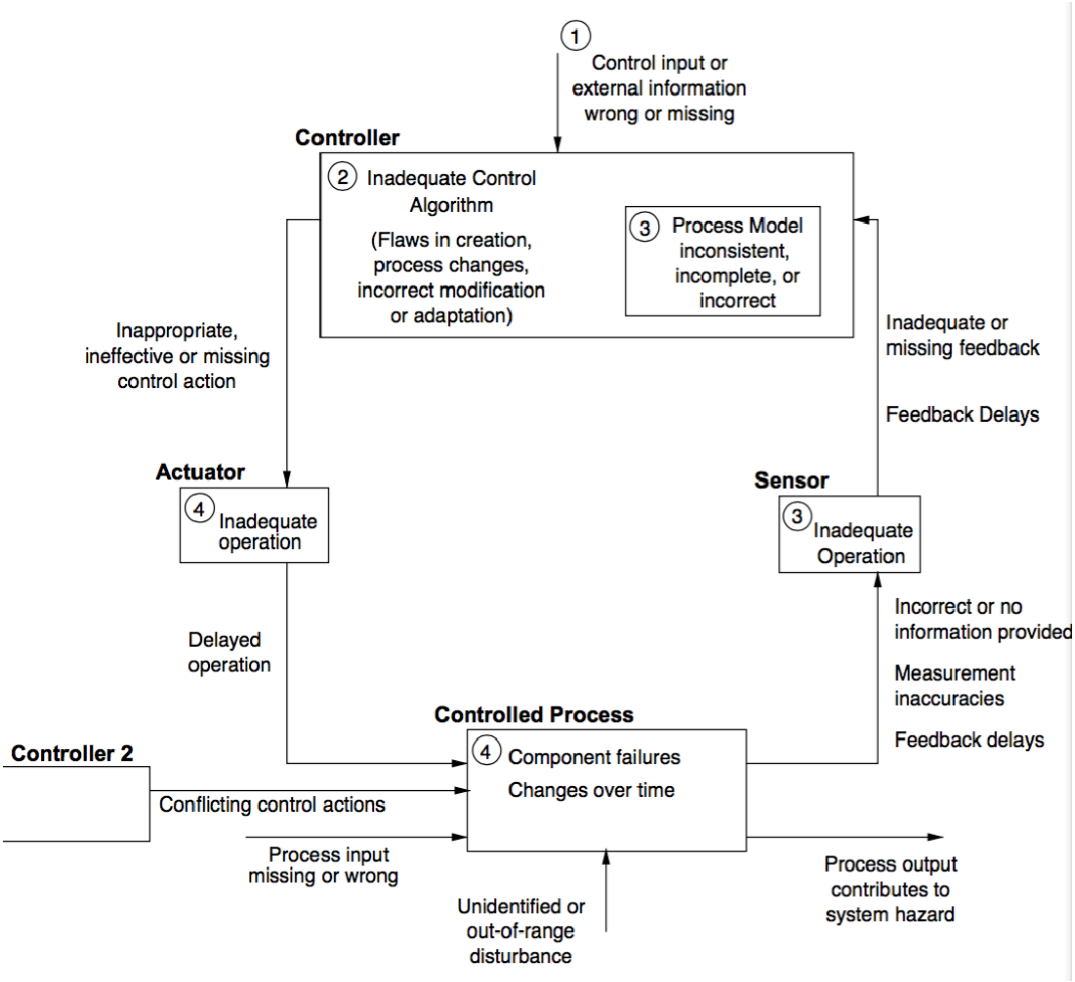
Ledelse og ansatte ellers kan også tenkes å oppleve at omstillingen blir krevende og at avstanden til sikkerhet blir noe større, hvilket kan potensielt bidra negativt på kommunikasjonen og samhandlingen i organisasjonen.

5.3.4.1 Fokus på prosesser som sikkerhetstiltak

Nye trusler som angrep mot operasjonell teknologi (OT) krever også mer av organisasjonene. Infrastrukturen er ofte mye eldre, og det er vanskelig å se farer eller forstå et trusselscenario når man ikke har kjennskap til det fra før. Å vite hvilket «svar» man selv eller systemet skal avgi på en trussel er avgjørende for å velge et tiltak som opprettholder sikkerheten (Leveson, 2011). Kunnskap om arbeidsprosessene som OT-systemene styrer, og effekten cyberangrep kan ha på disse, er kritisk informasjon som raskt må formidles til de som har bruk for den, ifm. ivaretakelsen av sikkerheten. Dette krever en helhetlig forståelse av systemene i organisasjonen, fra topp til bunn. Det systemiske perspektivet til Leveson (2011) er derfor ekstra aktuelt. Dersom ulike deler av organisasjonen har ulik forståelse av hva som konstituerer en fare, enten mot OT eller IT-systemer, så er det en stor sikkerhetsrisiko (Turner, 1976).

Når enkelte sikkerhetsavvik ikke rapporteres vil informasjonssikkerhetsarbeidet bli svekket. Bakgrunnen for dette er at rapportering og feedback fra ulike deler av organisasjonen er avgjørende for å gjennomføre korrekte kontrollhandlinger. Dersom systemets sikkerhetstiltak baserer seg på en antagelse, slik som at de ansatte følger sikkerhetsinstrukser og rutiner for avviksmelding, men

det ikke faktisk er tilfellet, vil dette skape problemer for et velfungerende sikkerhetssystem. Leveson (2011) sin prosessmodell (se figur 7) illustrerer dette godt.



Figur 7: «Klassifisering av kontrollfeil som fører til ulykker» (Leveson, 2011. s.93)

Skriving av prosedyrer eller design av sikkerhetssystemer gjøres gjerne på bakgrunn av et visst risikobilde. Hvis risikobildet er feil eller mangelfullt (1) vil dette prege designet av kontrollmekanismene og prosessmodellen (2) + (3). Dette utgangspunktet vil få følgefeil i sikkerhetssystemet og føre til problemer som forsinkelser og feilhandlinger, (4) samt dårlig feedback pga. manglende rapportering (Leveson. 2011). Når disse problemene sirkulerer i et system som omfatter informasjonssikkerhet, så vil det forsterkes av at stadig flere aktører (Controller 2) kommer inn i systemet og tilfører det kompleksitet, enten ved økt datamengde eller via egne arbeidsrutiner og handlingsmønstre. Når systemet ikke er designet for disse variablene vil det føre til feilhandlinger og forsinkelser som svekker sikkerheten til systemet som helhet.

Ved manglende rapportering fra det modellen beskriver som «sensorer», f.eks. de ansatte i organisasjonen får ikke systemet tilstrekkelig rask tilbakemelding for å redesignes fortløpende for å inkorporere de stadig nye variablene. Det blir da vanskelig å «bryte ut» av det opprinnelige feildesignet. Denne prosessen vil gjenta seg, og man har nå etablert en systemfare. Til tross for at man har prosesser, rutiner og antatt kontroll på informasjonssikkerheten, så vil den til slutt resultere i en hendelse.

Funnene som ble gjort i intervjuene viser at den interne informasjonsflyten er av vesentlig betydning i sikkerhetsarbeidet. En systemisk tilnærming var imidlertid ikke spesifikt nevnt av informantene, ei heller hvordan et slikt perspektiv kunne påvirke den totale sikkerheten.

Ved å benytte Levesons (2011) systemiske prosessmodell for sikkerhet vil flere organisasjoner kunne bli oppmerksomme på hvordan de ulike delene av organisasjonen påvirker hverandre. En slik forståelse blir stadig viktigere, spesielt når det kommer til et område som informasjonssikkerhet, da dette utvikles og endres raskt. Sikkerhetssystemet- må derfor også raskt kunne justeres for å ta høyde for nye og komplekse trusler. Et fokus på prosesser, fremfor enkelttiltak og standarder vil derfor kunne være hensiktsmessig.

5.3.4.2 Forebygging og dialog som verktøy

Ettersom mange av de nye truslene er mot områder som tradisjonelt sett ikke har vært koblet på nett, slik som OT, er det vanskelig å forutse hvordan en hendelse vil manifestere seg. Fremfor å prøve å forebygge en ukjent trussel kan det være hensiktsmessig å dreie fokuset over på resiliens og hvordan raskere komme tilbake. Et skifte fra å forebygge til å håndtere hendelser, fremstår som ekstra aktuelt i møte med trusler og farer man ikke kjenner til. HRO-er har etablert en tilnærming her som kan være verdt å se nærmere på, slik som at det ikke forutsettes at kjente risikoer og tidligere erfaringer gir grunnlag for korrekt håndtering i fremtiden (Weick, Sutcliffe, & Obstfeld, 1999).

I Equinor har de blant annet inkorporert sikkerhetsavtaler i kontrakter med underleverandører og har jevnlige møter disse (EQ1 og EQ2). Tett dialog mellom dem som lager retningslinjene for sikkerhet (Equinor) og dem som håndhever dem (underleverandører) er viktig da outsourcing kan svekke sikkerhetskulturen i hoved/kjøper-organisasjonen ved at underleverandører potensielt kan ha et «minimumsfokus» på sikkerhet. En avvikende sikkerhetskultur hos underleverandøren kan slik påvirke totalsikkerheten negativt.

Lignende problemstilling kom til syne rundt sikker utvikling, da flere av informantene fortalte om utviklere sitt fokus på produksjon på bekostning av sikkerhet, en avveining Reason (1997) påpeker er krevende.

Tett dialog med underleverandører handler heller ikke bare om viktigheten av å ha en god sikkerhetskultur. Det handler vel så mye om å forstå behovene og kulturen i kjøperorganisasjonen og verdiene de er satt til å forsvare.

Et annet moment er god bestillerkompetanse hos ledelsen. Forståelsen for sikkerhetsbehovet i alle deler av organisasjonen og løsningene som er tilgjengelig på markedet må være til stede hos lederne som inngår kontraktene. Dette igjen krever at alle nivåer og avdelinger er inkludert og formidler sine behov til beslutningstakere. Her vil security champions kunne løfte opp og konkretisere ulike avdelingers interne bekymringer og behov, slik at man får et tydeligere risikobilde. Å etablere klare feedbackkanaler slik som Tolletaten gjorde, vil deretter kunne løfte det justerte bildet opp til ledelsen. Videre bør dialogen mellom miljøene som representerer nye og gamle sikkerhetsutfordringer (henholdsvis OT og IT) gjennomføre sikkerhetsøvelser sammen og spre et omforent budskap om sikkerhet i hele organisasjonen.

6. Konklusjon

I oppgaven ble Tolletaten benyttet som case, men det ble også trukket inn andre aktører, slik som Equinor og eksterne virksomheter som sammenligningsgrunnlag grunnet størrelse og kompleksitet og som datakilde.

Målet med oppgaven har vært å besvare problemstillingen:

«Hvordan organisere sikkerhetsarbeidet for å øke informasjonssikkerheten i Tolletaten?».

For å svare på problemstillingen har jeg gjennom drøftingen av forskningsspørsmålene, med bakgrunn i safety- og systemteori, samt funn i empirien, kommet til følgende konklusjon:

Tolletaten benytter seg av anerkjente standarder og rammeverk som ISO27001, NIST mm. i informasjonssikkerhetsstyringen. Tolletaten har organisert sitt sikkerhetsarbeid etter enheter og funksjoner i en divisjonsbasert organisasjonsmodell. Både Tolletaten og Equinor prioriterer informasjonssikkerhet og jobber kontinuerlig for å forbedre og opprettholde et høyt sikkerhetsnivå. Begge virksomheter har et eget apparat for å håndtere og jobbe med informasjonssikkerheten.

Dette inkluderer også det å formidle informasjon ut i organisasjonen og øke bevisstheten rundt risikoer.

Funn gjort i denne studien tyder på at de største informasjonssikkerhetsutfordringene i store og komplekse organisasjoner er knyttet til informasjonsflyt og samhandling mellom- og på tvers av nivåene i organisasjonen, sikkerhetskultur og felles risikoforståelse. Funnene indikerer også at store organisasjoner fortsatt til en viss grad opererer med en hierarkisk organisasjonsstruktur som bidrar til siloeffekter, uklare ansvarsforhold og tidvis motstridende interesser. Det å balansere effektiv drift og sikkerhet oppfattes som spesielt krevende. Mangelfull inkludering av alle nivå fører til økt risiko for at man går glipp av viktige innspill og kunnskap om farer i den spisse enden, samt viktigheten av å være oppmerksom på særegne kulturelle faktorer som eksisterer i ulike deler av organisasjonen.

Selv om sikkerhetsarbeidet hos Tolletaten, i Equinor og trolig hos andre aktører er høyt prioritert og er god, er det likevel områder som de og andre komplekse virksomheter kan ha nytte av å se nærmere på. Disse er formulert som mine anbefalinger under punkt 6.1.

6.1 Anbefalinger:

For å øke informasjonssikkerheten anbefaler jeg følgende tiltak:

1) Økt fokus på prosesser i arbeidet med informasjonssikkerhet. Betydningen av informasjonsflyten og hvordan den påvirker de andre aktørene, gjennom et helhetlig og systemisk perspektiv bør vies større oppmerksomhet. Dette gjelder særlig i komplekse organisasjoner med mange aktører som har ulike ansvarsområder.

2) Organisasjonene må være bevisst på at sikkerhetstiltak kan forårsake skjulte og åpne interessekonflikter. Interne aktører kan ha egen agenda, ulik risikoappetitt og egne økonomiske insentiver som kan redusere den totale sikkerheten.
   Interne interessentanalyser i forkant, sammen med tydelig kommunikasjon og forventninger, er viktig for å redusere spenningen. Dersom det er uenigheter bør det eksistere en aktør med vilje, evne og autoritet til å skjære gjennom.

3) Organisasjonskulturen bør tillegges større vekt i arbeidet med utforming av sikkerhetsrutiner. Hva som anses viktig på de lavere nivåene bør undersøkes nærmere da det ikke nødvendigvis eksisterer en omforent risikoforståelse i hele organisasjonen.

4) Det bør jobbes for å inkludere hele organisasjonen, samt underleverandører i sikkerhetsarbeidet. Erfaringsutveksling mellom sikkerhetsmiljøer og andre deler av virksomheten bør gjennomføres regelmessig for å lære av hverandre.

5) Man bør i større grad innføre positive tilbakemeldinger og mer synlig belønning til dem som rapporterer inn avvik. Dette vil bygge tillitt og gi insentiv til økt rapportering. Det må etableres gode feedforward og feedback-kanaler som gjør det enkelt å formidle informasjon internt i organisasjonen.

6) Ledere og mellomledere må ha en helhetlig forståelse av informasjonssikkerhet, som strekker seg utover egen avdeling. Sikkerhet må vies tilstrekkelig tid blant toppledelsen, og fageksperter må gis tyngden og påvirkningsmulighet rollen deres krever.

7) Desentralisert risiko- og sikkerhetsstyring bør få større plass. Å ha sikkerhetseksperter flere steder enn blant ledelsen, vil bidra til kortere reaksjonstid og økt forståelse av sikkerhet som fagområde blant medlemmer på de lavere nivåene.

6.2 Anbefalt videre forskning

Det foreligger forholdsvis lite forskning om hvordan safetyteori kan benyttes på securityfeltet, og på informasjonssikkerhetsfeltet spesielt. Ytterligere forskning som kan belyse hvorvidt virksomhetene selv har vurdert andre tilnærminger enn dem som er mer forbundet med etablert securityteori hadde vært interessant.

Da denne studien er en enkelt case-studie kan ikke funnene generaliseres til å gjelde alle komplekse organisasjoner. Hvorvidt f.eks. utenlandske offentlige etater og virksomheter skiller seg fra norske med tanke på risikostyring og informasjonssikkerhet hadde vært spennende å vite mer om. Dette er særlig aktuelt da globalisering og digitalisering gjerne fører til mindre tydelige skiller mellom det nasjonale og internasjonale, også på sikkerhetsområdet.

Det har ikke vært mulig å få innblikk i toppledere sitt perspektiv grunnet tilgangen på slike informanter og begrensninger i oppgavens omfang. Deres syn og prioriteringer hadde vært av interesse, da det er disse som fatter beslutninger som får følger for hele organisasjonen. Hvorvidt det eksisterer kulturforskjeller mellom ledere og andre medlemmer av organisasjonen, som kan påvirke sikkerhetsarbeidet, er også relevant sett i sammenheng med funnene gjort i denne studien.

Referanser

Aven, T. (2015). *Risikostyring.* Oslo: Universitetsforlaget.

Dekker, S. (2014). *The Field Guide to Understanding Human Error.* Boca Raton, FL: Taylor & Francis Group.

Engen mfl, O. A. (2021). *Perspektiver på samfunnssikkerhet.* Cappelen Damm AS.

Guldenmund, F. (2000). The Nature of Safety Culture: A Review of Theory and Research. *Safety Science 34*.

Halvorsen, K. (2008). *Å forske på samfunnet: En innføring i samfunnsvitenskapelig metode.* Oslo: Cappelen Akademisk.

Internkontrollforskriften. (u.d.). *lovdata.no*. Hentet fra https://lovdata.no/dokument/SF/forskrift/1996-12-06-1127.

Johannesen mfl., A. (2010). *Introduksjon til samfunnsvitenskapelig metode.* Abstrakt forlag AS.

Jore, S. (2017). The Conceptual and Scientific Demarcation of Security. *European Journal for Security Research*.

Kruger, R., & Casey, M. (2015). *Focus Groups - A Practical gyude for Applied Research.* California: SAGE Puplications, Inc.

Laporte, T., & Consolini, P. (1991). Working in Practice but Not in Theory: Theoretical Challenges of "High-Reliability Organizations". *Journal of Public Administration Research and Theory: Vol. 1 No.1*.

Leveson, N. (2011). *Engineering a Safer World - Systems Thinking Applied to Safety.* Massachusets, USA: MIT Press.

Leveson, N., & Thomas, J. (2018). *STPA Handbook.* Leveson, Nancy; Thomas, John.

Rasmussen, J. (1990). Mental models and the control of action in complex environments. *In Mental Models and Human - Computer Interaction*, 41-69.

Reason, J. (1997). *Managing the Risk of Organizational Accidents.* New York: Routledge.

Rosness mfl, T. (2004). *Organisational Accidents and Resillient Organisations: Five Perspektives.* Trondheim: SINTEF.

Sikkerhetsloven. (2019). *Lovdata.no*. Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-01-24.

Thagaard, T. (2018). *Systematikk og innlevelse - En innføring i kvalitative metoder.* Vigmostad & Bjørke AS.

Tolletaten. (2020, Oktober). Direktiv for sikkerhet. Oslo.

Turner, B. (1976). *The Organizational and Interorganizational Development of Disasters*, Adminstrative Science Quarterly, Vol 21, No 378-397.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for High Relibility: Processes of Collective Mindfulness. *Research in Organizational Behaviour, Vol.1*.

Wildavsky, A. (1991). *Searching for Safety.* New Brunswick: Transaction Books.

Vedlegg 1: Samtykkeskjema med godkjenning fra NSD

Samtykkeskjema for deltakere i forskingsprosjektet:

Vil du delta i forskningsprosjektet

«Hvordan organisere sikkerhetsarbeidet for å øke informasjonssikkerheten i Tolletaten?»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å se nærmere på organiseringen av sikkerhetsstyringen i store virksomheter kan øke informasjonssikkerheten. Hvordan påvirker organisering arbeidet med informasjonssikkerhet og har det en effekt på andre områder?

I dette skrivet gir jeg deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Jeg er en student som har gått masterstudiet i Risikostyring og sikkerhetsledelse ved Universitetet i Stavanger siden våren 2021. Jeg planlegger å levere masteroppgaven min til våren 2023. Jeg har jobbet i Tolletaten siden 2011 og har en variert bakgrunn med både yrkesutdanning fra Tollskolen og høyere utdanning innen samfunnsvitenskapelig fag. Jeg jobber for tiden i vareførselsdivisjonen i Tolletaten i Bergen.

Formål

Forskingsprosjektet er en masteroppgave i Risikostyring og sikkerhetsledelse som utforsker hvordan organisering påvirker sikkerhetsstyring i store virksomheter. Oppgavens fokus er sikkerhetsstyring med vekt på organiseringens påvirkning på informasjonssikkerhet, da de fleste virksomheter, på lik linje med samfunnet gjennomgår store digitaliseringsprosesser.

Organisatoriske endringer kan påvirke både arbeidsoppgaver, samt hverdagen til de ansatte og ledere i virksomheten. Hvordan fungerer sikkerhetsstyringen etter gjeldene organisering og kan alternativer til dagens organisering benyttes?

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Stavanger er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Jeg ønsker at du deltar da din erfaring og kunnskap om organisasjonen kan være til hjelp med å svare på problemstillingen. Du jobber i en stor virksomhet som har ulike former sikkerhetsarbeid høyt på agendaen og jeg er interessert i dine erfaringer med sikkerhetsarbeid, informasjonssikkerhet og sikkerhetsstyring.

Hva innebærer det for deg å delta?

For å finne svar på problemstillingen ønsker jeg å gjennomføre semistrukturerte fokusgruppeintervjuer samt en-til-en intervjuer hvor dette er aktuelt. Et fokusgruppeintervju er et intervju hvor du deltar sammen med andre og har en samtale om de temaene og spørsmålene jeg på forhånd har laget i intervjuguiden. Samtalen vil være uformell av art og du oppfordres til å snakke fritt.

Det vil kunne bli stilt oppfølgingsspørsmål slik at synspunktene og erfaringene dine kommer tydeligere frem. Ledere og ansatte vil ikke bli plassert i samme fokusgrupper. Identiteten til deg som deltaker vil anonymiseres.

Jeg vil ta notater og lydopptak av samtalen som gruppen har. Dette gjøres for å fange opp nyanser i dialogen og sørge for at viktig informasjon ikke går tapt. Varigheten på intervjuet er beregnet til ca. 1.time. Intervjuet kan skje fysisk eller digitalt. Tid og sted avtales dersom du samtykker til å delta.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

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

Det er kun jeg som har tilgang til opplysningene og informasjonen. Dette vil ikke bli delt med andre, heller ikke din arbeidsgiver. Identitet- og kontaktinformasjonen din vil ikke bli brukt på en måte slik at du kan identifiseres. Innsamlede data vil kun behandles av meg og kun jeg vil ha tilgang til dataene.

Personopplysningene dine vil bli lagret adskilt fra andre data og navn og kontaktinformasjon vil bli endret til en anonym deltakerkode. Jeg vil selv stå for transkribering av intervjuene og de vil ikke bli lagret eller behandlet utenfor EU/EØS.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Prosjektet vil etter planen avsluttes juni 2023. Etter prosjektslutt vil datamaterialet med dine personopplysninger anonymiseres og lydopptak slettes senest ved godkjenning av masteroppgaven.

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

På oppdrag fra Universitetet i Stavanger har NSD vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

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

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

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

- Universitetet i Stavanger ved Christian Henrik Alexander Kuran på epost: christian.h.kuran@uis.no
- Vårt personvernombud på Universitetet i Stavanger: Rolf Jegervatn. Epost: personvernombud@uis.no,

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med: Personverntjenester på epost (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Baste M. Ramsdal

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *«Hvordan organisere sikkerhetsarbeidet for å øke informasjonssikkerheten i Tolletaten?»* og har fått anledning til å stille spørsmål.
Jeg samtykker til:

- Å delta i fysisk intervju sammen med studenten og det tas lydopptak av samtalen. Alternativt via digital videokonferanse med opptak.
- At kontaktinformasjon, lydopptak og data lagres utover planlagt tid, dersom prosjektet ikke fullføres etter planlagt tidsramme, men at jeg skal få informasjon om dette.

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, senest 18. juni 2023.

(Signert av prosjektdeltaker, dato)

Vedlegg 2: Intervjuguider (1-3):

Intervjuguide 1: Interne Informanter med IT-bakgrunn:

Innledning:

Velkommen, takk for at du deltar i studien.

Hva er din rolle i organisasjonen og relasjon til sikkerhetsarbeid?

Organisering & Samhandling: 15min

1) Hva er det teoretiske rammeverket for dagens organisering for informasjonssikkerhet?
2) Hvordan funger dagens IT-sikkerhetsstyring i praksis?
3) Hvordan opplever du dagens to-delte organisering på sikkerhetsområdet?
4) Hvordan opplever du tilgangen på beslutningstakere?
5) Hvordan opplever du samarbeidet om sikkerhet i de ulike delene av virksomheten?
    a. Opplever du organisatoriske utfordringer mtp. sikkerhetsstyringen i dag?
    b. Hvordan opplever du informasjonsflyten opp- og nedover i organisasjonen?

Sikkerhet & Sikkerhetskultur: 20 min

1) Hvilke utfordringer står virksomheter ovenfor med økt digitalisering?
2) Opplever du at ledelsen forstår og prioriterer nye sikkerhetstrusler?
3) I hvilken grad opplever du at faglige råd anerkjennes av ledelsen?
4) Hvordan opplever du rapporteringen og håndteringen av avvik i virksomheten?
5) Kunne sikkerhetsarbeidet vært organisert på en annen måte?

Refleksjoner: 10min

1) Er det noe du savner i tilnærmingen til informasjonssikkerhet i virksomheten?

Avslutningsspørsmål: 5min

- Er det noe mer du ønsker å legge til?

Intervjuguide 2: Eksterne konsulenter innen informasjonssikkerhet:

Innledning:

Velkommen, takk for at du deltar i studien.

Organisering/Samhandling:15min

6) Hvordan er sikkerhetsarbeidet i virksomhetene du besøker vanligvis organisert?
7) Hvordan funger sikkerhetsstyringen i en slik virksomhet?
8) Hvordan opplever du samhandlingen mellom Safety og Informasjonssikkerhet avd.?
9) Hvordan opplever du informasjonsflyten rundt sikkerhet i virksomhetene?

Avvik & Sikkerhetskultur ute hos kundene: 15min

6) Hvordan opplever du rapporteringen og håndteringen av avvik i kunden?
    a. Hva gjøres for å legge til rette for innmelding av avvik/rapportering?
7) Hva slags forhold har en typisk kunde til begreper som «Sikkerhetskultur»?
8) Hvilke tiltak foreslår dere for å bedre sikkerhetskulturen hos kunden?

Sikkerhet: 15min

1) Hva opplever du som den vanligste IT-sikkerhetsutfordringen hos kunden?
2) Hvordan opplever du viljen fra virksomhetene til å gjennomføre nye sikkerhetstiltak?
3) Hvilke sikkerhetsutfordringer tror du blir mest krevende fremover?

Avslutningsspørsmål: 5min

- Er det noe mer du ønsker å legge til?

Intervjuguide 3: Sikringsrådgivere fra Equinor:

Innledning:

Velkommen, takk for at dere deltar i studien.

Organisering/Samhandling: 15min

10) Hvordan er sikkerhetsarbeidet i Equinor organisert?
    a. (fells sikkerhet, Safety og Security delt? IT-sikkerhet for seg selv?)
11) Hvordan funger sikkerhetsstyringen i praksis?
12) Hvordan opplever du samhandlingen mellom Safety og Informasjonssikkerhet?
13) Hvordan opplever du informasjonsflyten internt rundt sikkerhet i Equinor?
    a. Er det noen punkter du tenker er ekstra relevant her?

Avvik & Sikkerhetskultur: 15min

9) Hva opplever du som den vanligste sikkerhetsutfordringen i dag?
10) Hvordan opplever du rapporteringen og håndteringen av avvik i Equinor?
11) Hva gjøres for å legge til rette for innmelding av avvik/rapportering?
12) Hvilke tiltak tas for å bedre sikkerhetskulturen i Equinor?

Sikkerhet: 15min

4) Hvilke eksterne og interne forhold opplever du vanskeliggjør sikkerhetsarbeidet?
5) Hvordan opplever du viljen fra ledelsen til å gjennomføre nye sikkerhetstiltak?
6) Hva opplever du som en utfordring når det gjelder å holde et høyt sikkerhetsnivå?
7) Hvilke sikkerhetsutfordringer tror du blir mest krevende fremover?

Avslutningsspørsmål: 5min

- Er det noe mer du ønsker å legge til?