Hvordan kan en ved hjelp av risikostyringsverktøy reduser sårbarheten og heve sikkerheten for informasjonssikkerhet i kraftforsyningssektoren.

Informasjonssikkerhet i et samfunnsperspektiv

Universitetet i Stavanger Masteroppgave 2017

Laila Refsland

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER: Høst 2017

FORFATTER:

Laila Refsland

VEILEDER:

Sinde Aske Høyland

TITTEL PÅ MASTEROPPGAVE:

Hvordan kan en ved hjelp av risikostyringsverktøy redusere sårbarheten og heve sikkerheten for informasjonssikkerhet i kraftbransjen

EMNEORD/STIKKORD:

Risikopersepsjon, Risiko, Risikobilde, Risikostyring, sårbarhet, sikkerhet/safety, informasjonssikkerhet, Sikring/security

SIDETALL: 81 (inkludert litteraturliste og vedlegg)

STAVANGER 18.10.2017

Forord

Denne oppgaven marker slutten av studiene erfarings basert master innen Risikostyring og Sikkerhetsledelse. Det har vært svært lærerikt, til tider kjekt og til tider svært travelt.

Det er mange som fortjener en takk i dette forordet, alt fra forelesere til alle medstudenter, som en har blitt kjent med gjennom studie. De jeg ønsker å trekke fram og gi en ekstra takk til i dette forordet, er informantene som stilte opp og delte sin tid og kompetanse med meg. Denne oppgaven hadde ikke blitt til uten deres engasjement under intervjuet som også førte til at jeg måte skrive om og reorganisere oppgaven. Videre vil jeg rette en takk til min veileder Sindre Aske Høyland for god støtte og finne innspill, som ga meg en trygghet om at jeg var på riktig retning. En takk til Ruth Ø. Skotnes og Sissel Johre for innspill til litteratur som ble brukt i denne oppgaven.

Vil også rette en takk til tidligere kollegaer og medstudenter. Som har hørt på frustrasjon og vært med meg på oppturer og nedturer i denne prosessen, og ikke minst for korrektur lesing Takk Laila Ueland Lunde. En takk til min tidligere arbeidsgiver ResQ for hjelp med innbinning og kopiering.

En stor takk må gå til mannen min og barna mine som tålmodig har levd med bøker og papirer overalt i huset i de siste par månedene. Til slutt en stor takk til bestefar som har passet barna, hund og katt og fått denne familien til å fungere i denne prosessen. Uten hans innsats hadde det vært vanskelig.

Laila Refsland

Stavanger 18.oktober 2017

Sammendrag

Bakgrunn for denne oppgaven startet som en nysgjerrighet til informasjonssikkerhet og dette med sikring/Security. Det har vært mye oppe i media om hendelser fra flere bransjer og ønsket å se på dette med informasjonssikkerhet i min masteroppgave. Ønsket var å finne ut hvordan kan en få en bedre informasjonssikkerhet ved hjelp av styringsverktøyer som er presentert gjennom studie risikostyring og sikkerhetsledelse. Ønsket også å ha et fokus på sikring/security siden av sikkerhet, for denne må være med når en snakker om informasjonssikkerhet. Valget falt da på kraftbransjen og nettselskapene. Grunnen til at det ble kraftselskapene og da nettselskapene jeg ønsket å se på. Er deres samfunnsfunksjon som kritisk infrastruktur. Bransjen er kjent for å ha god redundans men det kan ramme mange om en ikke klarer å få strømmen ut til kundene, som er alt fra private til industri og offentlige virksomheter som sykehus, sykehjem og skoler.

Formål med oppgaven er å vise viktigheten av å ha en helhetlig risikostyring av organisasjonene. I dette legger jeg at det er viktig å implementere informasjonssikkerhet inn i styringssystemet en har, for å få en helhetlig styring av risikoen. Teori valget i denne oppgaven er hovedsakelig hentet fra teorier rundt risiko, sikkerhet og sårbarhet.

Metoden for denne oppgaven falt valget på en kvalitativ metode. Det ble utarbeidet et forskningsdesign som baserer seg på Blaikie (2010). Der det ble utarbeidet forskningsspørsmål som skulle hjelpe meg i å finne et svar på problemstillingen min. Det ble utført intervjuer og dokumentanalyser i oppgaven.

Resultat har blitt en oppgave som viser at det er noen utfordringer når det gjelder informasjonssikkerhet. Utfordringene går på risikoforståelse, risikoanalyser og kunnskap rundt sikring/security.

Konklusjon av denne oppgaven er at den gir ikke en oppskrift på en bestemt måte å drive med risikostyring på for å oppnå suksess. Den viser at en må jobbe systematisk med risikostyring, en må bruke de verktøyene som egner seg best for å få fram risikoene, som ligger under informasjonssikkerhet. Til dette har oppgaven vist at det er verktøy tilstede. Det kreves kjennskap til verktøyene som kan brukes innen risikoanalyse for å få en god risikostyring. I denne oppgaven var det noe som viste seg å gå igjen i alle intervjuer og dokumenter. Dette med sikringskultur dette ble et kjernefunn, sikringskultur er det en mangel på. Dette var ikke noe

som jeg så for meg ville bli så framtredende, men det viser seg at dette er noe en må jobbe med i organisasjoner for å få. Det kan være vanskelig å ta informasjonssikkerhet og sikring/security delen av sikkerhet innover seg før en har en form for sikringskultur tilstede. Dette gir grunnlag for videre oppgaver rundt dette emnet informasjonssikkerhet.

Innholds-
fortegnelse

Figurliste

Tabell liste

1 Innledning

Våren 2016 var jeg deltaker på det første kurset på master nivå innen sikring/Security ved Universitetet i Stavanger – Risikostyring og sikkerhet til tilsiktede hendelser. Det var to dager med informasjonssikkerhet og dette fanget min interesse. Da vi kom til slutten av kurset fikk vi spørsmålet av faglærer Sissel Jore hva var bra, og hva kunne vært bedre? Ble litt overrasket av svarene som kom i klassen. De fleste følte at to dager med informasjons sikkerhet var for mye. Dette ble jeg litt nysgjerrig på, fordi det er et så stort område og berører oss som et samfunn i mye større grad, enn trusselen om mulig terror. Ikke at terror og forebygging av dette er mindre viktig, men sett med organisatoriske øyne vil dette med å forstå, eller få en god forståelse av dette med informasjonssikkerhet være viktig. Vi lever i ett av de mest digitaliserte landet i verden. Dette gjør oss sårbare. I følge NOU (2016:19) vil trusler mot det digitale rom øke, av at samfunnets økte avhengighet av informasjons- og kommunikasjonsteknologi (fra nå forkortet IKT) baserte informasjonssystemer. Dette vil føre til sårbarheter og trusler i det digitale rom.

Når det kommer til sikkerhetsbrister i IKT så er dette et sammensatt problem. Det er ikke bare barrierene som er bygget inn i systemene som benyttes av organisasjonene, men mye handler faktisk om bruken av systemene. Det å kunne utføre de nødvendige oppdateringene av systemene. Lar en all risikostyring være opp til IKT eller IT avdelingen så mister en gjerne helheten i organisasjonen når det gjelder informasjonssikkerhet.

I følge Traaviks innlegg på sikkerhetskonferansen ved UiS 2017. Snakket han en del om at det er mye som er bra innen sikkerhets arbeid innen tilsiktede hendelser men mange drar i ulike retninger. Dette belyses noe i NOUen samhandling for sikkerhet (2016) som ligger til høring.

Når det kommer til sikkerhet/safety og sikring/security så er ikke forskjellene så uendelig store. Det er noen særegenheter ved sikringsfaget blant annet usikkerhet som hva, hvordan og når kan et angrep skje. Innen sikring/security så har en også en tenkende angriper. Hackeren letter etter sårbarhetene i systemet, og finner de mulige omveier som trengs for å komme seg inn. Det vil si at en må sikre seg mot alle typer angrep for å ha god sikkerhet men angriperen trenger bare å finne et sikkerhetshull. For

å ha en helhetlig sikkerhets forståelse inn i risikostyringen så innebærer det at en har tekniske sikkerhets barrierer, sikkerhetskritiskatferd, risikoforståelse, beredskapshåndtering, organisatoriske sikkerhetsbarrierer og systemanalyse/organisasjonsutvikling. En må være i stand til å beherske ulike tilnærminger for å forstå og analysere hendelser og risiko. Være i stand til å differensiere mellom ulike typer hendelser.

Oppsummert så er hensikten med denne oppgaven å se på hvordan kan en integrere informasjonssikkerhet inn i tankesettene våre når det kommer til vurdering av risiko og risikostyring, er verktøyene tilstede for å kunne få dette godt nok til, eller er det en manglene kunnskap om verktøyene. Kraftforsyning har en samfunnsfunksjon som omfatter systemer og leveranser som er nødvendige for å ivareta samfunnets behov for elektrisitet (DSB 2016). Dette er grunnen til at jeg velger å se på kraftbransjen i denne oppgaven.

1.2 problemstilling

Følgende problemstilling danner grunnlaget for denne oppgaven:

Hvordan kan en ved hjelp av risikostyringsverktøy, redusere sårbarheten og heve sikkerheten for informasjonssikkerhet i kraftbransjen.

For å kunne finne svarene på denne problemstillingen er det valgt ut følgende forskningsspørsmål:

1. Hvilke fordeler og ulemper finner vi i risikostyringsverktøyene
2. Hvordan kan en redusere sårbarheten i kraftforsyningssektoren.
3. Hvor viktig er det at ledelsen er involvert og forstår risikobilde
4. Hvordan bedre sikkerheten innen informasjonssikkerhet

1.3 Avgrensning av oppgaven

Denne oppgaven har fokuset på informasjonssikkerhet i kraftbransjen. Har denne bransjen de risikostyringsverktøyene som trengs for å kunne ha en helhetlig risikostyring. Det er benyttet et utvalg av teorier for å belyse problemstillingen. Det betyr også at det er tatt en del bevisste valg om å utelate en del teori.

Da bestemmelsen var tatt for å se på kraftbransjen falt valget på å intervjue personer med HMS (helse, miljø og sikkerhet) med vekt på sikkerhet ansvar i nettselskapene. Det er nettselskaper som er ansvarlige for strømnettet og at strømmen kommer ut til kunder. Jeg oppdaget fort at det var vanskelig å finne informanter til oppgaven. Kontaktet over 10 selskaper der jeg ønsket 6 store selskaper og 4 små. Av de 10 selskapene som ble kontaktet fikk jeg intervjue to. Så på et tidspunkt måte jeg gjøre om på problemstillingen. Fokuset var fortsatt informasjonssikkerhet og kraftbransjen, men at jeg ville prøve å finne svarene hos Norsk vassdrags og energidirektoratet (fra nå kalt NVE), Nasjonalt sikkerhetsmyndighet (fra nå kalt NSM) og Direktoratet for forvaltning og IKT (fra nå Difi). NVE har tilsynsmyndighet opp mot nettselskapene og kraftbransjen. NSM har ansvaret for sikring på nasjonalt plan, og Difi har et ansvar opp mot informasjonssikkerhet i den offentlige sektor. NVE har god kunnskap om kraftbransjen, og på den måten kunne gi meg noen gode svar. Ønsket var at NVE NSM og Difi kunne belyse dette med risikostyring, risikoanalyser og perspektiver, i tillegg til å svare på hvordan en antar at kjennskapen til sikring/security siden i bransjen er. NSM og Difi har ingen direkte tilknytting til kraftbransjen men valgte disse ut fra at de har mye kunnskaper om emnet som jeg berører i denne oppgaven forholdsvis opp mot sikring/security og informasjonssikkerhet. I Empirien har det blitt brukt både intervju, veiledere og rapporter fra forholdsvis NVE, NSM og Difi.

1.4 Begrepsavklaringer

Risiko: Handler om hendelser som kan oppstå i fremtiden, og konsekvensene av disse. Siden vi ikke kan se inn i en krystallkule vet vi ikke om disse vil inntreffe og heller ikke hva som blir konsekvensene. Vi snakker om usikkerhet knyttet til hendelsene og konsekvensene. Dette kan uttrykkes ved hjelp av sannsynlighet (Aven, at.al 2008).

Risiko vurdering: Består av risikoanalyse og risikoevaluering (Aven, at.al, 2008)

Risiko og sårbarhetsanalyse kalt ROS analyse: Dette er en metode som kan benyttes både til å kartlegge og vurdere generelle tema. I ROS-analyser blir sårbarhet vektlagt fordi sårbarhet er et aspekt av risiko (Furevik, 2012).

Risikostyring: Forstås med alle tiltak og aktiviteter som gjøres for å styre risiko (Aven, s,13. 2007)

Sårbarhet: Sårbarhetsutvalget (NOU 2000) definerer sårbarhet som et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet.

Sikkerhet/Safety: Viser til risikoen og usikkerheten til hendelser som ikke er planlagte. Hendelser som industriulykker, trafikkuhell, naturkatastrofer.

Sikring/Security: Viser til risiko og usikkerheten knyttet til uønskede handlinger som kriminalitet, sabotasje og terror. Utfordringene er at personer som ønsker å begå disse handlingene vurderer både konsekvenser og muligheter for å oppnå ønsket effekt.

Ondsinnede handlinger: planlagte handlinger for bevisst å skade eller drepe mennesker (Engen at.al, 2016:28).

Tilsiktet uønskede handling: uønsket hendelse som forårsakes av en aktør som handler med hensikt (Terrorsikring 2015).

Uønskede hendelser: en hendelse som har forårsaket eller kunne forårsaket ulike typer skade på sentrale verdier som mennesker, materiell, miljø og omdømme (Engen, at.al, 2016:261).

Informasjonssikkerhet: Handler om å sikre konfidensialitet, integritet og tilgjengelighet på informasjon (sivilbeskyttelsesloven)

Konfidensialitet: Innebærer å hindre uautorisert innsyn i informasjon som ikke kan være åpent tilgjengelig for alle (sivilbeskyttelsesloven).

Integritet: Innebærer å hindre uautorisert endring av informasjon (sivilbeskyttelsesloven).

Tilgjengelighet: Innebærer å sikre tilgang til informasjon ved behov for tilgang (sivilbeskyttelsesloven).

KraftCERT (Computer Emergency respons team): jobber for å bedre sikring i prosesskontroll – systemer ved å bistå kraftbransjen slik at den kan være oppdaterte om relevante sårbarheter og trusler, og kan være i stand til å detektere og motvirke digitale angrep. KraftCERT ble stiftet av Statnett, Statkraft og Hafslund etter initiativ fra NorCERT og NVE for å sikre en støtte for hele bransjen (https://www.kraftcert.no/om.html).

Kritisk infrastruktur: forstås systemer som når de ikke fungerer vil ha en sterk negativ effekt på samfunnet. kritisk infrastruktur inkluderer blant annet informasjons og elektrisk kraft, gass og olje, bank og finans, transport og vannforsyning (NOU 2000:24)

1.5 Presentasjon av Kraftforsyningsbransjen- nettselskap

Strømmarkedet er strengt regulert i Norge. Kraftnettet skal transportere strømmen fra produsent til forbruker. Det er en forutsetning for sikker strømforsyning at en har et velfungerende nett.

Forskjellen på kraftleverandør og nettselskap:

Kraftleverandør er det selskapet som en kjøper strøm fra, det er flere kraftleverandører og som kraftleverandør trenger en ikke ha strømnett for dette kan leies. I denne oppgaven er det nettselskapene som har fokuset for det er disse selskapene som har ansvaret for at strømmen kommer ut til forbruker, og det er de som har ansvaret for selve strømnettet i sin region.

Nettselskap er det lokale nettselskapet som eier og drifter strømnettet i regionen en bor i. Det er deres ansvar at strømmen blir transportert til kundene. Nettselskapene er monopolstyrt det vil si at en kan ikke bytte nettselskap men kraftleverandør kan byttes. Dette for å unngå at en bygger opp hvert sitt parallelle strømnett. Strømnettet er bygd opp på en slik måte at det skal ha nok kapasitet til å dekke behovet til samfunnet. Transmisjonsnettet tidligere kalt sentralnettet, er hovedveien i kraftsystemet og forbinder produsenter og forbruker i ulike deler av landet sammen. Transmisjonsnettet sørger også for overføringsledninger til utlandet. Distribusjonsnettet tidligere regionalnett og distribusjonsnett. Omfatter strøm ut til husholdninger, tjenesteyting og industri.

Kraftbransjen er under lagt sikkerhetsloven i form av beredskapsforskriften. Formålet med forskriften er: § 1-1. *Formål*

- Innenfor formålene i energiloven § 1-2, skal forskriften sikre at energiforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene.

1.6 Myndighetenes rolle opp mot informasjonssikkerhet

Norges vassdrags- og energidirektorat (NVE) har ansvar for å forvalte de innenlandske energi ressursene og er nasjonal reguleringsmyndighet for elektrisitetssektoren. NVE har videre ansvar for å forvalte Norges vannressurser og har ansvar for forsyningssikkerheten i kraftsystemet. Forsyningssikkerhet er definert som energi, effektivitet og driftssikkerhet.

NVE har ansvaret for å samordne beredskaps- planleggingen og skal lede landets kraftforsyning under beredskap og i krig. For dette formål er det etablert en landsomfattende organisasjon – Kraftforsyningens beredskapsorganisasjon (KBO) – bestående av NVE og de virksomheter som står for kraftforsyningen. Dette omfatter alle enheter som eier eller driver kraftproduksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft og fjernvarme. Alle enheter i KBO har en selvstendig plikt til å sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, begrense og håndtere virkningene av ekstraordinære situasjoner.

Evne til å opprettholde konfidensialitet, integritet og tilgjengelighet for informasjon i

energiforsyningen er grunnleggende viktig for sikkerheten. For de viktigste anleggene i energiforsyningen stilles det krav om redundante sambandsveier for elektronisk kommunikasjon i driftskontrollsystemet.

Tilsynene til NVE går på etterleving av regelverket og reaksjoner ved avvik fra regelverket. Tilsynet blir i all hovedsak utført som revisjon eller inspeksjon. Samarbeidspartnere ved tilsyn er Direktoratet for samfunnssikkerhet og beredskap og Økokrim, Riksadvokaten.

Nasjonal sikkerhetsmyndighet er Norges ekspertorgan for informasjons og objektsikkerhet og de har det nasjonale fagmiljøet for IKT sikkerhet. Direktoratet har et nasjonalt varsling- og koordineringstans for alvorlige data angrep og IKT sikkerhetshendelser. Det kan trekkes en linje helt tilbake til da regjeringen satt i London og organiserte Forsvarets etterretnings og sikkerhetskapasiteter i 1943. I 2003 ble det etablert som direktorat underlagt forsvarsdepartementet og justis og beredskapsdepartementet. NSM har tilsynsmyndighet etter sikkerhetsloven, et nasjonalt ansvar for kryptosikkerhetstjenesten og sentral i forvaltningen av kryptomateriell. NSM har noen nasjonale funksjoner som de ivaretar:

- Funksjon som nasjonal sikkerhetsmyndighet.
- Funksjonene som nasjonalt CERT (Computer emergency team).
- Funksjonene som NDA (National Distribution Authority Norway).
- Funksjonene som NSA (National Security Agency).
- Funksjonen som SERTIT.
- Funksjonene som nasjonal fagmyndighet for krypto
- Funksjonene som nasjonal fagmyndighet for fysisks sikring.
- Funksjonene som nasjonal fagmyndighet for personellsikkerhetstjenesten.
- Klareringsmyndighet for COSMIC TOP SECRET (CTS).

Direktoratet for forvaltning og IKT (**Difi)** er underlagt kommunal og moderniseringsdepartementet (KSM). Fagstyringsansvaret for offentlige anskaffelser ligger hos Nærings og fiskeridepartementet (NFD). Direktoratet ble opprettet 1 januar i 2008. Målgruppene til Difi er statlig og kommunal sektor men jobber også mot næringsliv, frivillige organisasjoner og innbyggere. Fagområdene til Difi:

- Forvaltning, organisering, ledelse, innovasjon og kompetanseutvikling.
- Digitalisering av offentlige tjenester og arbeidsprosesser
- Utvikling og forvaltning av fellesløsninger
- Forebygge IKT sikkerhet i statsforvaltningen
- Universell utforming av IKT løsninger
- Difi har følgende hovedmål der Difi skal:
- Bidra til økt samordning i offentlig sektor
- Bygge opp og dokumentere kunnskap
- Bidra til kompetansebygging i offentlig sektor
- Utvikle og forvalte fellesløsninger for forvaltningen
- Føre tilsyn med virksomheter i privat og offentlig sektor etter forskrift om universell utforming av IKT.

1.7 Oppgavens disposisjon

Introduksjon	**Kapittel 1: Innledning**
Teori og Metode	Kapittel 2: Teori Kapittel 3: Metode
Empiri og Drøfting	Kapittel 4: Presentasjon av intervju Kapittel 5: Drøfting Kapittel 6: Konklusjon
Appendiks	Forespørsel om intervju Intervju guider Samtykkeerklæring

2. Teori

For å komme fram til noen svar på problemstillingen og forskningsspørsmålene mine er oppgaven oppbygd med seks hovedtema. Temaene er delt inn i følgende:

- Perspektiver på risiko
- Risiko
- Risikoanalyser
- Sårbarhet
- Sikkerhet
- Risikostyring

Det første delkapittelet i teorien vil jeg presentere et utvalg av teorier hovedsakelig bygger dette på teorier fra Aven og fra boka Perspektiver på samfunnssikkerhet (Engen, at.al 2016). Tenker at det er viktig å være bevist på dette med perspektiver opp mot risiko for det legger føringer opp mot hvordan en ser på risiko og hvordan en vil gå fram for å håndtere risikoen.

Delkapittel to: Vil i all hovedsak omhandle et utvalg av teorier rundt begrepet risiko fra Aven og Renn. Ønsker å få fram hva som menes med risiko og at en kan få begrepsavklaringer rundt dette.

Delkapittelet tre: Handler om risikoanalyser. Tar for seg en generell risikoanalyse hvordan en bør planlegge, gjennomføre og evaluere. I all hovedsak vil det være teorier rundt Aven og Renn i dette kapittelet. Ønsker med dette å vise til hvordan en går fram for å finne den analysen som egner seg best, i forhold til hva en ønsker å analysere. Denne oppgaven har fokus på informasjonssikkerhet. I tillegg til hvordan en presenterer risikobilde. Det å presentere et godt risikobilde er viktig når det kommer til informasjonssikkerhet.

Delkapittelet fire: Omhandler sårbarhet. Det er ett lite kapittel som har blitt stående litt for seg selv, dette fordi jeg ønsker å fremheve sårbarheten som ligge i informasjonssikkerhet.

Delkapittelet fem: Omhandler sikkerhet, vil inneholde generelt om sikkerhet som en finner i Reason og Turner, men vil også trekke inn dimensjonene med det som går på

sikring/security og i den forbindelse har jeg lagt vekt på Schiefloe som har utarbeidet en modell for samfunnssikkerhet som en kan overføre til organisasjonsnivå.

Delkapittelet seks: Omhandler risikostyring. Grunnen til at jeg har valgt å legge risikostyring til slutt er fordi: For å ha en god risikostyring i organisasjonen, må en ha en forståelse om sitt eget perspektiv på risiko. Dette for å kunne se og finne risikoen som virksomheten kan eller blir utsatt for. En må være bevisst over sine sårbarheter, og en må ha sikkerhetsforståelse/sikkerhetsstyring for virksomheten. En vil da kunne snakke om risikostyring. I følge Aven så er alle tiltak og aktiviteter som gjøres for å styre risiko, risikostyring (2009).

2.1 Perspektiver på samfunnssikkerhet

I boka samfunnsperspektiv som ble gitt ut 2016 (Engen, at.al 2016), starter de med å redegjøre for samfunnssikkerhet. En kan lese at det perspektivet man har på samfunnssikkerhet er avgjørende av det ståstedet, posisjonen eller faglige bakgrunn en har (Engen, at.al. 2016). Dette gjør det krevende å jobbe med samfunnssikkerhet og det er nødvendig med tverrfaglig samarbeid og evne til perspektivforskyvninger i arbeidet med risiko- og sikkerhetsspørsmål (Engen, at.al. 2016). *Det er en dårlig ide å arbeide med samfunnssikkerhet fra et snevert og rigid ståsted ettersom et perspektiv sjelden gir hele svaret på det aktuelle spørsmålet* (Engen, at.al. s, 25. 2016). I Norge er samfunnssikkerhet et sentralt begrep, samfunnssikkerhet styrer viktige prioriteringer i politikken og i utformingen av institusjoner i samfunnet (Engen, at.al, s. 25. 2016).

I teorien finner vi flere perspektiver på risiko i boka til Engen, at. al (2016) perspektiver på samfunnssikkerhet finer vi en god oversikt over perspektivene.

Ontologi	**Epistemologi**	**Tilhørende teorier/perspektiver**	**Problemstillinger**
Realistisk: Verden eksisterer uavhengig av menneskenes bevissthet.	Realistisk: Risiko er en objektiv trussel eller fare som eksisterer, og som kan måles uavhengig av sosiale og kulturelle prosesser,	Tekno-økonomiske teorier Psykologiske teorier Kognitive heuristikker Psykrometriske faktorer Semantiske	Hvilke risikoer eksisterer? Hvordan beregne dem? Hvordan responderer folk på risikoer? Hvordan håndterer vi dem?

	men beregningene kan påvirkes gjennom kognitive filtre og sosiale og kulturelle fortolkningsrammer	bilder Risikokompensasjon	
Svak konstruktivisme Verden eksisterer uavhengig av menneskenes bevissthet og fortolkes gjennom kognitive kategorier.	Svak konstruktivisme Risiko er en objektiv fare som blir mediert gjennom sosiale og kulturelle prosesser, og kan ikke forstås isolert fra disse prosessene. Den kan måles og vurderes, men metodene må ta hensyn til de kognitive og sosiale mekanismene.	Risiko sett ut fra Aven og Renns definisjon Risk governance. Risiko må vurderes med hensyn til om den er lineær, kompleks, usikker og tvetydig. Ekspertkunnskapen er adekvat for risikobeslutninger, men må settes i sammenheng med sosiale og politisk kontekst.	Hvordan er risiko forstått i ulike sosiokulturelle kontekster? Hvorfor er noen farer utvalgt som risiko og andre ikke? Hvordan påvirker konteksten våre oppfatninger av risiko? Hvordan blir risiko og risikoatferd internalisert i sosiale systemer? Hvordan styre risiko og legge grunnlaget for en risikopolitikk?
Sterk konstruktivisme: Verden kan ikke forstås utover kognitive, sosiale og kulturelle sammenhenger.	Sterk konstruktivisme: Ingenting er risiko i seg selv	Kulturelle utrykk /Douglas og Wildavsky Poststrukturalisme/ Niklas Luhmann Governmentality/ Michel Foucault	Hvordan operer diskurser og praksiser rundt risiko i konstruksjonen av individet og det sosiale? Hvordan påvirker makt og hegemoni denne diskursen?

Tabell 1. hentet fra perspektiver på samfunnssikkerhet (Engen at.al 2016 s. 92) som viser en oversikt over ontologi og epistemologi.

I tabellen kommer de forskjellige perspektivene frem og viser at risiko er et begrep det er stor uenighet om og siden det er stor uenighet om hva risiko er så vil det tilsvarende være stor uenighet om hvordan en bruker risikoanalyser. Om en går inn og ser på svak konstruktivisme så er det enn retninger som prøver å rette opp i de konfliktene som foreligger i de forskjellige perspektivene. Engen at.al (2016) viser til at dette har sammenheng med at risikoutfordringene i dag oppfattes mer komplekse, faretruende, grenseoverskridende og globale. Dette har ført til at en søker å bygge en bor mellom perspektiver som realismen og konstruktivismen for å ta de beste fra perspektiv (Engen, at.al 2016).

2.2 Risiko

Risiko handler om hendelser som kan oppstå i fremtiden, og konsekvensene av disse. Siden vi ikke kan se inn i en krystallkule vet vi ikke om disse vil inntreffe, og heller ikke hva som blir konsekvensene. Vi snakker om usikkerhet knyttet til hendelsene og konsekvensene. Dette kan uttrykkes ved hjelp av sannsynlighet (Aven, at.al 2008).

I boka til Aven fra 2007 risikostyring så defineres risiko som: Risiko er en kombinasjon av mulige konsekvenser (utfall) og tilhørende usikkerhet (Aven, 2007, s. 41). En annen definisjon som jeg ønsker å trekke frem i denne oppgaven i forhold til Risiko er definisjonen til Aven og Renn (2010), der de definerer risiko til

- usikkerheten om og alvorligheten av hendelsen og konsekvenser av en aktivitet med hensyn til det menneske verdsetter.

Aven og Renn viser til at risiko definisjoner kan kategoriseres på to måter.

1. Risiko uttrykkes ved hjelp av sannsynligheter og forventede verdier

2. Risiko uttrykkes gjennom hendelser / konsekvenser og usikkerheter
(Aven og Renn, 2010, s. 3)

Renn (2008) viser til ulike former for risiko og viser til en klassifiserings liste der en knytter sammen skadepotensial og sannsynligheter for at hendelsen skal inntreffe, med tilhørende risikobeskrivelser.

Vurderingskriterier	Risikobeskrivelser
Skadeomfang	Hva er tilhørende effekter, fysisk skade, sårende, produksjonstap
Sannsynlighet for hendelsen	Hva er sannsynlighetsfordelingen, frekvensfordelingen
Usikkerhet	Hva er den konstruerte og overordnede og generelle indikatoren for usikkerhet?
Utstrekning	Hva er geografisk utstrekning av mulig skade, også på tvers av nasjoner?
Utholdenhet varighet	Hva er varighet i tid av skadeomfang, også på tvers av generasjoner?
Reversibilitet	Er det mulighet til å reversere, det vil si bringe tilbake tilstanden før hendelsen?
Forsinket effekt	Hva er avstanden i tid mellom hendelsen og sannsynlige effekter?
Ødeleggelse av egenkapital	Er det uoverensstemmelse mellom dem som har nytte av risikoene og dem som bører omkostningene?
Mobiliseringspotensialet	Vil hendelsen generere sosiale konflikter og/eller psykologiske reaksjoner?

Tabell 2. Klassifisering av risiko etter vurderingskriterier og riskobeskrivelse klassifiseringen viser til forholdet mellom risiko og risikobeskrivelse og hensikten er å komme frem til metoder som bør benyttes i risikoanalysen. (Engen at.al 2016).

For å få en god prosess i å finne en god risikoanalyse viser Renn til lineære, komplekse, usikre og tvetydige risikoer.

Lineære: Risikoer som viser til hendelser og situasjoner som er kjente og det eksisterer mye data om. Eks. er effekter av røyking, trafikkatferd innen disse risikoene finner vi mye data som kan analyseres ved hjelp av metoder innen risikoanalyser.

Komplekse: Dette er risikoer som viser vanskeligheten med å avgjøre sammenhengen mellom de ulike årsakene og observerte effekter. I disse komplekse risikoene er det vanskelig å finne årsak virkningssammenhengene. Det kan være flere faktorer som virker inn på samme tid. Dette gjør at skadeomfang, sannsynligheter knyttet til

hendelser og konsekvenser, utstrekning og utholdenhet vil være vanskelig å forutse (Engen, 2016).

Usikre og tvetydige: Dette er risiko knyttet til problemet med å forutse en hendelse og konsekvensene av denne. Det kan være manglende kunnskap som går over til uvitenhet. Eksempler på dette kan være store naturkatastrofer, som tsunamien i 2004 og de store konsekvensene dette fikk for mange land. Graden av usikkerhet kan også variere. Det er noen risikofenomener vi vet at vi ikke vet noe om. Det er noen risikoer vi faktisk ikke vet at vi ikke vet noe om (Engen, at.al, 2016, s 84). Den siste setningen er gjerne det vi kaller for svarte svaner. Terrorhandlinger eller andre typer ondsinnede handlinger som tar sikte på å skade samfunnet faller innenfor disse to siste risikokategoriene. Det er vanskelig å forutse og beregne terrorhandlinger. Dette fordi terroristen vil omgjøre sine mål om det blir vanskelig å utføre terroren, en flytter bare målet. Det er knyttet stor usikkerhet om en gitt hendelse vil inntreffe, og hva konsekvenser vil dette gi. Vanskelig å tallfeste denne type risiko. Tvetydige risikoer viser til hvordan vi tenker, mener og vurderer de risikoene vi står ovenfor. For å håndtere vanskelige risikoutfordringer er det viktig å være enig om hvordan skal vi definere risiko, hvilke metoder skal man anvende og det er viktig med en kritisk til utvikling og anvendelse av metoder. Risikoanalyser skal gi beslutningsgrunnlag til politikere og myndigheter. Feilaktige risikoanalyser kan gi fatale konsekvenser. Det må være en enighet om hvordan en definerer risikoen og hva kriterier som ligger til grunn for å vurdere kvaliteten på metodene (Engen, at.al 2016).

2.2.1 Risiko for ondsinnede og ikke planlagte handlinger

Det skilles i Norge mellom sikkerhet og sikring. På engelsk er dette litt mer forståelig for der gir ordene Security og safety mer mening for oss nordmenn. Men også her er det forskjellig bruk av ordet. Safety/sikkerhet viser til risikoen og usikkerheten til hendelser som ikke er planlagte. Hendelser som industriulykker, trafikkuhell, naturkatastrofer. Sikring/Security viser til risiko og usikkerheten knyttet til uønskede handlinger som kriminalitet, sabotasje og terror. Utfordringene er at personer som ønsker å begå disse handlingene vurderer både konsekvenser og muligheter for å oppnå ønsket effekt. Risikoen kan uttrykkes som forholdet mellom trusselen mot en verdi og verdiens sårbarhet mot denne trusselen. Sårbarheten må også sees i sammenheng med evnene til å motstå og forsvare seg mot trusler (Engen, al.al 2016, Veileder NSM 2016).

I boken perspektiver til samfunnssikkerhet (2016) til Engen, at.al skriver de om at det kan virke som det er en motsetning mellom hvordan man bør vurdere risikoen for ondsinnede handlinger og risikoen for ikke planlagte handlinger. Argumentet går på sannsynlighet, enkelte ønsker å forlate sannsynlighetsbegrepet som er basert på frekvenssanssynlighet. Men sannsynlighet er ikke bare en frekvensvurdering av om en gitt hendelse skal skje. Sannsynlighetsvurderingen kan være basert på kunnskap om sannsynlighet, vurderingene til den som utfører analysen, og frekvenssannsynligheter. En må prøve å skille mellom styrker og svakheter ved analysemetodene og få til en felles plattform for analyse innenfor både sikring/security og sikkerhet/safety området. Dette finner en også igjen hos Jore og Egeli (2015) de hevder at metologien ikke er så forskjellig og det viktigste er å ha sikkerheten på dagsorden for å forbedre metoden. En må ha en felles forståelse av begreper for å unngå misforståelser (Jore og Egeli 2015). I konklusjonene til FFI (2015) kommer det fram at det er ingen internasjonale, eller nasjonale beste framgangsmåte for risikovurderinger for tilsiktede hendelser. Selv om det ikke eksisterer en beste framgangsmåte så kan en se følgende kjennetegn for en god tilnærming som vil inneholde en god struktur, det er en arbeidsgruppe med bred kompetanse. En må kartlegge kunnskapsstyrken og en må strebe etter å ha et helhetlig perspektiv på risikoen i virksomheten. En må være i stand til å kommunisere risiko og usikkerhet samt være gjennomsiktig, sporbar og etterprøvbar.

2.4 risikoanalyser

Målet med en risikoanalyse er å kartlegge og beskrive risiko. Risikoanalysen skal kunne presentere et risikobilde. Når det kommer til hvordan en gjør en risikoanalyse så viser Aven, at.al (2008) at en skiller mellom tre hovedkategorier av risikoanalyse metoder viser i tabell hovedkategori, framgangsmåte og beskrivelse.

Hovedkategori	Fremgangsmåte	beskrivelse
Forenklet risikoanalyse	Kvalitativ	Forenklet risikoanalyse som på en uformell måte kartlegger risikobilde ved hjelp av idedugnad og presenteres på en grov skala som liten, moderat og høy. Her brukes det ikke formaliserte risikoanalyse metoder
Standard risikoanalyse	Kvalitativ og kvantitativ	Standard risikoanalyse er en mer

		formalisert fremgangsmåte. Eks: HAZOP og grovanalyse. Presenteres gjerne ved hjelp av risikomatriser.
Modellbasert risikoanalyse	Kvantitativt	Modellbasert risikoanalyse tar i bruk teknikker som hendelsestreanalyse og feiltreanalyse for å beregne risiko

Tabell 3. hentet fra risikoanalyse av Aven at.al (2008, s.). Viser de ulike metodene innen for kategoriene av risikoanalyse.

Risikoanalysen brukes til å etablere ett risiko bilde og en kan sammenligne de ulike alternativene og løsningene med hensyn til risiko. Risikoanalysen hjelper oss med å identifisere forhold som kan ha stor betydning til risiko. Analysen får frem hvilke effekter ulike tiltak vil ha på risikoen. Dette gir grunnlag for at en kan velge mellom ulike løsninger og tiltak i planleggingsfasen av for eksempel av et IKT system, hva tilpasninger kan gjøres for at IKT systemet blir mindre sårbart hvordan kan en få systemet til å tåle påkjenninger. En kan måle om en tilfredsstiller de krav som er satt til systemet. En får dokumentert forsvarlig drift (Aven 2009). Nå er det slik at mange gjennomfører risikoanalyser for å tilfredsstille myndighetskrav og regelverk. Det er viktig, men hoved motivasjonen til å gjennomføre en risikoanalyse bør ligge i at en ønsker å få et godt beslutningsgrunnlag. Det å finne den rette balansen mellom ulike hensyn som sikkerhet og økonomi.

Figur 1. viser risikoanalyse prosessen og de ulike trinnene.

Problemdefinisjon, informasjonsinnhenting og organisering: en må tenke i gjennom hvorfor en skal gjennomføre en risikoanalyse. Det er vanskelig uten et klart formulert mål og problemstilling å finne de svarene som en trenger for å fatte en god beslutning. Det er en forutsetning for en god risikoanalyse at det er klare målforutsettinger

(Avenat.al, 2008). Aven at.al (2008) viser til at av erfaring legges det ofte stor vekt på risikovurderingen og mindre vekt på den innledende fasen og på den avsluttende fasen av prosessen.

Valg av analysemetoder: hva ønsker/trenger vi av metode forenklet, standard eller modellbasert. Finnes det bransjespesifikke analyseverktøy? Hva er naturlig å bruke (Aven at.al 2008). Metoder som vil være aktuelle opp mot risikoer opp mot informasjonssikkerhet vil en gjerne hele mot standard metoder og gjerne la de være kvalitative om det finnes lite kunnskap og statistikk. En kan i noen tilfeller når det gjelder risiko for informasjonssikkerhet også bruke feiltre og hendelsetre analyser som ligger under modellbaserte analyser (Hikstad, at.al 2012).

Identifikasjon av initierende hendelser: denne delen av prosessen er svært viktig, det er her vi skal identifisere farer/ trusler. Det du ikke har identifisert kan du ikke håndtere (Aven at.al, 2008). En skal være oppmerksom på at dette er en fase som kan bli rutinepreget. Når en har gjennomført analyser tidligere er det vanlig å kopiere listen over farer og trusler fra forrige analyse, i dette ligger faren i å ikke identifisere ny farer og trusler. Aven at.al (2008) viser til viktigheten av at denne jobben gjøres strukturert og systematisk, i tillegg at en involverer personer med den nødvendige kompetansen.

Årsaksanalyse: i denne analysen ser en på hva som må til for at de initierende hendelsene skal inntreffe. For å komme frem til disse årsakene finnes det flere teknikker. En kan bruke idedugnad eller en kan bruke feiltreanalyse for å kartlegge årsakene (Aven at.al, 2008).

Konsekvensanalyse: vi befinner oss nå på høyresiden av bow tien og på samme måte som ved årsaksanalysen så vil en nå vurdere mulige konsekvenser av hendelsen. Her kan det være snakk om økonomiske tap, sikkerhet for personell og miljø (Aven at.al, 2008).

Risikobilde: med utgangspunkt i årsaksanalysen og konsekvensanalysen etableres det et risikobilde. Dette risikobilde skal dekke prediksjoner, sannsynlighetsfordelinger, usikkerhetsfaktorer og styrbarhet (Aven at.al 2008).

Sammenligning av alternativer, identifisering og vurdering av tiltak: risikohåndteringen er prosessen og implementeringen av virkemidler for modifisering

som virkemidler for å unngå, redusere å optimalisere og overføre risiko. Vi snakker nå om å se på endring i risiko, kostnadseffektivitet, kost-nytteanalyser, risikoakseptkriterier og ALARP (As low as reasonably practicable)-vurderinger. Med andre ord når en sammenligner alternativene ved å se på risikobilde for du ulike alternativene og disse er omtrent like i forhold til eksempel økonomi så har vi en risikoanalyse som gir et godt underlag for et bestemt alternativ (Aven, et.al 2008). En skal være oppmerksom på at tiltak kan gi både positive og negative effekter. eksempler på dette gir Aven et.al (2008) som der en bruker kjemikalier som reduserer personellrisikoen, men som medfører økt risiko for skader på det ytre miljøet. Aven et.al (2008) kommer med et forslag til metode for å vurdere når et tiltak skal implementeres. Tiltak bør implementeres om en svarer ja på følgende spørsmål:

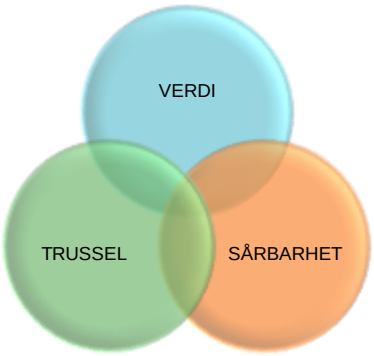
- Relativt høy personellrisiko/miljørisiko?
- Store usikkerheter (knyttet til fenomener, konsekvenser) og tiltaket vil redusere usikkerheten?
- Tiltaket øker styrbarheten i stor grad?
- Løsningen er robust sikkerhetsmessig?
- Benyttes best tilgjengelig teknologi?
- Er det uløste problemområder personsikkerhetsmessige eller arbeidsmiljømessig, er det konflikter mellom disse to aspektene?
- Strategiske hensyn?

Ledelsens vurdering og beslutning: Aven at.al (2008) viser til noen gode ledelses og styringsprinsipper. Beslutningene må være forankret i ledelsen og må bli sett som viktige for å nå målene til virksomheten. Det må komme klart frem hvem som har ansvaret for at beslutningen implementeres. Det må også utarbeides en plan for gjennomføring. Denne bør omfatte tidspunkter og frister for når beslutningen skal være iverksatt. Til slutt viser Aven et.al (2008) til at dersom beslutningen ikke blir fulgt opp bør det være systemer, som fanger dette opp.

I risikoanalyse boken til Aven et.al (2008) vises det til 4 suksessfaktorer for en god risikoanalyse. 1. Viktig å huske at risikoanalysen gir ikke beslutningen men beslutningsstøtte. Metodene som skal brukes må være tilpasset formålet med analysen, hva ønsker en beslutningsstøtte til hva skal analyseres? Aven at.al (2008) viser til at om det ikke foreligger en klar beslutningssituasjon trenger en ikke en analyse. I tillegg

presiseres det i boken som er viktig i denne oppgaven at om det er stor usikkerhet forbundet med det en ønsker å analysere som foreksempel hendelser opp mot informasjonssikkerhet. En må huske at en risikoanalyse er å systematisere og beskrive den kunnskap og manglede kunnskap en har om fenomenene og prosessene. Målet med analysen er å få beslutningsstøtte. 2. Risiko er mer enn å beregne sannsynligheter og forventningsverdier, Aven at.al (2008) etterlyser refleksjoner knyttet til usikkerhetsdimensjonene og styrbarheten. Det er for lite fokus på hva som styrer utfallet, men stort fokus på sannsynlighetstallene. 3. Risikoanalysen har både styrker og svakheter. Styrken er at analysen systematiserer tilgjengelig kunnskap og de usikkerhetene en har i forhold til fenomenene, systemene og aktivitetene vi studerer. Svakhetene eller begrensningene er risikoanalysens presisjon, det kan være vanskelig å gi de nøyaktige prediksjoner en trenger. Til det kreves det stor data mengde. Analysen kan være av dårlig kvalitet, det kan være upresise og uklare begrepsdefinisjoner. Det vises også til svakheter i forhold til risikomatriser, en bør være forsiktig med å innføre størrelser som er vanskelige å forklare (en kan ikke bruke matrisen for å vurdere nytten av tiltak) 4. Aven at.al (2008) etterlyser refleksjoner over tilnærmingen og metodene som er brukt. Det ender fort med at analytikere bruker de metodene og modellene som selskapet eller virksomheten har tilgjengelig. Dette må oppdragsgiveren være bevisst på.

NSM har utarbeidet en veiledning for risikobasert sikkerhetsstyring der fokuset er på uønskede handlinger gjerne kjent som tre faktor modellen se figur 3.nedenfor.



Figur 2. Viser modellen trefaktormodellen, og risikoen vil ligge i skjæringspunktet mellom disse tre faktorene.

NSMs veileder for NS 5832 tar utgangspunkt i verdi. Sikkerhet bygger på noe en har av verdi som en ønsker å beskytte. Der er ikke mulig å beskytte alt like godt, så en må prioritere det som er nødvendig. Det er heller ikke alle hendelser eller trusler som er like aktuelle og relevante. Dette gjør at denne veilederen tar utgangspunkt i verdien for risikovurderingen. Modellen består av følgende stadier:

Figur 3. Viser stadiene i modellen i Risikovurdering for sikring 2016.

Verdivurderingen er en kartlegging av virksomhetens verdier. Denne verdivurderingen må utføres på en systematisk måte med å vurdere hvilke konsekvenser det kan få dersom verdiene skulle rammes. Om risikovurderingen omfatter hele virksomheten vil det være hensiktsmessig å dele dette opp i avdelinger eller prosesser. Verdivurderingen er viktig i bevisstgjøringsprosessen om hvilke verdier virksomheten besitter som kan være et mål for en potensiell trussel aktør. Verdier kan være materielle og ikke-materielle (NSM, 2016)

Sikringsmål da skal virksomheten bestemme hva de aksepterer av skade og bortfall av kritiske verdier. Denne vurderingen gjøres på bakgrunn av klassifiseringen av konsekvensene, som er gjort tidligere. Disse vil ha betydning for hvor mye ressurser som må settes for å kunne beskytte virksomhetens kritiske verdier.

Trusselvurdering skal beskrive det gjeldende trusselbilde for det som en ønsker å beskytte. Denne vurderingen skal gi et bilde over hvordan kan trusselen utvikle seg. Fokuset må være på reelle og potensielle trussel aktørers intensjon om og kapasitet til å ramme virksomheten. NSM anbefaler å dele opp truslene i kategoriene spionasje, sabotasje, terrorhandlinger og annen alvorlig kriminalitet.

Scenario skal brukes for å få frem sårbarhetene, som er relevante for analysen. Det er verdivurderingene og trusselvurderingen, som er grunnlaget for utarbeiding av

scenarioer. Disse scenarioene bør beskrive hvordan trussel aktører kan gå fram for å skade verdiene, og forenkler sårbarhetsvurderingen og gjør det enklere for beslutningstaker å følge resonnementene.

Sårbarhetsvurdering skal vise om det er gap mellom innførte sikringstiltak og trussel aktørs intensjon og kapasitet

Risiko, i denne fasen sammenstiller en resultatene fra verdi, trussel og sårbarhetsvurderingen. Målet er å beskrive hver enkelt risiko som virksomheten er eksponert for og klassifisere disse. En må gjøre en bedømmelse av hva faktorer som er dimensjonerende for virksomheten og må tas hensyn til i bedømmelsen.

Avslutter dette kapittelet med at det er en stor utfordring med risikoanalysefaget. Det er noen risikofenomener som vi vet at vi ikke vet noe om. Det er noen risikoer vi faktisk ikke vet at vi vet noe om (Engen, at.al, s. 84). Den siste er gjerne det vi kaller for sorte svaner.

2.4 Sårbarhet i forhold til informasjonssikkerhet

Det er en del trender som kan påvirke sårbarhetsbilde for kraftbransjen blant annet digitalisering av samfunnet, skytjenester, automatisering av hverdagen og arbeidslivet. Lysne utvalgets (NOU 2015:13) er sårbarheten som samfunnet står ovenfor inndelt i to kategorier. Sårbarhet som er kjent og akseptert og sårbarheter som ikke blir gjenstand for tiltak fordi sårbarheten er ukjent, feilvurdert, en har ikke forstått og mangelfull kommunikasjon. Videre i Lysne utvalget (NOU 2015:13) viser de til at det er flere sårbare tjenester, som inngår i verdikjedene som spenner over flere sektorer, de er underlagt forskjellige lovverk og tilsynsregimer. Det er vanskelig for de som befinner seg på toppen av verdikjeden å ha oversikt over hvilke sårbarheter tjenesten er eksponert for lenger nede i verdikjeden.

Sårbarhetsutvalget (NOU 2000:24) definerer sårbarhet, som et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet. Sårbarhet er knyttet opp til mulig tap av verdi. System kan i denne sammenhengen for eksempel være en stat, den nasjonale kraftforsyningen. I stor grad er sårbarhet selvforskyldt. Det går an å påvirke sårbarhet, avgrense og redusere den (Aven, 2007).

Sårbarhet er ofte betraktet som det motsatte av robusthet. (Engen, at.al 2016). Risiko og sårbarhetsanalyser har en bred anvendelse som beslutningsstøtte i lokalforvaltningen og i private virksomheter. Det er mye lovverk som ROS analysen er forankret i blant annet Arbeidsmiljøloven §3-1, sivilbeskyttelsesloven §14, forskrift om kommunal beredskapsplikt §2 og plan- og bygningsloven § 3-1 (Engen, at.al 2016, s. 352) videre i boken til Engen at.al (2016) kan en lese at i tillegg til dette så har alle virksomheter både privat og offentlig sektor krav om å ha et system for internkontroll for helse, miljø og sikkerhet. I NOU samhandling for sikkerhet (2016:19) pekes det på at god sikkerhet i IKT systemer fordrer gode tekniske løsninger, så vel som god fysisk sikkerhet rundt infrastruktur og personellsikkerhet. Koblingene mellom informasjonssikkerhet og sikkerhet i IKT systemene er tette. IKT systemer i dag er bærere av de fleste funksjoner i samfunnet. Samfunnsfunksjoner er avhengig av sikkerheten i IKT systemene. Det vil si at sårbarheter i IKT systemene arves av samfunnsfunksjoner som disse understøtter (NOU 2016:19).

2.5 Sikkerhet

Det er mange definisjoner på sikkerhet, ønsker å trekke frem følgende definisjoner på sikkerhet. I dette delkapittelet vil jeg viser til både sikkerhet/safety og sikring/security.

Aven et.al (2004)

- *forebyggende tiltak der hensikten er å redusere sannsynligheten for at noe uønsket skal skje, eller redusere konsekvensene ved uønsket hendelser*.

Denne definisjonen kan relateres til det fysiske miljøet som teknologiske systemer, produkter og menneskelige og sosiale faktorer som struktur, politikk og beslutninger.

Reason (2008)

- *safety is a term defined more by its absence than its presence.*

Der han viser til de to sidene (Janus ansiktet) av sikkerhet. Det negative er utfallene som ulykker, skader, tap av eiendeler og miljøskader. Det positive der en forholder seg til systemets egen motstand mot operasjonelle farer reflekter en organisasjons helse både når det gjelder produktivitet og sikkerhet.

Balansen mellom produksjon og sikkerhet er viktig i den forstand at det er bare etter ulykker og alvorlige nesten – ulykker sikkerheter står fremst i bevisstheten blant leder i organisasjonene. De fleste som jobber i en organisasjon vil få mer opplæring rundt produksjon en sikkerhet, men produksjon bidrar med ressurser som gjør det mulig med sikkerhetsinnsats. Suksessfullt sikkerhetsarbeid vil vise seg som fravær av negative resultater. Det er lett å glemme ting som sjelden inntreffer og særlig når produksjonsøkning fører til vekst, profitt og økt markedsandel (Reason, 1997). Reason (1997) snakker om protection der målet er sikkerhet for mennesker og materiell og Defence er midlene for å nå målet. Reason (1997) snakker om forsvar der han deler dette inn i Hard Defences og Soft Defences. Hard defences er automatiserte sikkerhetsinnretninger, fysiske barrierer, alarmer og meddelelser, sperreanordninger og låser, personlig sikkerhetsutstyr. Sikringer. Mens soft defences er lovgivning, reguleringer og kontroller, regler og prosedyrer, trening og øvelser, brifing og administrativ kontroll sertifiseringer.

Forebygging og forsvar skal tjene ulike funksjoner og skape forsvar i dybden. Som etablering av forståelse og bevissthet om farer. Det å gi veiledning i sikker opptreden. Alarmere og varsle når farer er til stede. Gjenetablere sikkerhet når systemet kommer i unormal situasjon. Sette inn sikkerhetsbarrierer mellom farer og potensielle tap. Kunne eliminere farer dersom de skulle bryte gjennom barrierer.

Sikre rømning og redning dersom innrykking eliminasjon av hendelser mislykkes (Reason, 1997). Aktive feil og latente forhold. Aktive feil er den skarpe enden der vi finner de som begår aktive feil som piloten, operatøren eller vedlikeholds arbeider. Latente forhold organisasjonsulykker er ikke bare menneskelige feil eller prosedyre brudd, en må se på de bakenforliggende årsakene til at det gikk galt i den skarpe enden (Reason, 1997).

Mennesker produserer, opererer, vedlikeholder og drifter i komplekse systemer derfor er menneskers beslutninger og handlinger involvert i alle organisasjonsulykker (Reason, 1997).

2.5.1 En modell for samfunnssikkerhet Schiefloe (2012)

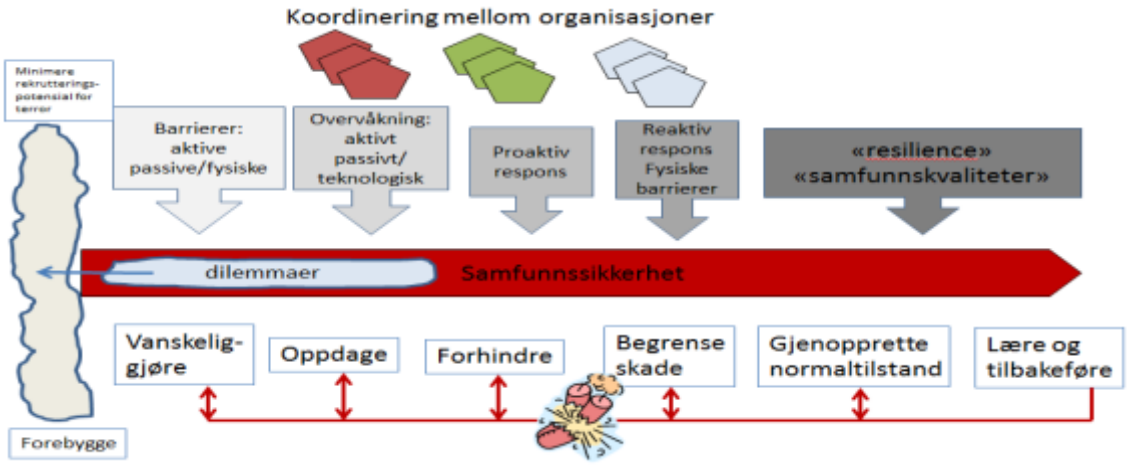
Schiefloe (2012) har tatt utgangspunkt i Reasons barrieremodell, Turners stadier modell og teorien om resilience.

Schiefloe (2012) modell for organisatorisk sikkerhet, viser til: organisasjoner som skal operere sikkert over tid, må utvikle fem ulike sett av organisatoriske egenskaper

1. Pålitelighet, virksomheten må være godt planlagt, med gode rutiner og tydelige ansvars og myndighetsforhold.
2. Sensitiv, virksomheten må ha prosedyrer, rutiner, praksis og kultur som oppdager forstår mulige faresignaler
3. Proaktiv handlingsdyktighet, kompetanse, rutiner og reaksjonsevne. Tilløp stoppes før de utvikles, evne til improvisasjon.
4. Reaktiv handlingsdyktighet, i stand til å håndtere hendelser og ulykker som måtte inntreffe.
5. Evne til læring, registrere og analysere ulykker og hendelser. Bruke dette som grunnlag for formell og uformell erfaringsoverføring og læring (Schiefloe, 2012).

Følgende elementer inngår i modellen til Schiefloe. Forebygge: en må fremme virkemidler som reduserer og eliminerer rekruteringspotensialet for terrorisme og høyreekstreme ungdomsmiljøer. Dette gjøres gjennom bedre integrering av minoriteter og fattighetsbekjempelse, utdanning og god tilgang til arbeidsmarkedet. Vanskeliggjøre: passive og fysiske barrierer mot terrorhandlinger. Disse barrierene kan være aktive eller passive som byråkratiske rutiner. Oppdage: Være i stand til å fange opp, kombinere og tolke informasjon eller signaler som kan indikere at noe er i utvikling. Dette kan en gjøre ved hjelp av overvåkning som kan foregå ved bruk av teknologi eller manuelt. Politiets sikkerhetstjeneste og militære etterretning har dette som primæroppgave. Forhindre: Innebærer at relevante aktører/myndigheter reagerer når noe oppdages (PST, politi). Eksempler er når terrorplaner avsløres og potensielle terrorister arresteres før planene settes ut i livet. Dette kan omtales som proaktiv respons. Begrense skade: Evne til å redusere virkningene av en hendelse som en ikke har lykkes i å forhindre. Dette kan skje ved etablering av fysiske barrierer. Gjenopprette normaltilstand: Etter at en hendelse har funnet sted, er det neste steg å gjenopprette normaltilstand. Dette omfatter fysiske, medisinske, sosiale og psykiske dimensjoner. På grunnlag av erfaringsinnhenting og analyser, kan en så lære av det som har skjedd og benytte kunnskapen på en slik måte at en er bedre i stand til å håndtere og eventuelt håndtere nye hendelser. I hendelser som omfatter større deler av et samfunn, kan vi

snakke om samfunnets iboende robusthet og kvaliteten. Resilience på samfunnsnivå.



Figur 4. Schiefloe (2012) sin modell for samfunnssikkerhet.

I følge Schiefloe (2012) vil sikker drift av en ulykkes utsatt organisasjon fordrer at ulike deler av organisasjonen kommuniserer, koordinerer ansvar og aktiviteter på en hensiktsmessig måte (Schiefloe, 2012). Denne koordinering forutsetter igjen sammenfall i mål- og middeloppfatning, kommunikasjon og samarbeid. I en kompleks organisasjon krever dette god koordinering. En må ha en kombinasjon av (1) sentral ledelse som setter retning og stiller krav og (2) lokal beslutningsmyndighet og ansvarliggjorte medarbeidere som har nødvendig frihet til å gjøre de tilpasningene som er nødvendige i forhold til ansvarsområde og arbeidssituasjon (Schiefloe 2012).

Det er et forhold som gjør at sikkerhetsmodellen på samfunnsnivå blir mer komplisert enn tilsvarende modell på organisasjonsnivå, og det er at de fleste elementene i modellen forutsetter koordinering mellom ulike offentlige etater og organisasjoner, dette er vanskelig å få til (Schiefloe, 2012).

De fleste industrielle organisasjoner som er ulykkes utsatte, har ledelse og ansatte sikkerhet og risikohåndtering kontinuerlig på agendaen. Det investeres i teknologiske løsninger som skal forhindre og begrense ulykker, og det gjennomføres jevnlige

beredskapsøvelser. I følge Schiefloe (2012) er drivkraft for aktivt sikkerhetsarbeid at de involverte i den skarpe enden selv kan bli ofre dersom ulykker inntreffer. For ledelsen og eiere er det også et potensiale i økonomiske konsekvenser en faktor som tas inn i vurderingene (Schiefloe, 2012). Schiefloe (2012) viser til ulykken på Deepwater Horizon som krevde 11 liv og var en økonomisk katastrofe for BP. Dette er erfaringer som gir gode argumenter for investeringer i økt sikkerhet (Schiefloe, 2012).

I følge Schiefloe (2012) er det vanskeligere å få gjennomslag for at investeringer i sikkerhet er nødvendige og «lønnsomme» på samfunnsnivå. Sikkerhet krever investeringer og driftsutgifter, dette er sikkerhetstiltak som ofte oppleves som plunder og heft i dagliglivet. Schiefloe viser til sikkerhetskontrollen på flyplassene (Schiefloe, 2012). Når politikeren skal ta avveininger mellom ulike interesser kan det være særlig vanskelig å prioritere formål som ikke vises. Schiefloe (2012) viser til 22 juli bombingen i regjeringskvartalet, hadde det vært fysiske barrierer til stede ville ikke hendelsen inntruffet og vi hadde hat en ikke hendelse som ingen hadde lagt merke til (Schiefloe, 2012)

2.5.2 Informasjonssikkerhet

Kraftbransjen er underlagt beredskapsforskriften og § 6 omhandler informasjonssikkerhet. Det er denne som skal etterleves for nettselskapene.

Når en snakker om informasjonssikkerhet må en ta inn over seg spekteret med ondsinnet handling, i tillegg til feil og hendelser som kan inntreffe i IKT systemene. Informasjonssikkerhet er ikke bare et teknisk problem, men er svært avhengig av personene og organisasjonene som er rundt systemet (Hikstad, at.al. s, 150. 2012).

Trusler mot IKT systemer blir inndelt i tre hoved grupper.

1. Utilsiktede hendelser er mulige fordi det er svakheter i IKT systemene, uheldige ansatte eller av eksterne hendelser. Disse hendelsene skjer med reint uhel. For eksempel lynnedslag, strøm stans, brann, disk crashes, kommunikasjons feil, feil i backups og feil utførelse av ansatte. For å begrense risiko i forhold til denne type trusler er det viktig å tenke gjennom de tekniske og menneskelige sidene av et IKT system. På den tekniske siden kan det gjøres målinger der en ser på hva som skjer om en mister en komponent, at dette ikke fører til at hele systemet slutter å fungere. På den menneskelige siden er

det viktig å huske å ha høyde for at bruker av IKT systemet og de som bygger IKT systemet og vedlikeholder IKT systemet kan gjøre feil eller bruke systemet på en uheldig måte. Mangel på kompetanse om hvordan systemet skal brukes og tilgang til nøkkel personell kan utgjøre en sårbarhet (Hikstad at.al. 2012)

2. Generelle angrep er angrep som ikke er direkte siktet på et spesielt IKT system. Men er heller et angrep som er rettet mot flere forskjellige IKT systemer. Eksempler er høyt antall av ondsinnede software som finnes på internett. Disse kan for eksempel være rettet for å gi tilgang til maskin resurser, eller få tak i personal informasjon som brukernavn og passord og kreditt kort nummer. Selv om disse ikke er direkte linket til et spesielt system kan de gjøre stor skade. Risikoen for generelle angrep øker når en bruker utsatte komponenter som COTS. Høy risiko får en når ansatte surfer på internett fra systemer som har kritiske funksjoner, remote tilgang til kontroll systemer og portable enheter til kritiske systemer (Hikstad, at.al. 2012).

3. Direkte angrep er direkte angrep som er rettet mot et spesielt system eller selskap. Disse laget for å skade dette ene systemet eller organisasjonene. Angrepet kan være alt fra fysisk skade som innbrudd, vandalisme til angrep via internett. Kommer angrepet fra internett kan den som utfører angrepet sitte langt borte eller det kan være en insider jobb for å ramme IKT systemet. Fysiske angrep kan også være kombinert med online angrep. Noen angrep vil trenge direkte tilgang til maskinene for å skade iKT systemene dette vil kreve personell som har kunnskap og er dedikerte. Disse angrepene er sjeldne men vil ha en stor konsekvens. disse angrepene må en også ta høyde for (Hikstad, at.al. 2012).

Flere av problemene som er relater til sikkerheten til IKT systemene har røter i kvaliteten til eksisterende løsninger. Erfaring viser at software inneholder en mengde av sårbarheter som kan brukes av angripere for å gjennomføre generelle uoppdagede angrep. Antallet på (malware) har økt de siste årene og er økende. Det finnes redskap for å utføre angrep mot systemer og en trenger liten kunnskap for å bruke disse. Da snakker vi om virus, ormer, trojaner, spyware, bakdører, nøkkellogger og mange andre, men hovedprinsippet er det samme det er en kode som brukeren ikke har kontroll over og ofte får det uheldige konsekvenser for brukeren eller virksomhetens systemer og nettverk. Målet med disse angrepene kan være:

- Tilgang til maskiner for konfidensiell person informasjon
- Høste personell informasjon for salg eller svindel
- Få tilgang til maskinens ressurser og så bruke maskinene til et større angrep.
- For å overvåke emails eller anen korrespondanse relatert til en spesiell person som er av interesse.
- For å få bruker navn og passord til mange internett tjenester, ved hjelp av nøkkel logging.
- For å logge en brukers aktiviteter på internett for å lage en markedsprofil.
- For å kryptere filer og forlange løsepenger for å av å kryptere
- For å ta kontroll over produksjons systemer for å skade en virksomhet eller et samfunns strøm leveranse, vann, olje produksjon, atomkraft forsyning eller trafikk signaler.

For å forbedre informasjonssikkerheten er det viktig å utføre oppdateringer når de er tilgjengelige for å minke sårbarheten som alltid vil være tilstede i et system. Oppdateringer kan være problematisk det tar tid og kan gi nede tid for systemene og kan også påvirke systemets stabilitet. Det å ikke utføre oppdateringene er en risiko vil føre til at systemet blir mer sårbart for angrep (Hikstad, at.al 2012). Å kjenne igjen et angrep kan være vanskelig for en person som ikke er vandt til dette. Eksempler fra dette har vi fra oljeindustrien, som viser at en maskin kan være ustabil i flere dager og uker uten at noen tenker at dette skyldes at maskinen er utsatt for et virus (Hikstad, at.al 2012). For å forvisse seg om at slike hendelser blir oppdaget og respondert på avhengig av organisasjons kultur ikke bare på de tekniske utfordringene. En IKT sikkerhets hendelse trenger ikke nødvendigvis lede til utilgjengelig system som til det beste stenger seg ned eller går inn i safe mode. Fakta er at slike hendelser kan gi alvorlige konsekvenser som at systemet forandrer seg eller ikke forandrer seg og det ser ut som alt er ved det samme. Men uten at en vet det, er det noen som overvåker kommunikasjonen eller kopierer konfidensiell informasjon. Flere angrep mot IKT system har fått store konsekvenser for kritisk infrastruktur. Som Stuxnet i juli 2001 (Hikstad, at.al 20012).

2.5.3 Sikkerhets kultur

I en lengre tid har det vært fokus på sikkerhetskultur i flere bransjer, det som er viktig å merke seg er at alle har en sikkerhetskultur spørsmålet er hvor god er

sikkerhetskulturen i virksomheten. Det er vanskelig å forklare og beskrive kultur. Mange oppfatter det slik har vi det hos oss. Reasons sier om kultur.

- Few phrases occur more frequently in discussions about hazardous technologies than safety culture. Few thing are so south after and yet so little understod. (Reason, 1997)

Reason (1997) mener at en må ha en velorientert kultur for å få dette til må en ha ansatte som rapporterer om feil og nestenulykker. Det er da viktig at organisasjonene er rettferdig, det må være en tillit til de som behandler rapportene om hendelsene og nestenulykkene. Ledelsen må oppmuntre til informasjonsflyt om sikkerhet. Organisasjonen må være fleksibel slik at den kan endres uavhengig av organisasjonsstrukturen. Ikke minst må organisasjonene være lærende den må ha evne til å trekke riktige konklusjoner ut fra sikkerhetsinformasjon og villig til å gjennomføre endringer om det er behov for dette. Reason (1997) viser til noen sentrale kjennetegn ved en god sikkerhetskultur.

1. Informert kultur det vil si en organisasjon som innhenter data både om eventuelle ulykker, men også nestenulykker. En gjennomfører proaktive tiltak som sikkerhetsrevisjoner og undersøkelser av sikkerhetsklima.

2. Rapporterende kultur der alle ansatte stimuleres til å rapportere hendelser der de ansatte har tillit til at ledelsen behandler hendelsesrappotene og impliserer personer på en rettferdig måte.

3. Fleksibel kultur der organisasjonene evner å lære av de rapporterende hendelsene og sikkerhetsrevisjonene slik at sikkerheten forbedres.

Turner (1978) og Turner og Pidgeon (1997) i menneskeskapte ulykker viser til at sikkerhetskultur er måten en ser verden på og en måte å ikke se verden på. I følge Truner er det et grunnleggende og langvarig avvik mellom kulturelle antagelser og det som faktisk foregår. Kultur kan altså skape en blindhet (en ser ikke skogen for bare tre) for visse farer og trusler. Turner kaller dette for inkubasjonsfasen og denne kan føre til en alvorlig hendelse eller katastrofe.

Figur 5. Viser stadiene i Turners failure of forsight model.

Kultur er et sentralt begrep når det gjelder organisasjoners sårbarhet og problemer, organisasjonskultur i forvaltningen ble trukket fram som en av forklaringene på den dårlige håndteringen av terrorangrepene 22 juli 2011 i Oslo og på Utøya. Det som kan synes å være vanskelig å se er om kulturen er et premiss for systemets sårbarhet og kan øke risikoen for ulykker eller om den er en del av løsningen (Engen, at.al 2016).

Janne M Hagen (2009) utførte en undersøkelse på hvordan ansatte forholdt seg til organisasjonens sikkerhetsretningslinjer, og om de hadde de forventede holdningene som var ønsket. Hun fant et gap mellom hva som var forventet og hva som var av holdninger til sikkerhet. Hun fant noen barrierer som må overstiges for å få en god sikkerhetskultur rundt dette med sikring/security hendelser. 1. Det ble ikke innrapportert, 2. Liten kunnskap om sikring/security ikke i stand til å kjenne igjen et brudd på sikring/security. 3. Hvordan ser de ansatte på dette med å innrapportere hendelser som angiveri? Eller at nyansatte må få en ny sjanse for å lære. Noe mente at dette ikke var deres ansvar (Hagen, 2009).

2.6 Risikostyring

I boka risikostyring til Aven (2007) skriver han at med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko (Aven, s, 13. 2007). Det vil si at på den ene siden må en skaffe seg en oversikt over risikoforhold, effekt av tiltak og grad av styrbarhet av risiko. På den andre siden må en se på metoder, prosesser og strategier en kan benytte seg av for å styre risikoene (Aven, 2009). Tradisjonelt blir risikostyringen gjennomført som en styringsprosess, der en kartlegger situasjonene og problemformulering. Dernest må en sette noen mål opp mot økonomi eller sikkerhet. Videre må en søke etter løsninger for å nå målet ved hjelp av analyse verktøyer får å se hva som bringer oss best opp mot de målene som er satt. Når vi har analysert og funnet de beste løsningene må en ta et valg og gjennomføre dette. Det er viktig å få

tilbakemeldinger og evaluere etter prosessen slik at en kan ta med seg læring av prosessen (Aven, 2009).

Figur 6. Generell styringsprosess. Modellen er beskrevet ovenfor.

Risikoanalyse delen av styringsprosessen er viktig, det er disse analysene som gir oss beslutningsstøtte i valg av alternativer og løsninger. Risikoanalyser bør inneholde en identifikasjon av initierende hendelser som farer, trusler og muligheter. Det må foreligge en årsaksanalyse der en ser på hva som må til for å få en hendelse. Konsekvensanalysen gir oss en forståelse av hva konsekvenser en kan få om hendelsen inntreffer. Det bør også foreligge en risikobeskrivelse i analysen (Aven, 2007).

Risiko påvirkes av vår oppfatning til risiko som om den er kontrollerbar, frivillig, hva avstand har jeg til risikokilden, kan jeg se den, er den godt kjent og hva hendelse innebærer risikoen.

I boka risikostyring til Aven (2007) så skriver han om fem suksessfaktorer for risikostyringen. Første faktor er betydningen av å forstå de grunnleggende prinsippene. Han hevder at mange eksperter og ledere innen risikoanalyse og styring ikke forstår de fundamentale byggeklossene innen fagområdet. Blant annet hva risiko og usikkerhet betyr, sannsynlighetsmodell, rasjonale for bruk av forventning verdier i risikostyringen, bruk av forsiktighetsprinsippet og føre var, hva som er kost-nytteanalysens basis (Aven, 2009 s, 153.). Han fremhever at det er et stort forbedrings potensiale. Faktor to

synliggjøring av usikkerhet for ledelse og beslutningstaker. Utfordringen ligger i å presentere usikkerhet på en hensiktsmessig måte, slik at beslutningstakere får et godt beslutningsunderlag. En må ha:

A. mål og problemdefinisjon

B. generering og vurdering av alternativer.

C. beslutningstakers gjennomgang og beslutning.

D. implementering

Faktor tre er bruken av sensitivitets og robusthetsanalyser. Disse bør ta utgangspunkt i endringer i inngangs parameter og så se på effekten på resultatene. Når en tester robustheten i konklusjoner går en motsatt vei. Da ser en på hva som må til av endringer for at en skal komme til å endre konklusjon. Faktor fire går på kost nytteanalyser som ofte blir sett på som det rette redskapet i forhold til å velge blant løsninger (Aven, 2007). Aven (2007) advarer med at dette er ikke alltid det beste. Han stiller spørsmålet med all informasjon når har en det? I noen tilfeller vil en kost nytte analyse gi svar som er negativ, men det er også et spørsmål om hvor risikosøkende eller hvor risikoavers en er. Det vil alltid være usikkerhet rundt hva konsekvenser blir med de alternativene som foreligger. Aven (2007) viser til er vi for forsiktige skaper vi ingenting og er vi for uforsiktige ender det med en katastrofe. Han viser til at forventet nytteteori har et sterkere teoretisk fundament, men ikke særlig egnet for praktisk bruk. Den femte og siste faktoren er bruk av beslutningskriterier, risikoaspektkriterier og andre krav. Det må være en klarhet i beslutningskriteriene for å kunne ta en god beslutning. I industrien i dag er det en utstrakt bruk av risikoakseptkrigerier. Selv om en gjennomfører risikostyringen uten bruk av risikoakseptgrenser så vil det være et behov for å sette krav til løsninger og tiltak for å forenkle beslutningsprosessen. Utfordringen blir å finne en måte som er på linje med virksomhetens filosofi og er praktisk gjennomførbar (Aven, 2009). Aven og Renn (2010) viser til tre komponenter for å ha god risikostyring.

Det må være en Risikovurdering som beskriver oppgaven med å identifisere og utforske typer, intensiteter og sannsynlighet og konsekvensene knyttet til fare eller trussel. Risikovurdering kan antas som et verktøy for å få kunnskap om mulige hendelser og deres konsekvenser. Risikostyring må på den andre siden beskriver oppgaven å

forhindre, redusere eller endre konsekvensene identifisert ved vurderingen ved å velge passende tiltak (Aven og Renn, 2010). Risikokommunikasjon har fire hovedfunksjoner.

- Utdanning og opplysning
- Risikotrening og induksjon av atferdsendringer
- Fremme tillit til institusjoner for vurdering og styring av risiko
- Engasjement i risikobeslutninger og konfliktløsning

3 Metode

Dette kapittelet vil ta for seg hva valg som er gjort i denne oppgaven og presentere forskningsdesign og metode. Vil gjøre rede for hvordan denne oppgaven er gjennomført og hva oppfatninger som kan stilles til oppgavens reabilitet og validitet. Vil også ha en gjennomgang av hvilke utfordringer som oppgaven har gitt i forhold til valg av metode, gjennomføring av intervjuer og utforming av oppgaven.

Denne oppgaven bygger på en kvalitativ metode som forskningsmetode. Denzin og Lincoln (2005) beskriver kvalitativ metode som forskning der en skal lokalisere observatøren i verden.

3.1 Forskningsdesign

Forskningsdesignet er utarbeidet med utgangspunktet til Blaikie (2010). følge Blaikie (2010) skal Forskningsdesignet referer til prosessen og sammenfatter problemstilling, empiri og konklusjon. En må kunne henvise til det som undersøkes, hvorfor en undersøker og hva metode en benytter.

I denne oppgaven er formålet å se på hvordan kan kraftbransjen bruke risikostyring for å redusere sårbarhet og øke sikkerheten opp mot informasjonssikkerhet.

3.2 Forskningsstrategi

En forskningsstrategi skal gi en logikk til det som anvendes for å kunne svare på problemstillingen og forskningsspørsmålene som er stilt i oppgaven (Blaikie, 2010). Det er fire forskjellige forskningsstrategier: Induktiv, deduktiv, retroduktiv og abduktiv. Disse forskningsstrategiene representerer ulike måter av tankesett og måter å trekke

slutninger på for å komme til det en hadde som utgangspunkt (Danemark, 1997). Forskere kan fritt velge en eller flere av disse forskningsstrategiene, men det valget som blir tatt må henge i sammen med problemstillingen og forskningsspørsmålene som skal besvares i oppgaven (Blaikie, 2010).

Denne oppgaven inneholder elementer av induktiv forskningsstrategi. Induktiv forskningsstrategi brukes der enn går fra datainnsamling til teori (Blaikie, 2010, s. 84). Men informasjonen som informantene gir vil ikke kunne gi noen konklusjoner. Informanter vil alltid være påvirket av tolkninger (Blaikie, 2010, s. 85). Abduktiv forskningsstrategi har som mål å beskrive og forstå sosiale prosesser, gjennom utforskning av sosiale aktørers meninger, fortolkninger, motiver, og forklaringer (Blaikie, 2010). Det finnes flere forklaringer på abduktiv forskningsstrategi. Denne oppgaven bygger på Danemarks (1997) forståelse av Abduktiv forskningsstrategi. Da denne oppgaven har som mål å oppnå en ny beskrivelse eller en rekontekstualisering av det som blir forsket på i denne oppgaven. Det handler om en forestilling om noe, og gjennom tolkning, komme fram til en ny forståelse av samme hendelse eller observasjon. Denne nye forestillingen kan være mer utviklet og fordypet i hendelsen eller observasjoner. Det vil si, i denne oppgaven søkes det en forståelse og informanten vil gi meninger og tolkninger som vil stå i sentrum for denne oppgaven (Blaikie, 2010, s 92).

I denne oppgaven benyttes det seg av en kombinasjon av induktiv og abduksjon forskningsstrategi. Intervjuspørsmålene ble utarbeidet med tanke om å få fram data som kunne danne universelle generaliseringer for å forklare mønster og regularitet. Ut fra teorier om Risiko, sikkerhet og sårbarhet. Dette samsvarer med en iduktiv forskningsstrategi, der en benytter seg av tolkningene til informantene opp mot risiko, sikkerhet, sårbarhet opp mot informasjonssikkerhet. I neste omgang ønsket jeg å finne ut om aktørenes motiver og forklaringer opp mot risiko, sikkerhet og sårbarhet opp mot informasjonssikkerhet, om det er en bevissthet rundt dette med elementet av villede hendelser i informasjonssikkerhet. Valget ble da å henvende meg til nøkkelpersoner for å få deres tanker omkring temaene og få en bedre forståelse av den verdenen som blir undersøkt i denne oppgaven. Dette kan betraktes som abduktiv forskningsstrategi. Ønsket var å komme frem til en ny forståelse, gjerne få noen læringspunkter som kan overføres på tvers av bransjer. Dette er noe som kan forstås er i tråd men denne

forskningsstrategien.

Formuleringen av forsknings spørsmål er de mest kritiske i forskningsdesignet ifølge Blaikie (2010, s. 57) det er gjennom disse spørsmålene en velger fokus og retning for det en skal forske på. I denne oppgaven landet jeg på hvordan, hvor spørsmål som tilhører kategorien hvordan *How* spørsmål, disse beskriver hvordan en kan forandre eller få til en forandring (Blaikie, 2010, s. 60).

3.3 Datakilder

I boken til Blaikie (2010) så skilles det mellom primærdata, sekundærdata og tertiærdata. Dette beskriver avstanden forskeren har til dataen som samles inn. Primærdataen er data som forskeren selv samler inn, analyserer og formidler. Dette anses som en styrke siden forskeren selv sitter på førsthåndskilden til denne type data. Sekundærdata er innsamlet av andre enn forskeren. Dette blir da anvendt til andre formål enn de var samlet inn for. Eksempler på sekundærdata er statesikk eller annen rådata. Tertiærdata er data som er samlet inn og analysert av andre, dette øker avstanden mellom forsker og dataene som kan være en svakhet. Når de bruker tertiærdata kan det være begrenset tilgang til de opprinnelige kildene eller råmaterialer som er anvendt (Blaikie, 2010).

Det ble i denne oppgaven valgt å benytte seg av to datatyper; primærdata, i form av intervjuer med nøkkelpersoner og tertiærdata i form av dokumenter og data som er samlet inn, analysert av andre forskere. Det vil si at en som forsker fortolker meningsinnholdet i de allerede skrevne dokumentene som blir anvendt.

Dokumentene som er benyttet i denne oppgaven er offentlige dokumenter som er funnet på nettet. Disse dokumentene er med å beskrive verden og skape mening for det temaet som er valgt.

Nedenfor vises en tabell med en oversikt over hvilke dokumenter som er benyttet i denne oppgaven.

Sektor dokumentet tilhører	**Navn på dokument**	**Utgitt årstall**	**Tilgjengelig fra**	**Type data**

NVE	Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen	2010	Internett	Tertiærdata
NVE	Beskyttelse av kritiske IKT- system i energiforsyningen	2012	Internett	Tertiærdata
Difi	Internkontroll i praksis – informasjonssikkerhet	2017	Internett	Tertiærdata
Difi	Styringssystem for informasjonssikkerhet	2012	Internett	Tertiærdata
NSM	Kan sikkerhet styres	2016	Internett	Tertiærdata
NSM	Håndbok Risikovurdering for sikring	2016	Internett	Tertiærdata
NSM	Veileder Sikkerhetsstyring		Internett	Tertiærdata

Tabell 4. Oversikt over dokumenter benyttet i denne oppgaven

3.4 Valg av informanter

Valget i denne oppgaven ble å intervjue nøkkelpersoner som i følge Andersen (2006) er personer med god oversikt over temaene som forskeren ønsker å finne ut mer om. For denne oppgaven var dette viktig, da det gjennom samtaler med personell som sitter med kunnskapen, kan gi en bedre forståelse for hvordan risiko, sikkerhet og sårbarhet styres opp mot informasjonssikkerhet.

I denne oppgaven er kraftbransjen valgt for å spisse oppgaven, og i den forbindelse valgt jeg å intervjue personell med HMS ansvar fra nettselskapene som har ansvaret for strømnettet. Forespørselen om informanter til oppgaven var bred, ønsket å intervjue personer i nettselskapene som hadde ansvar for HMS ikke IKT selv om informasjonssikkerhet ofte er underlagt IT avdelinger. Dette var bevisst fordi jeg ønsker å se etter den helhetlige risikostyringen ikke avdelingsvis. Det viste seg fort at dette ga meg noen utfordringer, de forskjellige selskapene hadde forskjellige navn på

funksjonene alt fra HMS leder, driftsleder, sikkerhetsansvarlig og IKT ansvarlig. Det skulle vise seg at det var vanskelig å få informanter innen emnet jeg hadde valgt. Av ti henvendelser ble resultatet at jeg fikk intervjuet to personer med ansvar inne HMS. Det kan være mange årsaker til at selskapene ikke ønsket å la seg intervjue. I noen tilfeller fikk jeg tilbakemelding på at de var i ansettelse faser for å få inn personell med sikringskompetanse andre hørte jeg ikke fra. Det førte til at jeg måtte ta en bestemmelse om at jeg omformulerte den opprinnelige problemstillingen min og gikk for å intervjue myndigheter som har et ansvar opp mot bransjen og generelt opp mot sikkerhet. De jeg valgte å intervjue fra myndighetene var NVE som har ansvaret opp mot kraftselskaper, NSM som sitter med den største kompetansen innen sikring og Difi som har et ansvar for informasjonssikkerhet innen forvaltninger.

Dette kan ha forringet mitt utgangspunkt for å komme med konklusjoner opp mot kraftbransjen siden noen av disse myndigheten ikke har et eget ansvar med kraftbransjen, men et overordnet ansvar for flere virksomheter i Norge. Utfordringen med en så nøye utvelgelse prosess er at jeg kan ha kommet i skade til å velge personer som deler, eller som jeg underbevisst tror deler de antakelse som jeg hadde i forkant av oppgaven.

Organisasjon	**Kjønn**	**Omtales i oppgaven som**
Nettselskap	Mann	Selskap 1
Nettselskap	Mann	Selskap 2
NVE	Kvinne	Informant NVE
NSM	Mann	Informant NSM
Difi	Mann	Informant Difi

Tabell 5. Oversikt over informantene.

3.4.1 Gjennomføring av intervjuene

I denne oppgaven ble det utarbeidet to intervjuguider. Ønsket med intervjuene var å få så mye informasjon og betraktninger fra de som ble intervjuet, derfor falt valget på en intervjuguide som hadde åpne spørsmål og der jeg kunne stille tilleggsspørsmål utover

det som allerede var fastsatt i guiden. Graden av struktur i intervjuet var å ha en intervjuguide med tema, en fast rekkefølge og med kun åpne svar (Jacobsen, 2005, s. 145).

Under intervjuene ble guiden benyttet som en mal der jeg stilte spørsmål og lot personen som jeg intervjuet snakke fritt, en del av spørsmålene i guiden ble dermed svart på uten at disse ble direkte tatt opp med den som ble intervjuet. Intervju guiden til kraftselskapene/ nettselskapene hadde noen tilleggs spørsmål som ikke ble stilt til NVE, NSM og Difi. De ble det utarbeidet en annen intervjuguide til. Teknikken som jeg brukte med å få til samtale under intervjuet brukte jeg på begge gruppene.

Spørsmålene som ble utarbeidet er i den grad jeg har hatt kunnskap til å bli så presise så mulig samtidig være åpne nok til å få fram områder som kan belyse og gi svar opp mot problemstillingen som er i oppgaven. Ønsket var ikke å sammenligne risikostyrings verktøy som ISO standere opp mot NS 3832, men se på hva som ligger av verktøy, som kan brukes for å bedre risikostyring i virksomheten uavhengig av stander en velger.

Alle informanter har mottatt den samme informasjonen om oppgaven i forkant av intervjuene. Opplevde informantene godt forberedte til intervjuene og flere av informantene har gitt meg tips om hvor jeg kan finne mer informasjon rundt området som jeg har hatt ønske om å se på i denne oppgaven. Informantene var åpne og ga mange finne svar som har gitt meg mye og mer en det jeg trengte for denne oppgaven. En utfordring med å la informantene få snakke fritt er at en kan komme i den situasjonen at informanten overtar intervjuet, dette er en utfordring når en bruker nøkkelpersoner (Andersen, 2006). Det er viktig at en som forsker klarer å styre intervjuet slik at informanten ikke tar overhånd. Som forsker må en være aktiv i rollen som intervjuer og være påpasselig at en holder seg til temaene i guiden. Andersen (2006) kaller dette en aktiv intervjuing, og er en god til å styre vil dette øke validiteten og reabiliteten i forskningen. I denne oppgaven har jeg prøvd å ha en så aktiv forsker rolle som det for meg lot seg gjøre.

Intervjuene varte alt fra 60 minutter til 45 minutter, informantene snakket lenge og det var stort sett jeg som avrundet intervjuene etter en time da det var det som var satt i forespørselen til informantene. I alle intervjuer fikk jeg godt i gjennom alle spørsmål som jeg ønsket svar på.

Intervjuene ble utført på følgende måte:

To av intervjuene ble utført med båndopptaker og ansikt til ansikt.

Ett av intervjuene ble utført over telefon med båndopptaker

To intervjuer ble utført over telefon uten båndopptaker.

Det er en liten svakhet at jeg ikke fikk intervjuet alle informantene ansikt til ansikt, men på grunn av lange avstander og tidsbruk ble det en enighet mellom informant og meg avtalt telefon intervju der reise avstanden var stor. Dette kan ha svekket oppgaven min noe opp mot validitet og reabilitet.

3.4. Datareduksjon og analyse

Da intervjuene var gjennomført og transkribert, ble det sett etter mønstre som gikk igjen hos informantene. Datareduksjon er mest synlig når den gjøres i kvantitative analyser. Denne oppgaven har en kvalitativ utforming og i kvalitativ forskning er datareduksjonene mer utfordrende å fordi skille mellom datareduksjon og dataanalyse. prosessene med innsamling, reduksjon og analyse av data overlapper (Blaikie, 2010). Det som er sentralt i en kvalitativ analyse av data finnes det koding som omhandler forklaring, analyse og generalisering av teori. Sentralt i kvalitative analyse av data finnes det koding i følge Balikie (2010) omhandler dette forklaringer, samt analyser og generalisering av teori. Åpen koding omhandler å bryte ned data til ulike kategorier og sub- kategorier. Axial koding blir utført ved å bruke kodeparadigme som involverer det å tenke på ulike årsaksforklaringer, kontekster, inngripende forhold, handlingsstrategier for respons på ulike strategier og de mulige konsekvensene av handlingen som ikke har oppstått (Blaikie, 2010). Denne formen for koding forklart av Day (gjengitt i Balikie, 2010) som en sirkulær prosess der det dreier seg om å forklare, klassifisere og koble sammen. I denne oppgaven er det elementer av denne kodingen. Intervjuguiden er inndelt i kategorier og dette har gjort det enklere for meg når det kom til å analyser funnene. Det ble dermed enklere å sette disse funnene opp mot forskningsspørsmålene som ble utarbeidet i denne oppgaven. I empirien har funnene blitt slått sammen med dokumenter og intervjuer og tilslutt koblet teori, dokumentanalyse og funn fra intervjuer opp mot hverandre for å kunne drøfte, og svare på problemstillingen.

3.5 reliabilitet og validitet

I all forskning vil forforståelsen være med å forme forskningen og problemstillingen som er gitt. Denne oppgaven er ingen unntak. Oppgaven bærer preg av mine forestillinger om hva kjennskap kraftbransjen har til informasjonssikkerhet, risiko, sikkerhet og sårbarhet opp mot dette. Basert på en del som har vært i media så gikk jeg nok inn med en forestilling om at det kunne være mangler på forståelse rundt dette med risiko, sikkerhet, sårbarhet rundt informasjonssikkerhet. Har likevel prøvd å ha et åpent sinn gjennom arbeidet med oppgaven.

Det å arbeide alene i denne oppgaven kan ha gitt noen svakheter fordi det er bare mine betraktninger som kommer frem. Alle intervjuer ble transkribert, dette har vært hjelpsomt for å kunne gå tilbake å sammenligne svarene som ble gitt under intervjuene.

En svakhet ved oppgaven var at informantene fra NSM og Difi ikke hadde inngående kjennskap til kraftbransjen men kun kunne uttale seg generelt og komme med sine antakelser. Dette var noe som jeg så på forhånd og dette kan svekke validiteten på funnene som har komt fram i denne oppgaven.

3.6 Etiske betraktninger

Grunnleggende prinsipper for forholdet mellom informant og forsker bygger på informert samtykke, krav om privatliv og korrekt gjengitt (Jakobsen, 2006). Dette har vært et hensyn som har vært i tankene gjennom hele prosessen.

Det ble sendt ut en informasjonsmail i forkant der det ble nevnt at en ønsket å benytte båndopptaker for å kunne transkribere intervjuene. Ingen av informantene stilte spørsmål rundt dette, selv om de hadde valget til å avstå fra å bli tatt opp på bånd. To var klar på at det var viktig at jeg slettet lydfilen etter transkribering. Alle informantene ble informert om at samtlige bånd opptak ville bli slettet når transkribering var utført. Dette er blitt utført. I noen av intervjuene ble det avtalt at noen deler skulle utelattes fra transkriberingen, da dette var særs personlige betraktninger og som ikke tilhørte oppgaven.

4 Empiri

Empiriske undersøkelser har som hensikt å utvikle ny kunnskap enten man er ute etter å beskrive et fenomen eller man ønsker å forklare sammenhenger (Jacobsen, 2005) i denne oppgaven ønsker jeg å se på hvordan kraftbransjen kan bruke risikostyringsverktøy for å bedre sikkerheten for informasjonssikkerhet. Kraftbransjen er en del av den kritiske infrastrukturen i Norge.

I denne oppgaven har det blitt intervjuet to fra nettselskaper. Det ble utarbeidet enn intervju guide (jf. Vedlegg), det var denne som dannet grunnlaget for samtalene med representanter fra selskapene. Jeg var interessert i å snakke med personer med et lederansvar opp mot HMS. I tillegg falt valgte på å intervjue personer fra tilsynsmyndigheter. Valgte da NVE som er myndighetene som fører tilsyn med bransjen, samt NSM og Difi. Samt å se på veiledningene og aktuelle rapporter utarbeidet av myndighetene NVE, NSM og Difi. Ønsket var å se om det fra NVE sin side var noen styringer opp mot dette med risikostyrings systemer og hvordan de går frem for å heve kompetansen rundt emnet sikring/security. I tillegg valgte jeg NSM og Difi som har et myndighetstilsyn til henholdsvis opp mot forebygging av å villede handlinger og informasjonssikkerhet. Det var interessant og se hva inntrykk de har av jobben som blir utført i bransjen og hva anbefalinger og føringer som ligger fra dem.

Har valgt å kategorisere og sammenfatte svarene som kom frem i intervjuene og i de tilfeller der det er ulike syn vil det komme frem av teksten. Deler av datamaterialet er utelatt da de er blitt vurdert som mindre relevant for problemstillingen. Empirikapittelet vil bli avsluttet av en kommentar til hovedfunnene fra denne undersøkelsen.

I kapitel 5 vil jeg drøfte funnene opp mot den utvalgte teorien og det data materialet som foreligger.

4.1. risikopersepsjon

I starten av intervjuene både for nettselskapene og myndighetene (NVE, NSM og Difi). Fikk Informantene spørsmål om å beskrive sitt perspektiv på risiko, og forklare risiko på en enkel måte. Dette for å se om de er bevisste de briller som de har når de ser på risiko generelt.

- ***Det finnes flere perspektiver og definisjoner på risiko, hvordan vil du beskrive og forklare risiko på en enkel måte?***

Nettselskapene svarte på dette litt sprikende, det ene selskapet beskrev at de jobbet utfra et helhetlig risikostyrings system med definerte risikokriterier. Men begge selskapene ga utrykk for at de jobbet mye med risiko nedover i organisasjonene. Selskap 1 og 2 jobbet med risiko på avdelingsnivå, det blir utført ca. 100 analyser i året i hvert selskap, og at dette var noe de jobbet *jamt og trutt med*. Begge selskapene ga utrykk for at det også fantes en overordnet ROS analyse for hele virksomheten som blir dannet på grunnlag av risikoanalysene som er tatt avdelingsvis.

Fra myndighetssiden ble dette spørsmålet mer utdypet.

NVE ga uttrykk for at det overordnede risikoperspektivet er å sørge for at det kommer strøm ut til forbruker. I den forbindelse er det naturkrefter som vær, hendelser utløst av skred og branner som vil være den største trusselen for strøm brudd. NVE sitt syn er opp mot leveransen av strøm, de er opptatt av forsyningssikkerheten. De trussel aktørene som NVE er mest opptatt av er natur krefter, som vær, og det er dette som er overordnet når NVE ser på risiko. Samtidig nevnes det at bransjen er i endring når det gjelder digitalisering og modernisering blant annet digitale strømmålere.

> *-Vi vet jo at når vi legger noe ut på internett og en ikke har satt i gang sikringstiltak så blir det infisert med virus.*

NSM sitt syn på risiko retter seg mot villede handlinger, handlinger som er begått med hensikt. Det er det som er NSMs perspektiv på risiko. NSM har spesialisert seg på feltet som går på villede uønskede handlinger. NSM fremhever at det er viktig at virksomheter selv setter i sammen risiko bilde og at de finner den måten som passer for den enkelte virksomhet. Det vil si at virksomhetene må både se på risiko innen det tradisjonelle uønskede hendelser som oppstår og uønskede hendelser som kan bli utført med vilje.

Difi har et enda mer spesifikt syn på risiko. Deres perspektiv er forankret i mye av teorien til Aven og ISO 31000. Der de ser på risiko som målet. At en må ta med seg dette med effektivitet. Samtidig vier de til at ISO standerne kan i noen tilfeller være

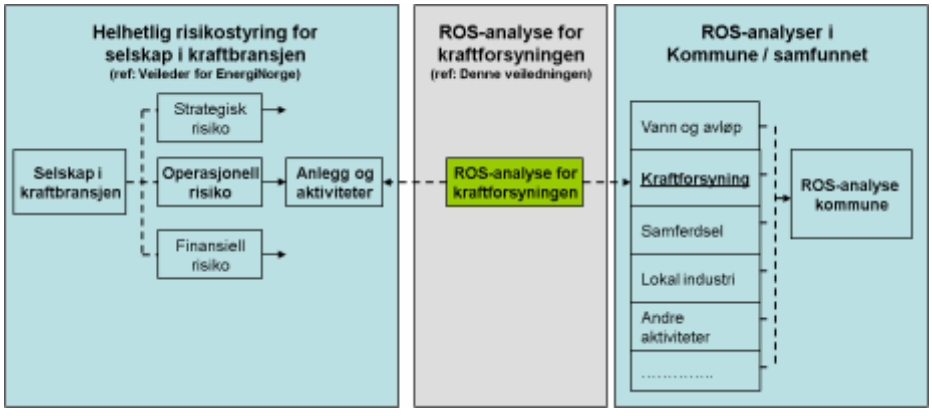
dårlig oversatt til Norsk og at dette i noen tilfeller fører til misforståelse eller er misvisende.

4.2 Risikostyring

Intervju objektene fikk flere spørsmål som gikk på risikostyring. Fra NVE er det laget en veileder til selskapene som viser i detalj hvordan en kan komme i gang og gjennomføre en ROS analyse. Veilederen peker på noen viktige gevinster og anvendelser ved riktig bruk av ROS analyser for kraftbransjen som:

- Økt evne til å forebygge og håndtere ekstraordinære hendelser
- Mer stabil strømforsyning og færre avbrudd
- Mer fokusert ressursbruk til forebyggende og skadereduserende tiltak
- Synliggjøre hvilke konsekvenser ekstraordinære hendelser kan medføre for virksomhetene og samfunnet, sik at ledelsen i virksomheten kan bruke dette som en viktig planforutsetning
- Systematisere og dokumentere risiko og sårbarhet i forbindelse med hendelser som virksomheten kan stå ovenfor
- Et ledelsesverktøy for bedre måloppnåelse i virksomheten

NVE viser til at ROS analysen blir en del av samfunnets risikostyring på den ene siden og virksomhetens helhetlige risikostyring på den andre siden se figur 7.



Figur 7. Viser sammenhengen mellom risikostyring på selskapsnivå, ROS analyse av et kraftforsyningsanlegg og samfunnssikkerhet.

I innledningen til veilederen peker den på at kraftforsyningen representerer en grunnleggende infrastruktur i samfunnet. Videre vises det til forskrift om beredskap i kraftforsynings (Beredskapsforskriften- Bfk) der det stilles krav til utførelse av risiko

og sårbarhetsanalyser (ROS analyser) for alle kraftforsyningselskaper årlig.

Veiledningen til NVE tar for seg følgende spørsmål:

- Hvilke krav stiller beredskapsforskriften til risiko og sårbarhetsvurderinger?
- Hvilken metode bør benyttes?
- Hvordan planlegger man en ros analyse og hvordan kommer man i gang?
- Hvordan gjennomføres de ulike stegende i ros analysen?
- Hvordan følger man opp resultatene fra ros analysen
- Hvordan kan resultatene visualiseres og kommuniseres?
- Når det kommer til metoder for å finne sårbarheter henviser veilederen til bow-tie
- Diagram for å vise hva som inngår i ros analysen.

Videre viser veiledningen til risikoanalyse som er beskrevet i boken Risikoanalyse-prinsipper og metoder med anvendelser (Aven at.al 2008). Denne prosessen er basert på ISO 31000.

Veiledningen deler ROS analysen opp i 3 nivåer der nivå 1: er en overordnet ros analyse for å danne en fullstendig oversikt over alle anlegg og kritiske prosesser som virksomhet eier eller driver. Finne hvilken betydning disse har for totallsystemer i en ekstraordinær situasjon. Da vil man kunne identifisere hvilke anlegg som har størst betydning i verdikjeden. Nivå 2: Ros analyse av anlegg der en har en omfattende kartlegging av mulige farer, trusler og uønskede hendelser og tilhørende risiko. De viser til fordelen med å bruke grovanalyser er, en kan gjennomføre denne med begrensede ressurser men samtidig vil metoden gi muligheter for å etablere et nyansert bilde av risikoen. Den vil også avdekke om det er behov for mer detaljert ros analyser (Nivå 3). Nivå 3: er en detaljert ROS analyse av delsystemer eller komponenter. Viser da til feiltre eller hendelsestranalyser.

På spørsmålet om hvilke fordeler og ulemper finner en ved risikostyringsvertøyene som dere benytter svarte begge selskapene at de ikke benyttet seg av ROS veilederen til NVE. Selskap 1 benyttet seg av analyser som bygges ut av detaljer men at de bruker veilederen først og fremst som et hjelpemiddel for å se hvor de skal gjøre analyser først.

- *Vi gjør det ikke ulikt veiledningen til NVE men vi hopper rett inn i nivå 3.*

Selskap 2 svare at de bruker et system som er utviklet av et selskap og av historiske årsaker så er dette blir tilpasset i et system. Dette systemet føler de fungerer bra, fordelene er at sentralt, så ivaretas deres behov, følger opp tidsfrister prosjekter og lignende. Informanten fra selskap 2 klarer ikke komme på noen bakdeler ved systemet som de bruker.

- *Overordnet Ros analyse kjøres 1 gang i året i henhold til lovverk, dette ligger i systemet, og når det nærmer seg fyrer systemet av til alle deler av selskapet og disse starter opp med egne ros analyser. Videre blir disse innrapportert i systemet, dette legges så inn i den overordnede ros analysen for hele konsernet.*

I avdelingen kjørers det ikke dybde ros analyser som NVE anbefaler i veiledningen.

Myndighetene svarte på dette spørsmålet på følgende måte.

NVE viser til veiledere som de har utgitt, der en viser til sannsynlighet og konsekvens. Videre ble det nevnt at når det gjelder informasjonssikkerhet, så er det en del som en kan få statistikk på om en tenker på virusinfeksjoner. Men så er det nye typer angrep, fordelen er at generelt sett så vil en risikoanalyse bidra til å heve kompetansen og forståelsen for risiko og en får et bevisst forhold til hva en kan håndtere og hva en må overføre til en beredskapsplan. Prosessen kan være vel så viktig som selve resultatet. Viktig å involvere folk og lære.

Difi svarte på dette spørsmålet med at ulempene med ROS er håndteringen av selve analysen.

- *I prinsippet er dette ISO 31000.*
- *Risiko analysen ser på sårbarheter og konsekvenser, veilederen 31010 er full av metoder, rosen i seg selv er en grovanalyse.*

Han peker på problemet med at en blander inn risikoanalyse / risikovurdering. Hans erfaring er at de som utfører disse ikke er helt klar over hva de gjør av analyse eller vurdering. Resultatet blir en matrise som er god visuell, men viser ikke nødvendigvis den reelle trusselen, og om en må ta handling for å redusere risiko. Han viser til at det

bør legges til rette for gode analyser og det må være en begrepsforståelse i organisasjonene. Informanten viser til at det ofte er to typer av perspektiver på risiko forankret i fagtradisjoner og dette må kommuniseres. Rapporten til Difi (styringssystemer for informasjonssikkerhet 2012) viser at om en lar IT avdelingen ha hele ansvaret for styring av risikovurderinger opp mot informasjonssikkerhet så ender det ofte opp med fokus på IKT systemenes funksjoner ikke på informasjonssikkerhet.

NSM mente at fordelen til ROS ligger i det visuelle og at dette gjør det enklere når en skal diskutere eller bestemme om en ønsker å bruke ressurser på å løse et problem. Bakdelen kan være at det blir en felle, at en fremstiller dette som en sannhet. Informanten tar opp dette med sannsynligheter og konsekvenser og at med dette treffer modellen rett inn i beslutningsprosessen.

> *- Den treffer rett inn i en beslutningsprosess, det gjør ikke NSMs veiledning, for denne er mer analyse rettet, den er mer faglig, og derfor kan det godt hende at for mange kan det være riktig å transformere dette inn i en annen sammenheng.*

4.3 Risikoanalyser

På spørsmål til selskap 1 og 2 om hva risikoanalyser som brukes for å avdekke risiko. Svarte selskap 1 at de har ikke har noen metodikk på disse analysene, men de viser til at de bruker nivå 3 i veilederen til NVE. Selskap 2 svarte på dette, at dette ble varetatt uten å utdype dette noe mer. Selskap 2 viser til KraftCERT som kartlegger mulige trusler innen for cyber kriminalitet. Begge selskapene var opptatt av at det var barriere styringen som var viktigst.

- *Det er barriere styringen som betyr noe, når risikoanalysen er utført dreier vi over til barriere syring.*

Begge selskapene er en del av kraft CERT som kartlegger mulige trusler innen cyber kriminalitet.

NVE og NSM viser til veiledningen til NSM tre faktorer modellen som tar utgangspunkt i verdi, trussel og sårbarhet.

- *Akkurat den analysefasen så er modellen 5830 serien veldig fin, for den behandler ting som du likevel jobber med når du jobber med sikkerhet. Du jobber med sårbarheter, trusler og verdier.*

Informanten fra NSM gjør det klart at der er ikke sikkert at denne modellen passer for alle, men at det er en del som bruker denne modellen. informanten er også klar på at det viktigste med å gjennomføre en analyse er å kunne presentere den etter på.

- *Da må du presentere den på en måte som går hjem. Som passer i den virksomheten. Om man er vant til å gjøre noe på en måte så bruk gjerne den måten, ikke nødvendig å gjøre dette til en smal disiplin, som går helt til topps. Putte det sammen er viktig og om en leder er vant til å se det på en bestemt måte, så la han få det på den måten.*

4.4 Sikkerhet

Begge nettselskapene fikk spørsmål angående holdnings kampanjer rundt dette med avviks håndtering og hva tiltak som ble gjort i forhold til å bedre og fostre en god sikkerhet opp mot informasjonssikkerhet.

Begge selskapene ga utrykk for at de ikke hadde direkte holdningskampanjer rundt dette emnet. Hos selskap 1 hadde de en egen avviks håndtering for informasjonssikkerhets avvik. Disse kjøres ikke åpent. Videre kunne han formidle at det er få avvik på brudd opp mot informasjonssikkerhet. Selskap 2 kan og melde om at det har vært noen forsøk på svindel som har godt i gjennom barrierene som er satt opp. Begge selskapene ser et forbedrings potensiale opp mot avviksregistrering. Selskap 1 skal i sikkerhetsmåneden ha en undersøkelse internt for å danne seg et bilde over utbredelsen av fishing og sosial altivering i virksomheten. Når det kommer til sikkerhet har begge selskapene, selskaps rutiner på dette med ned lasting av programmer og det er sikkerhetsforskrifter til de ansatte som de skal følge.

Fra myndighetenes side ble det trukket fram at for å få en god sikkerhetsstyring var det viktig at ikke dette ikke ble et IT anliggende men at ledelsen er involvert. Ledelsen må være involvert også opp mot informasjonssikkerhet og det som går på sikring/Security. Dette fordi det handler om leveranser.

- *Alvorlige sikkerhetsbrudd kan jo stoppe leveransene og det er jo åpenbart en sak for ledelsen.*

Difi viser til at sikringstiltak kan ha sideeffekter som en må være oppmerksomme på, når det gjelder tilsiktede uønskede hendelser.

I rapporten fra Difi (styringssystemer for informasjonssikkerhet) peker et av funnen opp til kultur. Rapporten peker på at for å ha en god sikkerhet rundt informasjonssikkerhet så trenger en at styringssystemet er etablert av interne ressurser. Rapporten peker på at en kan ikke kjøpe seg et styringssystem for informasjonssikkerhet det må ligge som en del av kulturen med definerte ansvarsfordelinger.

4.5 Sårbarhet

På spørsmål rundt dette med å redusere sårbarheten svarte begge selskapene at de kjører øvelser opp mot informasjonssikkerhet. Selskap 2 var beviste på at det var viktig å kjøre øvelser uanmeldt og dette ble gjennomført. Øvelsene ble gjennomført på alle nivåer. Selskap 1 ønsket seg mer øvelser som var uanmeldte og av eksterne slik at det ikke ble de som hadde god kjennskap til beredskapen som alltid stod for øvelsene. Han uttalte at det kan fort bli

- *bukken som passer havresekken.*

NVE svarte følgende på dette spørsmålet at det er lovverket som regulerer sårbarheten. Det ligge grundige analyser bak utarbeidingen av det. Det eksisterende regelverket er nå til revisjon. Med vekt på å forbedre regelverket på informasjonssikkerhet, i rapporten fra 2016 så regisseres et regime for helhetlig sikkerhet. Der en anbefaler mer grunnsikring. Dagens regelverk har stort fokus på driftskontroll sikkerhet. Med det nye regime vektlegges også sikring av det administrative støtte system.

Difi var også inne på at det er lovverket som er med og styrer sårbarheten bant annet henviser de til internkontrollforskriften.

Myndigheten fikk anledning til å komme med anbefalinger for å styre risikoen for tilsiktede hendelser mot informasjonssikkerhet innen kraftforsyningssektoren.

- *Vi har ikke utarbeidet noe dokumentasjon på akkurat dette i form av veiledning eller noe sånt, det som foreligger nå er veiledningen til beredskapsforskriften, for 2013.*

NVE viser til at det er teksten som ofte setter en minste stander på internkontrollsystemet og at en gjør en risikoanalyse for å avdekke restrisikoen, restrisikoen må dekkes opp med forebyggende sikkerhet. Selskapene skal ha en beredskapsplan for dette og dette må øves på. NVE viser til at det er ingen steder der det er laget noen anbefalinger om hvor ofte det skal for eksempel gjennomføres risikoanalyser.

Difi mener at ved å følge internkontroll forskriften og eventuelt følge ISO 27000 og ISO 31000 som styringsverktøy og være systematisk vil hjelpe på sårbarheten.

- *Risikoen må systematiseres og forstås og spres ned i hele organisasjonene. Tiltak må følges opp, internkontroll, når hendelser skjer må virksomheten ikke bare håndtere, men gå tilbake å finne årsaken for så å rette opp slik at en ikke får gjentakelse av hendelsene.*

Informanten viser til at sikringstiltak kan ha sideeffekter som en må være oppmerksom på, viktig å få belyst dette. Informanten er inne på at det er viktig med risikostyring for å se helheten. Viser til at tilsiktede uønskede hendelser er bare en av mange hendelser som kan skje i en virksomhet.

NSM viser til dette med å bruke den nyeste programvaren og kjøre oppdateringene.

- *For det første bruke den nyeste programvaren hele tiden, fordi det ligger litt i sakens natur, fordi at angrep retter seg gjerne mot programvarens feil, den utnytter feil,*

Informanten viser også til at NSM har 10 punkter som er viktige for å forbedre informasjonssikkerheten og at 4 av disse er tekniske.

4.6 Kunnskap til emnet sikring/security

I denne oppgaven var jeg interessert i å finne litt ut om kunnskapsnivået for emnet sikring/security som ikke er nytt, men gjerne mer aktuelt nå en før. I den forbindelse så stilte jeg spørsmål til både selskapene og myndigheten om hvordan de vil si at kunnskapsnivået er opp mot sikring/security.

På dette svarte informanten fra NVE at en har ikke kjennskap til alle selskaper. Men viser til at regelverket som NVE bygger på, så ligger det forutsetninger på at bransjen vil være et mål under en eventuell krig. Regelverket som brukes er under revidering og har utviklet seg over tid.

- *historien går tilbake til andre verdenskrig.*

Informanten fra NVE viser til at kunnskapen til sikring/security er varierende.

- *det er noen som er veldig flinke og så er det noen som ikke er så flinke*

Dette har med fagmiljø å gjøre, det er ikke utført noen analyse på det, og det er ikke utført noen kartlegging av kunnskapen av sikring/security i bransjen.

NSM jobber gjennom det som en kaller for sektor tilsyn det vil si at det er NVE som er deres samarbeidspartner opp mot kraft bransjen. Informanten fra NSM viser til at det generelle inntrykket er at det jobbes mye med oppetid. Sikkerheten opp mot vær eller mot hendelser som forårsaker at det blir nedetid for strømnettet. NSM er opptatt at bransjene har sine egne CERT som kraftCERT for da kommer de nærmere bransjen. NSM utrykker at:

- *vi er ikke gode nok for det forandrer seg hele tiden, og det som skjer er at trusselen endrer seg det har blitt mer alvor en det det var før.*

NSMs informant mener at dette er ikke noe en lærer i en engang.

- *pluss man bytter jo folk hele tiden, man bytter stillinger man tar oppdrag, ting forandrer seg. En får inn nye partnere høyst dynamisk.*

NSM viser til at skolene kommer etter hvert når det gjelder sikring/security. Sikring/security er et relativt nytt område som er ganske umodent. Informanten trekker fram Universitetet i Stavanger og da Sissel Jore. NSM gjør masse, har fått nye oppgaver

og jobber en stor del med dette, men de føler ikke de når alle. NSM har som hoved gruppe det offentlige Norge.

- *NEI ikke godt nok.*

Difi oppfatter ikke bransjer i Norge som generelt flinke til å utføre risikovurderinger opp mot sikring/security eller for den sak opp mot safete. Informanten fra Difi viser til at det er ofte misforståelser om hva risiko er. Han sammenligner ofte det å finne risiko er som spillet som en fant på mobiltelefoner som het minesweeper. Det er ofte litt slik at det er tilfeldig, han etterlyser det systematiske arbeidet med å jobbe med risiko. Han viser til at de fleste virksomheter er flinke til å håndtere risiko i hverdagen men når det kommer til risikovurderinger og risikoanalyser så er det mye myter og misforståelser som gjør arbeidet vanskelig og uoversiktlig og tilfeldig.

Difi sitter med det inntrykket at risikostyring mangler systematikk av alle hendelser. Det må være en helhet. Når det gjelder sikring/security så må sikringsvurderingen og forslag til håndtering ligge som beslutningsgrunnlag, og dette må kommuniseres til ledelsen og utdypes. Det vil alltid være et kostnadsspørsmål. Informanten viser til at risikovurderingen må se på sårbarheten, trusselen og verdien.

Begge nettselskapene svarte unisont på at dette var et forbedringsområde. Selskap 1 svarte at de hadde konsentrert seg hovedsakelig med å forbedre og øke risikoanalyser på sikkerhetssiden (safety) siden 2013 for å komme opp på et godt nivå. Videre kunne han fortelle at de nå hadde startet jobben med å få på plass verktøy opp mot informasjonssikkerhet. I tillegg til at de så sine begrensninger innen dette området var begge nettselskaper inne med at det som går på informasjonssikkerhet var knyttet til hovedsakelig IT avdelingen.

På spørsmål om de hadde kjennskap til NS 5830 serien var det ingen av de som kjente til denne standeren, men de hadde kjennskap til NSM, og et av selskapene hadde hatt kontakt med NSM rundt spørsmål forbunnet med sikring/security. Begge selskapene viste til beredskapsforskriften.

- *I energi loven og beredskapsforskriften der står det noen om informasjonssikkerhet*

Begge nettselskapene oppgir at når det gjelder analyser på sikring/security siden så leies dette inn.

- *Vi har nå blitt godt oppbemannet, men vi må oppbygge videre vi må få kompetansen. Vi ønsker ikke spiss kompetanser bare vi klarer oss i det daglige så kan en benytte seg av eksterne spesialisert.*

4.7 Forankring i ledelsen

Et av spørsmålene som jeg ønsket svar på er hvor forankret er dette med informasjonssikkerhet forankret i ledelsen, for å kunne ha en god risikostyring må ledelsen være involvert. Eller er det slik at det er IT avdelingen som står for ansvaret for dette.

Selskapene svarte på dette spørsmålet med at det var en større interesse for dette i ledelsen.

- *Ja vi er selv ansvarlige, det er godt forankret, i de nye EU reglene, når det gjelder personsikkerhet og størrelsen på bøtene om dette brytes har skrudd en del til på fokuset for ledelsen.*

Selskap 1 hadde tanker om at det gjerne hadde vært vanskeligere å få dette fokuset om en ikke hadde hatt lovverket som tvinger ledelsen til å ta innover seg informasjonssikkerhet. Begge selskapene hadde fokus på at det nå var strengere krav til dette med objektsikring og problematikken med dette og det var der gjerne fokuset var.

På dette spørsmålet så er myndighetene alle enige i at det er svært viktig å ha med ledelsen. Når det skal utføres en risikoanalyse må en fra ansvarsområde være en prosessleder og få alle som er brukere og som jobber innen dette område være delaktige i analyse arbeidet. Difi viser til 4 hovedregler som en finner på Difi sine hjemmesider. Informanten påpeker at styringskompetanse hos ledelsen og hos nøkkelpersoner i virksomheten er helt sentralt når det kommer til den faktiske ledelsesforankringen av styringssystemet. De viser til at der ledelsen er involvert så skjer fremgangen raskere. NVE er også inne på dette. Om ledelsen ikke er med, så vil en ikke kunne få

gjennomslag for hvordan en ønsker å håndterer risikoen. I undersøkelsen til Difi (Styringssystemer for informasjonssikkerhet 2012) kommer det frem at revisjoner og tilsyn i virksomheter innen forvaltningen synes gjennomgående å slite med forståelsen av hva et styringssystem er. De har overordnede mål og retningslinjer, men det mangler tilhørende risikovurderinger, koblinger til valgte sikkerhetstiltak, avviks håndtering, jevnlige revisjoner samt ledelsesforankring. Det viser seg at det er varierende oppfattelse om en bør ha et eget styringssystem for informasjonssikkerhet, eller om det bør være et helhetlig styringssystem som dekker mer som målstyring, HMS, miljøledelse osv. Revisjoner og tilsyn viser at de aller fleste virksomheter har bra styring med HMS og regnskap. Dette kan skyldes at dette har blitt sterkt vektlagt tidligere og lederne blir ofte målt på dette. Hos en del virksomheter ser de saksansvarlige styringssystemet ofte kun ut fra sitt ansvarsområde. Det blir gitt et eksempel der HMS ansvarlig bare ser HMS området, informasjonssikkerhetsansvarlig ser bare informasjonssikkerhet. Det viser seg at der en har en ledelsesforankring av styringssystemet har en større driv og framgang for å få på plass et styringssystem. En ser også at varsel om tilsyn, revisjoner eller anmerkninger etter besøk har en sterk igangsettelseskraft. I NSM veileder for sikkerhetsstyring legges det vekt på at det er viktig for at ett styringssystem skal fungere må dette være forankret i ledelsen hos virksomheten.

Under intervjuene og gjennom dokumentene som ligger til grunn for min empiri kom det fram noen interessante punkter som jeg vil ta med meg videre inn i drøftingen.

Noe av det som stikker seg fram er dette med begrepsforståelse og hva en legger i de forskjellige begrepene, dette samsvarer med det som kom fram under sikkerhetskonferansen ved UiS 2017. Det er heller ikke så overraskende at kunnskap er noe mangelfull rundt dette med informasjonssikkerhet, og dette med å trekke inn sikring/security inn i sikkerhetstenkningen. Det som har kommet godt fram og som blir kjerne funnet i denne oppgaven er dette med sikringskultur.

5 Drøfting

I dette kapittelet vil det trekkes linjer mellom teori, funn fra intervjuer og dokumenter som er benyttet for å kunne svare på problemstilling:

- *Hvordan bruke risikostyringsverktøy til å redusere sårbarhet og heve sikkerheten for informasjonssikkerhet.*

Kapittelet er inndelt etter de fire forskningsspørsmålene som ble presentert i kapittel 1 og vil drøft hvert enkelt forskningsspørsmål.

1. Hvilke fordeler og ulemper finner vi i risikostyringsverktøyene
2. Hvordan kan en redusere sårbarheten i kraftforsyningssektoren.
3. Hvordan bedre informasjonssikkerhet i bransjen
4. Hvor viktig er det at ledelsen er involvert og forstår risikobilde

5.1 Hvilke fordeler og ulemper finner vi i risikostyringsverktøyene

På dette forskningsspørsmålet ønsker jeg å drøfte det som kom fram under intervjuene med nettselskapene og fra NVE, NSM og Difi opp mot teorien. Kategoriene som jeg har valgt er følgende: Risikopersepsjon, risikostyring og risikoanalyser. Vil ikke gå inn i den enkelte stander og vil ikke komme med et bestemt forslag.

5.1.1 Risikopersepsjon

Startet teori kapittelet med en redegjørelse av risikopersepsjon, hva innebærer dette og hvordan påvirkes vårt syn på risiko våre beslutninger (Engen, at.al (2016). Boken perspektiver på samfunnssikkerhet viser hvor viktig den faglige bakgrunnen, og det tverrfaglig samarbeid er i arbeidet med risiko og sikkerhetsspørsmål. Av svarene fra nettselskapene og myndighetene kommer det frem at de har tanker og er bevisste sitt faglige og teoretiske standpunkt opp mot risikopersepsjon. Samtlige av intervju objektene er inne på dette som en finner i Engen at.al (2016) om at risikoutfordringene i dag er mer komplekse, faretruende, grenseoverskridende og globale. NVE viser til forsyningssikkerheten, og at en derfor er mest opptatt av naturkrefter som kan påvirke denne sikkerheten. Men viser også til endringer når det gjelder digitalisering og modernisering blant annet digitale strømmålere. Dette fører som sakt inn mer kompleksitet. Flere av de intervjuede nevner Aven i sine svar rundt dette med risikopersepsjon. I tabellen som en finner i perspektiver på samfunnssikkerhet (Engen, at.al, 2016) se tabell 1, ligger perspektivet innen det som kalles svak konstruktivisme og det innebærer at risiko er en objektiv fare som blir mediert gjennom sosiale og kulturelle prosesser, og kan ikke forstås isolert fra disse prosessene. Den kan måles og

vurderes, men metodene må ta hensyn til de kognitive og sosiale mekanismene (Engen, at.al 2016). Det vil si et de ser på risiko som noe som må vurderes utfra hensyn til om den er lineær, kompleks, usikker og tvetydig. Videre trenger enn ekspertkunnskaper for risikobeslutninger men dette må settes i sammen med den sosiale og politisk konteksten (Engen, at.al 2016). Av de intervjuede fra nettselskapene kommer det frem at de er opptatte av at risikoanalysene blir utført på avdelingsnivå. Det er bra i forhold til at de kan regnes som ekspertene. De viser til at de har mange analyser i året men stort sett var dette analyser som var rettet til å opprettholde sikkerhet for ansatte. Når det gjelder informasjonssikkerhet så faller denne inn i det som blir kalt usikre og tvetydige risikoer. NVE viser dette med å svaret - *Vi vet jo at når vi legger noe ut på internett og en ikke har satt i gang sikringstiltak så blir det infisert med virus.* Det er vanskelig å knytte risiko opp mot informasjonssikkerhet. En av grunnene kan være manglede kunnskap noe som kraftselskapene og myndigheten påpeker i intervjuene at det er i bransjen(e). Det er forbundet med stor usikkerhet, det er risikofenomener en vet at vi ikke vet noe om og det er noen risikoer vi faktisk ikke vet at vi ikke vet noen om (Engen, at.al 2016, s 84). Den siste setningen er gjerne det vi kaller for svarte svaner. Terrorhandlinger eller ondsinnede handlinger som tar sikte på å skade samfunnet faller innenfor disse to siste risikokategoriene. For å håndtere vanskelige risikoutfordringer er det viktig å være enig om hvordan skal risiko defineres, hva metoder skal man anvende (Engen, at.al 2016). Det er viktig å være kritisk til utvikling og anvendelse av metoder. Risikoanalyser skal gi beslutningsgrunnlag. Feilaktige risikoanalyser kan gi fatale konsekvenser. Det må være en enighet om hvordan en definerer risikoen og hva kriterier som ligger til grunn for å vurdere kvaliteten på metodene (Engen, at.al 2016).

5.1.2 Risikostyring

Risikostyring er et viktig tema og det finnes mange standere som kan fungere som et hjelpemiddel. Under sikkerhetskonferansen i Stavanger 2017, kom det frem at sikring/security er en del av den helhetlige risikostyringen. I tillegg kom det frem at det kreves en balanse mellom struktur, kompetanse og kultur. Intervju objektene fra nettselskapene hadde et forhold til risikostyringssystem. Men ingen av de to jeg intervjuet fulgte veilederen til NVE. Nå finnes det mange varianter for hjelpemidler for risikostyring som ISO 31000, ISO 22301 – Business continuity management, COSO rammeverk, Barrierestyring – Petroleums tilsynet (Ptil) og NS 5830 beskyttelse mot tilsiktede uønskede hendelser. I følge Aven så er risikostyring alle de tiltak og

aktiviteter som gjøres for å styre risiko (Aven 2009). Det handler om å få innsikt i risikoforhold, hva effekter får en av tiltakene en setter i gang, hvor god er styrbarheten i risikoen. Til dette trenger enn metoder, prosesser og strategier for å kunne kartlegge og styre risikoene. Informant 1 fra nettselskapet, viste til viktigheten av å jobbe med risiko i alle deler av virksomheten for å få en god risikostyring. Han kaller det helhetlig risikostyring. Han viser til at de jobber ut fra risikokriterier. Videre ga han eksempel at ved risiko ved hendelser opp mot mennesker er kriteriene lave og ved risiko opp mot økonomi er kriteriene høye. Et risikoakseptkriterie skal angi et område som er slik at dersom den beregnede risikoen er innenfor dette området vurderes det som uakseptabelt og tiltak må utføres for å redusere risikoen (Aven 2009).

I boka til Aven risikostyring (2009) kan en lese at risikostyring tradisjonelt blir gjennomført som en styringsprosess, der en kartlegger situasjonene og problemformulering. Dernest må en sette noen mål opp mot økonomi eller sikkerhet. Videre må en søke etter løsninger for å nå målet ved hjelp av analyse verktøyer får å se hva som bringer oss best opp mot de målene som er satt. Når vi har analysert og funnet de beste løsningene må en ta et valg og gjennomføre dette. Det er viktig å få tilbakemeldinger og evaluere etter prosessen slik at en kan ta med seg læring av prosessen (Aven, 2007). NVE har laget veilederen i sammen med Proactima som viser hvordan en kan komme i gang. I tillegg er den rettet spesifikk mot kraftbransjen. De viser til at dette vil være et ledelses verktøy for bedre måloppnåelse. Når det gjaldt nettselskapene var det ingen av disse to som brukte ROS analysen som et fullverdigverktøy, men begge ga utrykk for at de følger en form for tradisjonell styringsprosess. Difi var mer spesifikk om hva de ønsket å se av styringsverktøy og henviser til ISO standere. I tillegg viser de til Internforskriften. NSM mente at det best er at selskapene selv bestemmer hva som fungerer best bare en er innen for rammen til lovverket. Fordelene og ulempene med ROS analysen kommer frem i svarene til særlig myndighetene. NVE nevner spesielt fordelene med at en med en ROS analyse får kartlagt sannsynligheter og konsekvenser. Og at innen for informasjonssikkerhet så finnes det en del statistikk som kan hjelpe en i denne jobben. Utfordringene ligger i å kartlegge nye typer av angrep. NVE viser også til at bare med å utføre ROS analysen så vil en heve kompetansen og forståelsen til risiko og en får et bevisst forhold til hva en kan håndtere og hva en må overføre til beredskapsplanene. NVE viser til viktigheten av selve prosessen og læringen av utførelsen av arbeidet. Aven (2007) viser også til

dette med læring, altså evalueringen etter at analysen er utført og beslutningen er tatt. Det å vise til godheten i beslutningene som er komt ut av analysen. Et annet synspunkt som kom fram under intervjuet med Difi, som er viktig rundt dette med risikostyring. God begrepsforståelse i organisasjonene. Informanten tar opp dette med hva perspektiv en har til risiko, han viser til Aven (2007) at det finnes to typer av risikopersepsjon den økonomiske der en ser på kost nytte og perspektivet til en ingeniør der en ser på sannsynlighet x konsekvens. Mener at dette må komme tydeligere fram i analysene. Difi har en veiledning der det viser til Internkontroll forskriften for å bruke denne som en rettesnor for risikostyring. Alle informantene fra myndighetene var klare på at det er viktig å velge den risikoanalysen som egner seg til det en ønsker å analysere. I tillegg kommer det godt fram at struktur er viktig når en skal ha en god risikostyring.

5.1.3 Risikoanalyser

Som det kommer frem av teorien så er målet med en risikoanalyse å kartlegge og beskrive risiko, den skal gi oss et risikobilde. I boka Risikoanalyse til Aven at.al (2008) viser de til tre kategorier innen risikoanalyse, forenklet risikoanalyse, standard risikoanalyse og Modellbasert risikoanalyse. Under intervjuene med kraftselskapene kom det frem at det ble brukt forskjellig analyser, ingen av de som ble intervjuet utdypet dette noe mer. Nettselskapene viser til at det viktigste er barriere styring, dette er riktig men, det er viktig å huske på at det er med bakgrunn av analysene en utfører barriere styringen. Det vil si at om vi har en dårlig utført analyse vil heller ikke barriere styringen kunne sies å være den beste, i verstefall vil den ikke fungere som tenkt. Når det gjelder informasjonssikkerhet så kan en nesten daglig lese i aviser og se på nyheter at det stadig dukker opp brister og mangler, akkurat rundt dette med barrierene som er satt opp mot informasjonssikkerhet. Det gjør det enda viktigere å finne den gode analysen som passer til akkurat det en ønsker å se på. Aven at.al (2008) viser til 4 suksess faktorer for å ha en god analyse. 1 målet er å få beslutningsstøtte, 2 mer enn sannsynligheter og forventningsverdier dette var også begge kraftselskapene inne på når de snakket om risikoanalyser og risikostyring det er dette Aven at.al (2008) etterlyser, at en kan reflektere over usikkerhetsdimensjonene og styrbarheten. 3. Det er både styrker og svakheter rundt en risikoanalyse. Styrken er at analysen systematiserer tilgjengelig kunnskap og de usikkerheten en har i forhold til fenomener og systemer. Svakheter som

en risikoanalyse kan ha er dårlig kvalitet, dårlige begrepsdefinisjoner i tillegg kan det være dårlig kvalitet eller brister i risikomatrisene. Når det gjelder risiko opp mot Sikring/security så ser en at det er en del forskjellige begrepsforklaringer. Dette kan være en utfordring, det er viktig å finne likhetene mellom begrepene som er brukt opp mot sikring/security som også brukes opp mot sikkerhet/sefety. 4. En må være reflektert over metoden ikke falle for den samme metoden og modellen som en tidligere har brukt. Da NVE fikk spørsmålet viste informanten til tre faktorer modellen til NSM, som er en analyse en kan benytte opp mot informasjonssikkerhet, men ingen av de jeg intervjuet fra nettselskapene hadde kjennskap til denne. Det betyr ikke at den ikke blir brukt i selskapet. Hikstad at.al (2012) viser til at det er viktig med risikoanalyser opp mot informasjonssikkerhet, i boka går det fram at en kan godt benytte seg av stander risikoanalyser, men en må være bevisste på at dette ikke bare blir et IKT problem. Det kommer fram av boken at når en starter opp med en analyse så må en ta med seg alle som kjenner og bruker, og helst som det står i boken ta med de som ikke er så flinke til å bruke systemene. Hikstad at.al (2012) legger stor vekt på den menneskelige siden, vi gjør feil, vi bruker systemene feil. Hikstad at.al (2012) viser til at det har vært hendelser der maskinvarer har vært infisert men bruker av maskinen eller programmet har ikke vært klar over at maskinene er infisert. En tror bare at det er normalt at maskinen jobber noe seint. Aven at.al (2008) viser også til at i identifiseringsfasen av mulige trusler eller initierende hendelser så er det viktig at denne ikke blir rutinemessig. Mange har standardiserte lister som en benytter og en kan da komme i fare for å ikke se nye trusler og farer. Aven at.al (2008) legger vekt på at det er viktig med personer med nødvendig kompetanse i denne fasen.

I ROS analysen så har en ofte med seg en Bow tie og denne kan videre brekkes opp i analyser som for eksempel inn i feiltre og hendelse tre analyser, dette kan være analyser som passer bra for informasjonssikkerhet og i boken til Hikstad at.al (2012) henviser han til at denne type risikoanalyser kan brukes i noen tilfeller.

NSMs veileder for risikovurdering for tilsiktede hendelser. Er en veileder som tar oss gjennom tre faktorer modellen. En ser på styrkeforholdet mellom verdier, trusler og sårbarheter. Dette brukes for å beskrive den aktuelle risikoen. Denne håndboken beskriver hvordan risikovurderinger av tilsiktede uønskede hendelser kan planlegges, gjennomføres og dokumenters. Denne modellen er ikke så annerledes som en gjerne

tror og kan godt utføres i virksomheter som i nettselskaper. Den blir anbefalt av både NVE og NSM i intervjuene.

Oppsummering av forskningsspørsmål:

Avslutter med en liten oppsummering av forskningsspørsmålet. Det kan se ut som nettselskapene som ble intervjuet og myndighetene (NVE, NSM og Difi) er bevisste på dette med risikopersepsjon. Men det kan se ut som det er mangler når det gjelder kunnskap rundt dette med informasjonssikkerhet/securiy. For nettselskapene som vil gi noen utfordringer opp mot risikostyringsvertøyene. Det kan vise seg at en trenger noen begrepsavklaringer i bransjen slik at en forstår hva en snakker om til enhver tid. Som risikovurdering, i følge Aven at.al (2008) er dette resultatet av risikoanalyse og risikoevaluering. En kan ikke gjøre en risikovurdering før en risikoanalyse. Ledelsen må også skaffe seg mer innsyn i dette som går på informasjonssikkerhet/ security for å bedre kunne si, en har en ledelsesforankring. Vanskelig å implementere informasjonssikkerhet inn i risikostyringen om ledelsen ikke ser på dette som noe som kan true leveransen eller som en del av styringen av risiko for hele virksomheten. Ved bruk av risikoanalyser er det viktig å tenke gjennom hvordan en ønsker å presentere analysen, en må være oppmerksom på brister i riskomatriser som kan gi et feilaktig bilde over risikoen som fremstilles. En må kunne være i stand til å reflektere over usikkerhetsdimensjonene, og ha gode begrepsdefinisjoner i analysen.

5.2 Hvordan kan en redusere sårbarheten i kraftforsyningssektoren.

5.2.1 Sårbarhet

I teorien er ofte sårbarhet innbakt i risikobegrepet. Der en viser til at sårbarhet oppfattes som kombinasjoner av mulige konsekvenser og usikkerhet, gitt at systemet utsettes for en initierende hendelse (Aven, 2007). Sårbarhetsutvalget (NOU 2000:24) definerer sårbarhet som et uttrykk for de problemer et system vil få med å fungere når det utsettes for en hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet.

I Håndboken risikovurdering (NSM, 2016) for sikring som baserer seg på NS 5832 finner vi sårbarhetsvurdering, denne skal vise eventuelle gap mellom innførte sikringstiltak og en trussel aktørs intensjon og kapasitet. Får å kunne gjøre denne

vurderingen kan en om en følger NS 5832 etter hvert scenario se på eksisterende sikrings tiltak. Hvor godt de virker, er de dekkende nok? En deler sårbarhet og sikrings tiltak opp i tre hovedkategorier. Organisatoriske som tar for seg dokumentasjon og styring. Menneskelige som tar for seg personellsikkerhet og den menneskelige delen av systemene. Teknologiske som IKT sikkerhet og fysisk sikkerhet. I veilederen til NSM er det listet opp 16 eksempler på sårbarheter en kan finne i den organisatoriske delen. noen av eksemplene er vilje til å avsette nok ressurser til sikkerhet, ledere bør måles på hvor godt de ivaretar sikkerheten, manglede systemer for avvik og hendelseshåndtering og manglede øving av beredskapsplaner (NSM Håndbok Risikovurdering for sikring 2016). NVEs informant er inne på dette under intervjuet at rest risikoen må legges inn i beredskapsplanen dette gjelder også innen for informasjonssikkerhet. Av eksempler å trekke fram fra den menneskelige delen av sårbarheter er å være oppmerksomme på svak forståelse blant medarbeidere om hvorfor sikkerhet er viktig for virksomheten. Informantene fra nettselskapene var inne på at de hadde retningslinjer for medarbeiderne og at noen stillinger var det nødvendig med vandels attest. Slik jeg tolker dataene fra informantene i denne oppgaven vil jeg tro at det vil være et forbedrings potensiale i dette, undersøkelsen til Hagen (2009) der hun ser på dette med avviksrapportering viser at det er liten forståelse blant de fleste om at dette med sikkerhet opp mot informasjonssikkerhet. I tillegg så er liten kunnskap rundt emnet sikring/security og det gjør også at det er vanskeligere for medarbeidere å se farene rundt dette med informasjonssikkerhet. Inn i dette kommer også manglende evne til å rapportere avvik innen sikkerhet opp mot informasjonssikkerhet. Nå hadde begge selskapene avviksrapporterings systemer som ville fange opp brudd på informasjonssikkerhet men det var størst fokus på avvik opp mot sikkerhet på safety siden.

På de teknologiske sårbarhetene vil jeg trekke fram 1 av totalt 12 sårbarheter. manglede oppgradering av program og maskinvare. Dette utføres ofte av bruker av maskinen om en ikke har lagt inn rutiner at alle maskiner tilhørende avdeling eller virksomhet skal oppgraderes for eksempel gjennom natten. Det svake ledet er om en ikke oppdaterer eller utsetter oppdateringen kan det gå i glemmeboken og en får svakheter ved systemet. Det må være gode rutiner og en må gjøres oppmerksom på at en følger oppdateringen og får de nyeste versjonene av maskinvaren.

5.2.2 Lovverk

Det er mye lovverk som regulerer virksomhetene i Norge, når det gjelder kraftbransjen så reguleres den opp mot informasjonssikkerhet av beredskapsforskriften. Forskriften forebyggende sikkerhet og beredskap i energiforsyningen kalt beredskapsforskriften. Beredskapsforskriften har som formål å sikre at energiforsyning opprettholdes og at en kan normalisere forsyningen så raskt som mulig og at produksjon kan gjenopptas § 1-1. Dette for å redusere samfunnsmessige konsekvenser (DSB, 2016) I Norge er alle virksomheter offentlige og private pålagte til å følge internkontroll forskriften. Difi henviser til denne under intervjuet og visert til at ved å følge denne forskriften så vil en få dekket inn de områdene som inngår i risikostyring og dermed vil en redusere sårbarheten. I boka til Engen at.al (2016) kan en også lese om internkontroll systemet og at alle offentlige og private sektorer er underlagt å ha et system for helse, miljø og sikkerhet. Et annet tiltak er å kjøre sårbarhetsanalyser eller ROS. Dette anbefaler NVE og har utarbeidet en god veiledning for ROS analyse. Nettselskaper er pålagt å kjøre risiko og sårbarhetsanalyser, oppdatere beredskapsplaner og øve regelmessig gjennom forskriften forebyggende sikkerhet og beredskap (DSB, 2016) i tillegg er også selskapene pålagte å gjennomføre forebyggende sikkerhetstiltak ved alle anlegg og objekter av betydning for forsyningssikkerheten og ha tilgang på nødvendige ressurser og kompetanse for rask gjenoppretting ved skader og havari. Forskriften har en rekke krav til sikring av anlegg avhengig av klassifisering og beredskap rundt kritiske IKT systemer (DSB, 2016). Det er viktig at motivasjonen til gode risikoanalyser eller god risikostyring bør ligge i å kunne ta gode beslutninger ikke i at det er lovpålagt. Informant fra nettselskap 1 er inne på at ledelsen har blitt mer opptatt av informasjonssikkerhet etter de nye EU direktivet som regulerer dette med personsikkerhet og at det er en god pisk i store bøter.

5.2.3 Trening og øvelser

Selskap 1 og 2 var klare på at det ble gjennomført øvelser opp mot informasjonssikkerhet i selskapene og av dette er med å redusere sårbarheten. I modellen for samfunnssikkerhet til Schiefloe (2012) så inngår begrensning av skade og gjenopprette normal tilstand. Dette kjenner en igjen fra beredskaps planlegging og beredskapsanalyse. Det er viktig å ha en evne til å reduser virkningene av hendelsen som en ikke har klart å forhindre. En må opparbeide en evne til å redusere virkningene ved å etablere barrierer både menneskelige at en evner å oppdage at noe er feil,

teknologiske systemene fungerer og oppdager feil (Schiefloe, 2012). Nettselskapene har et godt hjelpe middel i kraftCERT. Det vil likevel være viktig å ha øyne og ører åpne, selv også. En kan ikke setter all sin litt til at en vil bli informert om forhold som kan komme til å skade virksomheten. For kraftbransjen så vil dette være strøm ut til kundene. På det organisatoriske plan er det viktig at rutiner, prosedyrer og retningslinjer er oppdaterte og fungerer til sitt formål. Ledelsen må være inne forstått med at sikkerheten for hele virksomheten innebefatter sikkerhet både opp mot sikkerhet/sefety og sikring/security (Schiefloe, 2012). Det å gjenopprette normaltilstanden er viktig når en hendelse har funnet sted. Dette gjelder fysiske, medisinske, sosiale og psykiske dimensjoner. Det som er like så viktig etter en hendelse har inntruffet er å lære av denne. Dette krever at det blir utført grundige analyser i etter tiden av en hendelse. Disse må brukes til å se etter ny kunnskap slik at en kan i større grad bli mer robuste i håndteringen av selve hendelsen.

Selskap 1 uttaler blant annet at det er viktig at en ikke kommer i den situasjonen at det er bukken som passer havresekken. Når det kommer til øvelser så kan det være lønnsomt å innhente eksterne selskaper for å kjøre øvelser. Det som er viktig er at øvelsene har en relevans, god planlegging og et gode mål for hva enn ønsker å øve på. På dette viset vil kompetansen øke og en får en bedre håndterings evne.

Oppsummering av forskningsspørsmål:

Det kan se ut som at etterlevelsen av lovverket er tilstede i nettselskapene. Det som kan vise seg er dette med viktigheten i å få alle i virksomheten til å få nok kunnskaper om sårbarheter opp mot informasjonssikkerhet. En kan nok få redusert en del av sårbarhetene ved å ha et like stort fokus på informasjonssikkerhet som ved fare for fall og det å bruke riktig verneutstyr. Om en i tillegg klarer å ha øvelser og trening opp mot informasjonssikkerhets hendelser kan en også få kartlagt hvor sårbarhetene ligger.

5.3 Hvor viktig er det at ledelsen er involvert og forstår risikobilde

Det kom godt fram under intervjuene at også dette er viktig for nettselskapene. Får en ikke ledelsen med, vil det heller ikke investert i sikkerhetstiltak som går på sikring/security eller informasjonssikkerhet. I forbindelse med informasjonssikkerhet er det gjerne viktig at ledelsen setter seg inn i problematikken. I det siste så har det kommet opp mange avisreportasjer som den i Dagens Næringsliv fra mai 2017 om store

brister når det gjelder informasjonssikkerhet, det har vært ganske normalt å outsorser deler av IT til blant annet land som India og andre land. Dette har en hatt forskjellige erfaringer med fra gode til heller dårlige. Det trenger i utgangspunktet ikke være negativt å outsorse deler av IT. Det ledelsen må være sikre på, er at denne beslutningen bli tatt på informasjon og prediksjoner som er av en karakter at en ikke etter, ett eller noen år ser at en ikke har hatt kontroll på informasjonssikkerheten. Aven at.al (2008) viser til noen gode ledelses og styringsprinsipper, en må se på beslutningene innen risiko og sikkerhetsledelse som viktige for å nå målene for virksomheten. Et annet viktig element er å følge opp beslutningene og hvem som gjør dette. Difis rapport styringssystemer for informasjonssikkerhet, erfaringer og anbefalinger (2012) kommer det godt fram at skal en lykkes i informasjonssikkerhets styring, så må dette være forankret i ledelsen. Det kommer fram av rapporten at styringskompetanse hos lederne og hos nøkkelpersonell i virksomhetene, er sentralt når det kommer til den faktiske ledelsesforankringen av styringssystemet for informasjonssikkerhet. Det kan se ut fra denne rapporten at det er en sammenheng mellom implementeringstilnærmingen for styringssystemer, og virksomhetenes evne til å få styringsdelen til å fungere. Det som også kom fram i Rapporten styringssystemer for informasjonssikkerhet (2012) at toppstyrt innføring ofte er det som gir mest innretning mot en helhetlig styrings og kvalitetssystem. Det viste seg at når initiativene kommer nedenfra i organisasjonene, får en egne selvstendige styringssystemer for informasjonssikkerhet men da med svakere forankring hos ledelsen og i virksomheten. Rapporten viser også til at ledere i stor grad prioriterer de aktiviteter som de blir målt på. For å få den nødvendige ledelsesprioriteringen for arbeid med styring av informasjonssikkerhet, er det klare signaler fra revisjons og tilsynsmyndigheter og virksomheter om at toppledere bør måles på også dette i følge rapporten til Difi.

Oppsummering av forskningsspørsmål:

Vil oppsummere med at det som kommer godt fram under dette spørsmålet. Er viktigheten av ledelsens kompetanse og involvering er viktig for virksomhetens evne til å ha en god risikostyring.

5.4 Hvordan bedre informasjonssikkerhet i bransjen

For å komme fram til dette svaret har jeg delt inn dette kapittelet i noen under overskrifter og vil prøve å komme meg frem til et svar basert på teori og det som jeg kan tolke ut fra svarene som kom frem under intervjuene med kraftselskapene og fra NVE, NSM og Difi.

5.4.1 Sikkerhet

Som det kommer fram i teori kapittelet så er det mange definisjoner på sikkerhet. I denne oppgaven er fokuset på informasjonssikkerhet opp mot kraftbransjen. Dette er en bransje som er en del av den kritiske infrastrukturen i Norge.

Det som kommer fram er at balansen mellom produksjon og sikkerhet er viktig, i den forstand at det er bare etter ulykker eller alvorlige nesten ulykker at sikkerheten står fremst i bevisstheten blant ledere i organisasjonene (Reason, 1997). Gjennom denne oppgaven så har jeg vært særlig oppmerksom på avisartikler rundt, og om dette emnet informasjonssikkerhet. Dagens Næringsliv skrev 26.mai i år om cyberanagrep etter at flere land var utsatt for angrepet som ble kalt WannaCry. Det er naturlig at alle organisasjoner er opptatt av produksjon og det å skape verdier, og det er nok mest naturlige at de fleste vil få mer opplæring rundt produksjonen en sikkerhet når en starter som nyansatt. Dette gjelde de fleste organisasjoner. Når en snakker om sikkerhet så er det alltid et spørsmål om hvordan en fordeler ressursene og investeringslysten opp mot sikkerhet. Reasen (1997) snakker om Protection der målet er sikkerhet for mennesker og materiell. Han deler Defence inn i Hard Defences og Soft Defences. Når det gjelder informasjonssikkerhet så er det viktig at IKT systemene har de sikkerhetsinnretningene som kreves og gode fysiske barrierer. Dette har de fleste nye systemer på plass. Men det er viktig å huske på at dette er også systemer som er laget av mennesker og det kan være feil og svakheter i alle systemer (Hikstad, at.al, 2012). Det finnes lovgivning opp mot informasjonssikkerhet og sikkerhetsloven ligger til revisjon og skal opp i Storting. I intervjuet med NVE så gir informanten meg en forståelse av at forandringene i sikkerhetsloven vil føre til forandringer for NVE. Det samme kom fram i intervjuet med NSM. Ofte trenger en lovgivning for å få til endringer som øker sikkerheten. Dette har en sett i mange bransjer blant annet i offshore næringen. I tillegg til lovgivning så trengs det også en bevisstgjøring rundt dette med at sikkerhet deles inn i to, en må se på

sikkerhet opp mot uønskede hendelser som skapt av naturkrefter og uønskede hendelser som er tilsiktede. Det vil si at det må utarbeides gode kontroller og regler og prosedyrer internt i hver organisasjon. Det må utarbeides beredskapsplanverk som ikke bare dekker de mest kjente hendelsene for kraftbransjen som naturkrefter kan forårsake men også opp mot informasjonssikkerhet. Dette må også trenes og øves på. Schiefloe (2012) har utarbeidet en modell for samfunnssikkerhet som viser til fem punkter som må være tilstede for å ha god organisatorisk sikkerhet over tid. Organisasjonene må være pålitelig, ha gode rutiner. Under intervjuene med kraftselskapene kom det fram at det var etablerte rutiner rundt dette med informasjonssikkerhet i forhold til retningslinjer opp mot hva ansatte kan laste ned av programmer og hva ansatte kan gjøre. En må være sensitiv for faresignaler en må ha en kultur i organisasjonen som klarer å fange opp disse. For å ha denne sensitiviteten trenger en gode prosedyrer, rutiner og praksis. En må være proaktiv det må være en handlingsdyktighet som krever kompetanse, rutiner og reaksjonsevne. Det må være en evne til improvisasjon (Schiefloe, 2012). Denne er det godt mulig at det mangler i dag men selskapene som ble intervjuet var bevisste på at det manglet kunnskaper rundt emnet informasjonssikkerhet og var begge i en prosess der en oppbemannet innen dette emnet. I tillegg til å være proaktiv må en også kunne være reaktiv, være i stand til å håndtere hendelsene når de inntreffer. Det vil si at en må ha en beredskapsplan for informasjonssikkerhets hendelser. I tillegg må det være en evne til å lære av hendelsene og bruke dette som grunnlag for formell og uformell erfaringsoverføring (Schiefloe, 2012, Reason, 1997).

5.4.2 Informasjonssikkerhet

I følge Difis rapport styringssystem for informasjonssikkerhet, erfaringer og anbefalinger (2012). Handler Informasjonssikkerhet om å sikre konfidensialitet, integritet og tilgjengelighet på informasjon som trenger sikring. Det vil si at virksomheten må avgjøre hvilken informasjon dette gjelder på bakgrunn av virksomhetens mål, arbeidsprosesser og bestemmelser i lover og forskrifter.

Når det kommer til informasjonssikkerhet så må en ta innover seg dette med ondsinnede handlinger selv om det kan oppstå feil og hendelser som kan inntreffe IKT systemene. Hikstad at.al (2012) tar opp dette med viktigheten av at informasjonssikkerhet ikke bare er et teknisk problem men at det er viktig å huske at IKT systemene brukes av personer og organisasjonene som er rundt systemet. Når en intervjuet kraftselskapene så var de

begge innforstått med at innen dette så var de klar over at kunnskapsnivået kunne vært bedre. Begge selskapene var i prosesser der de oppbemannet og hadde styrket kunnskapen. Det som også kom fram gjennom intervjuene var at informasjonssikkerhet var underlagt IKT eller IT avdeling. I NOU 2015:19, NOU 1016:24 og NOU 2006:24) viser alle til at IKT er ikke bare et IT anliggende. Hikstad at.al (2012) viser til at det er tre hoved grupper når det gjelder IKT trusler som en må være klar over. Første trussel er utilsiktede hendelser dette er hendelser som går på at en har uheldige ansatte som ved uhel gjør feil som fører til at en får virus inn i systemene. Dette er ikke uvanlig og de fleste organisasjoner har opplevd dette. Det som kommer fram i Hikstad at.al (2012) er at for å unngå dette er det viktig å tenke gjennom de tekniske og menneskelige sidene av IKT. Kan en gjøre systemene mer robuste med å sørge for redundans. På den menneskelige siden kan en sørge for god kompetanse på hvordan en bruker systemene. Hikstad at al (2012) advarer mot nøkkelpersoner for dette kan utgjøre en sårbarhet. Når det gjelder trussel nr. 2 generelle angrep så snakker vi om angrep som ikke er rettet mot et spesielt IKT system. Eksempler på dette er ondsinnede software som finnes på internett. Selv om disse ikke er linket til et spesielt system kan de gjøre stor skade. I følge Hikstad at al (2012) gir det høy risiko når ansatte surfer på internett fra systemer som har kritiske funksjoner. Trussel nr.3 i følge Hikstad at al (2012) er direkte angrep disse er rettet mot et spesielt system eller selskap. De er laget for å skade systemet eller organisasjonen. Vi snakker da om angrep som kan være fysiske som innbrudd, vandalisme og angrep via internett. Kraftselskapene som ble intervjuet i denne oppgaven kunne fortelle om at det var en del kontroller som til dels vil kunne dekke opp noen av disse angrepene. Det er adgangskontroll i de fleste virksomheter etter hvert slik at en unngår uvedkommende å komme seg inn, en er til linket ett alarm system for å unngå innbrudd. Problemene er alle trafostasjoner og ikke minst det å sørge for at en har gode nok rutiner slik at en ikke får for mange hendelser av typer direktør svindel eller av feil som ved wannacry som kryptere innholdet på maskinene og ønsker løsepenger (bitcoin) for å av kryptere innholdet. Ved starten av 90 tallet i olje industrien så var det fokus på sikkerhet men ikke slik vi kjenner det i dag. En må opparbeide seg en kompetanse og ikke minst en må tørre å tenke tanken at dette kan ramme oss og hva blir da konsekvensene, og starte det forebyggende arbeidet for å få en god sikkerhet opp mot informasjonssikkerhet.

5.4.3 Kunnskaper

Når det gjelder kunnskap så kom det godt frem av de som ble intervjuet at det er en mangel på kunnskaper innen emnet informasjonssikkerhet og sikring/security tenkning. Dette var gjerne ikke så overraskende. Det viser at myndigheter og virksomheter har et ansvar når det gjelder å få den nødvendige kompetansen som trengs, også innen dette området. Samtlige av informantene svarte at det var mangel på kunnskap rundt emnet sikring/security. Nå skal det sies at det er begynt et arbeid for å øke kunnskapen rundt dette emnet. En ny sikkerhetslov er på trappene og det blir spennende å se hva som vil komme ut av denne. Som alltid rundt ny lovgivning er det de som ser fordelene og ulempene med lovverket. NSM vil slik den fremstår i NOU samhandling for sikkerhet 2017 til å få et større ansvar for sikkerheten som innbefatter securety/security. Tilsynsordninger kan se ut som den vil dekke en større del av virksomhetene dette kommer fram i spørsmålene som ble stilt til informantene der NSM tror at loven vil få mye å si i fremtiden. Loven vil bli mer funksjonell og det betyr at aktørene må finne sine egne løsninger. Dette kan være positivt med at virksomheter i større grad må ta et eieransvar opp mot sikkerhet på sikring/security siden. Det vil si at NVE vil på sikt gjerne måtte stille mer krav til selskapene som de er tilsynsmyndigheter til. Difi er mer skeptisk til ny lovgivning men dette går mer på at de ser en del farer med å skjule all informasjon for offentligheten. De er absolutt enige i at noe må skjules. De mener at det som skal skjules for offentligheten skal vurderes strengt. Difi viser til internkontroll forskriften og om denne følges på en god måte så er mye på plass. Begge selskapene som ble intervjuet ga uttrykk for at de jobbet med å øke kompetansen innen dette området. Nå er det viktig også å klare å bruke den kompetansen som finnes i organisasjonen innen risiko, sårbarhet og sikkerhet en trenger ikke begynne helt på nytt for å få kompetanse. I rapporten til Difi styringssystemer for informasjonssikkerhet, erfaringer og anbefalinger (2012) viser de til at styringskompetanse er en utfordring. Videre viser de til at det er en utfordring med risikostyring. Rapporten peker på at skal en få kontroll må sikringstiltak henge sammen med risikovurderinger. Det er flere likheter mellom sikkerhet/safety og sikring/security og forskjellene er ikke så store som en tror. Særegenheter ved sikringsfaget er usikkerheten og denne viser til hvem, hva og hvordan vil et angrep skje. En ulikhet er at i Security snakker en om en angriper som er strategisk. Den vil kunne finne de berømte hullene i Reasons barriere modell. Det er også verd å ta med seg at sikringsfaget er mer en terror, som det ofte blir forstått som. Men sikringsfaget tar for seg alt fra kriminalitet, sabotasje, terror, sikkerhetspoliske kriser, cyberangrep, atom, biologisk og kjemiske angrep og spionasje.

Angrepene blir drevet av motivasjoner som kan være økonomisk vinning, politisk, berømmelse og status.

5.4.1 Sikkerhetskultur

Personlig så har jeg jobbet en del år innen offshore bransjen og ordet sikkerhetskultur er velkjent. I mange år har det vært fokus på å jobbe fram en kultur som involverer alle til å tenke sikkerhet om en jobber i produksjon eller ledelse. Det har vært kampanjer som har vært gode, og det har vært kampanjer for å øke sikkerheten som har vært feilslåtte. Det har blitt jobbet lenge med dette i offshore bransjen og en kan gjerne si at inne offshore næringen så har en god sikkerhetskultur. Til nå har jeg ikke opplevd at det er blir satt noe nevneverdig fokus på å forbedre sikkerhetskulturen til å gjelde sikkerhet opp mot tilsiktede uønskede hendelser i samme grad og intensitet som opp mot uønskede hendelser. Heller ikke offshore. Det kommer også fram at det kan være slik i kraft bransjen. Informantene fra kraftselskapene gir uttrykk for at det er få holdningskampanjer som settes ut i livet fra selskapet rettet mot akkurat informasjonssikkerhet. Myndighetene kan også formidle at kompetansen og bevisstheten rundt dette emnet kunne med fordel vært høyere. I følge Turner og Pidgon (1997) så ser de på sikkerhetskultur som den måten en velger å se verden på. dette er viktig når det gjelder informasjonssikkerhet. Informasjonssikkerhet omhandler mye om feil og mangler i selve systemene som skal forhindres og oppdages, men vi snakker også mye om ondsinnede hendelser. Om en velger å se verden på den måten at det ikke rammer oss, eller at de ansatte vil oppdage det om en blir utsatt for ondsinnede hendelser så kan en komme til å få det som Turner og Pidgon (1997) mener er en kultur som skaper blindhet for farer og trusler. Det er dette han mener når han snakker om inkubasjon. Og det er dette som kan føre til alvorlige hendelser eller i verstefall katastrofer. Turner og Pidgon (1997) viser til organisasjonenes sårbarhet når det gjelder kultur og i rapporten til terrorangrepene 22 juli 2011 i Oslo og på Utøya blir dette med kultur trukket fram som en av forklaringene på den dårlige håndteringen. Det som kan synes å være vanskelig å se er om kulturen er et premiss for systemets sårbarhet og kan øke risikoen for ulykker eller om den er en del av løsningen (Engen, at.al 2016).

I følge teorien til Reason (1997) må en har fem sentrale kjennetegn til stede. 1. *En organisasjon som innhenter data om eventuelle ulykker men også nesten ulykker*. Det fremkommer av intervjuene av kraftselskapene at de har et rapporterings system for

hendelser som er tilsiktet og det er bra. Men forskning viser også at det er en stor underrapportering bla Hagen (2009) der det kommer fram at mange unnlater å rapportere hendelser rettet opp mot informasjonssikkerhet. Hagen (2009) fant et gap mellom hva som var forventet og hva som var av holdninger til sikkerhet. I tillegg så kan det vært vanskelig å rapportere om hendelser om en ikke er klar over at du er rammet av en hendelse. 2. *De ansatt må stimuleres til å rapportere hendelser og nesten hendelser*. For å få opp rapporteringen så hjelper det om ledelsen er involvert og, det blir tatt alvorlig. Det må også gis tilbakemelding da vil en få en økning av innrapporteringen. Det er da viktig at en har en forståelse fra bunn til topp om hvor viktig informasjonssikkerhet er for virksomheten. En må ikke komme i en setting der en gjør personer som rapporterer om feil og mangler til syndebukker. 3. *Fleksibel kultur der organisasjonen lærer av de rapporterende hendelsen*. Dette er viktig, rapporteres det om feil og dette ikke rettes opp i, ser en gjerne ikke hensikten med å rapportere inn andre eller flere hendelser.

I undersøkelsen til Hagen (2009) fant hun noen barrierer som må overstiges for å få en god sikkerhetskultur opp mot informasjonssikkerhet/Security hendelser. Hun fant at det ble ikke innrapportert, det er liten kunnskap om sikring/security og en er ikke i stand til å kjenne igjen et brudd på sikring/security. Dette kommer også fram i boken til Hikstad at.al (2012) der han viser til at vi som mennesker ikke alltid forstår at vi er utsatt for ondsinnede handlinger. De ansatte kan ser på dette med å innrapportere som angiveri, Reason (1997) sier jo noe om at det må være åpenhet rundt dette og en må få til en kultur der en ser på hendelsen uavhengig av den personen som er i den skarpe enden. Det kom også fram fra Hagen (2009) at mange ser på dette med informasjonssikkerhet/ security som at det ikke er deres ansvar. At det som går på Security/informasjonssikkerhet er noe som tilhører IKT/IT avdelingen. Tenker at om en ønsker en kultur opp mot sikring/security og spesielt opp mot informasjonssikkerhet så er det viktig å starte med å se på informasjonssikkerhet ikke bare opp mot systemene, de blir laget så gode som de kan bli, men en må ta innover seg det menneskelige perspektivet.

6 Konklusjon

I denne oppgaven har en prøvd å besvare følgende problemstilling – *hvordan kan en ved hjelp av risikostyringsverktøy redusere sårbarheter og heve sikkerheten for informasjonssikkerhet i kraftbransjen?*

Til dette ble det benyttet forskningsspørsmål som jeg håpet ville gi meg noen svar.

Svarene er ikke entydige, i følge min oppgave kan en ikke peke på et verktøy og si at dette er oppskriften på suksess.

Det som jeg vil trekke fram i denne konklusjonen er følgende:

Risikoanalyser: Som det kommer fram i oppgaven er det flere måter å utføre en risikoanalyse. Det er viktig å finne den analysen som passer til det en ønsker å analysere. Nettselskapene kan forbedre sikkerheten ved å være mer flinke til å ha god planlegging, struktur og refleksjoner over hva typer analyser som passer til formålet. Det å skaffe seg kunnskaper om dette med risikoanalyser om tilsiktede uønskede hendelser, som å eventuelt å ta i bruk trefaktor modellen til NSM.

Risikobilde: Det kommer fram i oppgaven både gjennom teori og intervjuer at det er viktig å klare å presentere et godt risikobilde. Det er viktig at ledelsen forstår bilde av risikoen som presenteres. På den måten får en satt i gang med de sikkerhetstiltak som er nødvendige for å ha en god informasjonssikkerhet.

Risikostyring: For å ha en god drift av en virksomhet så trenger en god styring, dette gjelder også opp mot risikostyring. En må tilstrebe å få med alle risikoer for å kunne styre disse. Da må også sikring/security problematikken inn i prosessen for å fremme en god risikostyring. For å kunne ha god risikostyring, trengs det gode retningslinjer og prosedyrer som er rettet opp mot informasjonssikkerhet. Det finnes mange hjelpemidder for å få til et godt styringssystem som det har komt fram i denne oppgaven.

Kunnskap: Det kommer tydelig fram at det er en mangel på kunnskap opp mot sikring/security. Nå var det bare to selskaper som ble intervjuet i denne oppgaven, men ut fra tolkning fra myndighetene (NVE, NSM og Difi). Kan det se ut som at det er en mangel på kunnskap rundt dette med sikring/security generelt. Sikring/security dimensjonen av sikkerhet må trekkes inn i informasjonssikkerhet. Myndighetene både

NVE, NSM jobber med å bringe ut kunnskap men, selskapene må også i større grad søke etter ny kunnskap. Informasjonssikkerhet kan med fordel trekkes ut fra IT avdelingene, og alle i virksomheten må få kunnskap om hva dette handler om. Det kan godt leies inn kompetanse i noen tilfeller, men det er selskapet som må sitte med eierskapet. Det er vanskelig å sitte med dette eierskapet om en ikke har noen form for kunnskap rundt dette emnet.

Sikringskultur: Dette er det jeg vil kalle ett kjerne funn i oppgaven. Det var ikke dette som var målet mitt med oppgaven, heller ikke det som jeg trodde ville stikke seg ut. Etter empiri kapittelet så jeg et mønster av dette med kultur. Det kommer klart fram i intervju både med nettselskapene, myndighetene og det som ble innhentet fra veiledere og rapporter. Det savnes en sikringskultur. For å få en god risikostyring må det jobbes fram en sikringskultur i virksomheten, på lik linje som en har opp mot sikkerhet for uønskede hendelser (safety). Dette er en jobb det med all sannsynlighet vil ta en del år å få til, derfor er det viktig at dette blir påbegynt. Det vil være vanskelig å få en god struktur på noe, en ikke har liggende i ryggen at det må være struktur rundt. Min erfaring fra tidligere er offshore bransjen og for å ha en god sikkerhetskultur må den jobbes med daglig. Kulturen må ligge som en refleks i alle ledd i virksomheten fra topp til bunn. Det må startes et arbeid med å få til en sikringskultur på lik linje som vi har innen sikkerhetskultur. Hvordan dette kan gjøres og hvordan en kan bruke synergier fra sikkerhetskultur arbeidet inn i denne sikringskulturen hadde vært spennende å se på i en annen oppgave og jeg håper at noen tar den stafett pinnen.

Den endelige konklusjonen på denne oppgaven er da følgende:

For å få til få til en god bruk av risikostyringsverktøy for å redusere sårbarheten og heve sikkerheten for informasjonssikkerhet i kraftbransjen? Må en jobbe for å få en sikringskultur, som gjør det mulig å se potensialet i de verktøyene som finnes. En må jobbe fram en sikringskultur på lik linje som en har jobbet for å få sikkerhetskultur. En vil da gjerne være nærmere en god risikostyring.

7 Referanser

Andersen, S. S (2006). *Aktiv informantintervjuing.* Norsk statsvitenskapelig tidsskrift, Vol. 22, 278-298, 2006.

Aven, T (2007) *Risikostyring. Grunnleggende prinsipper og ideer*. Oslo: Universitetsforlaget. Berlin/Heidelberg: Springer- Verlag. 2.opplag 2009

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

Aven, T., Renn, O. (2008). *Risk, Governance and society concept, guidelines and applications*

Aven, T., Røed, W., Wiencke, H, S (2008) *Risikoanslyse. Prinsipper og metoder, med anvendelser*. Oslo: Universitetsforlaget.

Beredskapsforskriften (2002) *Forskrift om beredskap i kraftforsyningen.* FOR- 2002-12-16-1606. Tilgjengelig fra:https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157 (nedlastet 1.juni 2017)

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

Bernstein, P. (1996) *Againast the Gods*. New York: John Wiley og Sons. Ltd.

Busmundrud, O. Maal, M. Hagness, J. K. Endregård, M. (2015): *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. FFI-rapport 2015/00923 https://www.ffi.no/no/Rapporter/15-00923.pdf

Dagens Næringsliv: Cyberangrep vi vil se mer av: Fredag 26.mai 2017 https://www.dn.no/meninger/2017/05/25/1947/Innlegg/cyberangrep-vi-vil-se-mer-av

Denzin, N.K., & Lincoln, Y.S (2005). *The Sage Handbook og Qualitativ Research (3rd ed.)* Thousand Oaks, CA: Sage

DSB, (2016) *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enver tid?* Direktoratet for samfunnssikkerhet og beredskap 2016

Direktoratet for forvaltning og IKT (2012:15) Styringssystemer for informasjonssikkerhet. Erfaringer med anbefalinger om standardene ISO 27001 og ISO 27002. ISSN 1890-6583, Direktoratet for forvaltning og IKT.

Direktoratet for forvaltning og IKT (2017) Veiledningsmateriellet. Internkontroll i praksis- informasjonssikkerhet. Grunnleggende innføring. Direktoratet for forvaltning og IKT

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

Hagen, J.M. (2009) *"The Human Factor behind the Security Perimeter: Evaluating the E ectiveness of Organizational Information Security Measures and Employees' Contribution to Security,"* PhD dissertation submitted to the University of Oslo for defense.

Hikstad, P., Utne, P.I., Vatn, J. (2012). *Risk and Interdependencies in critical infrastrukturs a guideline for analysis,* Springer – Verlang London

Jacobsen, D.I. (2005): *Hvordan gjennomføre undersøkelser? Innføring samfunnsvitenskapelig metode.* Oslo, Abstrakt forlag AS.

Nasjonal Sikkerhets Myndighet (2016) Veileder: Sikkerhetsstyring Nasjonal sikkerhetsmydighet.

Nasjonal Sikkerhets Myndighet (2016) Håndbok: Risikovurdering for sikring Nasjonal sikkerhetsmyndighte.

Norges Vassdrags og Energidirektorat (2012) beskyttelse av kritiske IKT- system i energiforsyningen. Muligheter og utfordringer i forlengelse av en CSIRT (Computer

Security Incident Response Team) som understøttelse av IKT- sikkerheten i energiforsyningen. Norges vassdrags- energidirektorat Rapport nr. 69. 2012.

Norges Vassdrags og Energidirektorat (2010) *Veiledning i risiko- og sårbarhetsanalyser for kraftforsyingen*. Norges vassdrags- og energiNOU 2000:24 *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Oslo: Justis- og beredskapsdepartementet.

Notat 10/12 Per Morten Schiefloe: *En modell for samfunnssikkerhet. 22.juli kommisjonens bakgrunnsnotater*, Tilgjengelig på: http://www.22.julikommisjonen.no/Bakgrunnsnotater/Materiale-fra-kommisjonens-moeter

NOU 2006:6 Når sikkerhet er viktigst. Beskyttelse av lnadets kritiske infrastrukturer og kritiske samfunnsfunksjoenr. Oslo: Justis- beredskapsdepatementet.

NOU 2012:14 *Rapport fra 22. Juli-kommisjonen*. Oslo: statsministerens kontor. https://www.regjeringen.no/contentassets/bb3dc76229c64735b4f6eb4dbfcdbfe8/no/pdfs/nou201220120014000dddpdfs.pdf. (Nedlastet oktober 2017)

NOU 2015: Digial sårbarhet-sikkert samfunn-beskytte enkeltmennesker og samfunn i en digitalisert verden. Oslo: justis- beredskapsdepartementet.

NOU 2016:19 Samhandling om sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskriftelig tid. Oslo: Justis- beredskapsdepartementet.

Internkontrollforskriften (1996) *Forskrift om systematisk helse-,miljø- og sikkerhetsarbeid i virksomheter* FOR-1996-12-06-1127 https://lovdata.no/dokument/SF/forskrift/1996-12-06-1127 (sist nedlastet oktober 2017)

Jore, S. H., Egeli, A. (2015). *Risk Management Methodology for Protecting Against Malicious Acts – Are Probabilities Adequate Means for Describing Terrorism and Other Security Risks?* European Safety and Reliability Conference (ESREL) 2015, Zurich Switzerland.

Reason, J. (1997). *Managing the risks of organiational accidents.* Alderhot, Storbritania: Ashgate.

Renn, O. (2008) *Risk Governance. Coping with Unertainty in a Complex World.*

London. Earthscan

Turner, B.A., & Pidgeon N.F. (1997). *Man-made Disasters.* Oxford: Butterworth Heineman

Turner, B.A. (1978). Man-made Disasters. London: wykeham Science Press.

8 Vedlegg

Vedlegg 1

Guide til spørsmål til master oppgave i Risikostyring og sikkerhetsledelse

Tema: informasjonssikkerhet i et samfunnsperspektiv.

Problemstilling:

Hvordan kan en ved hjelp av risikostyringsverktøy redusere sårbarheten, og heve sikkerheten for informasjonssikkerhet i kraftforsyningsbransjen.

1. Det finnes flere perspektiver og definisjoner på Risiko, hvordan vil du (NSM, NVE, Difi,) beskrive og forklare risiko på en enkel måte. (forventningsverdi?)

2. Er bransjen tradisjonelt kjent for å være flinke til å foreta risikovurderinger opp mot sikring/security? Hva er din oppfatning av forståelsen av risikovurderinger opp mot sikring/security i bransjen?

3. Hvordan vil den nye sikkerhetsloven få av betydning for bransjen? Kan du gi noen konkrete eksempler?

4. Hva er deres anbefaling for å styre risikoen for tilsiktede handlinger mot informasjonssikkerheter innen kraftforsyningssektoren?

5. Hvilke risikoanalysemetoder vil dere anbefale opp mot denne bransjen får å fange opp eventuelle framtidige trusler?

6. Hvilke fordeler og ulemper er det i risikostyringsvertøyene (ROS analyse) som bransjen må være klar over for å kunne bruke disse på en hensiktsmessig måte?

7. Hvordan kan bransjen bedre informasjonssikkerheten?

8. Hvordan kan en redusere sårbarheten i bransjen?

9. Anbefales det inntrengingstesting uten forutgående samtykke?

10. Hvordan er deres oppfatning av kunnskapen av sikring/security er for bransjen?

11. Hvor viktig mener dere det er at risiko forståelsen er forankret i ledelsen?

12. Hva gjør dere som myndigheter/eksperter/ opp mot bransjen for å hjelpe de til å bli mer styrket opp mot fagfeltet sikring/security?

13. Hvordan bedre/håndtere sikkerheten innen informasjonssikkerhet?

Vedlegg 2

Risiko:

1. Hvordan vil du beskrive risiko, jobber dere ut fra noen bestemte definisjoner? *(kombinasjon av sannsynlighet og konsekvens eller ser en på risiko som en vurdering av fremtiden der det er flere kvalifiserte vurderinger, der det er kunnskapsgrunnlaget og vurderingen som er bakgrunnen for risikovurderingene som er viktige for beslutningsmaterialet).*

2. Hvilke fordeler og ulemper finner dere ved risikostyringsverktøyene som dere benytter. Eks. hva er fordelen med ROS analysen hva er det denne ikke fanger opp?

3. Hvor godt kjenner dere til anbefalingene til NSM og deres risikostyrings anbefalinger NS 5830 serien?

4. Hvilke typer risikoanalyser tas i bruk hos dere for å avdekke risiko og hvordan benyttes disse analysene for deres beslutning opp mot håndtering av risikoen?

5. Når dere identifiserer hendelser hvor godt presenterer en dette i siste del av risikohåndteringen? Hvem er med i identifiseringen av farer? Hvem sitter i gruppen?

Sikkerhet:

6. Hva tiltak er iverksatt hos dere for å redusere risiko og sårbarheten, innen fysiske trusler, logiske ondsinnet programvare, sosiale trusler, systemfeil og gjensidige avhengigheter?

7. Er noe av sikkerheten/IKT systemer outsourset?

8. Hvor ofte drives det holdningskampanjer inne avviks rapportering innen brudd på informasjonssikkerhet?

9. Hva tiltak er blir igangsatt for å bedre og fostre en god sikkerhetskultur?

10. Hvilke verktøy bruker din virksomhet for å måle risikoen for tilsiktede hendelser?

11. Hvordan vil du si deres kunnskap om sikring/security områder er og hva utfordringer/fordeler gir dette dere i deres risikovurderinger?

12. Sikring blir ofte sett opp mot villede handlinger og sikkerhet opp mot hendelser/ulykker. Hvem har ansvaret for sikkerhet og hvem har ansvaret for sikring eller er det en ansvarlig for begge?

13. Hvordan jobber dere med å redusere/håndtere informasjonssikkerhet i deres virksomhet?

14. Hvordan sikrer dere at sikkerheten for IKT systemer og bruken av denne, er godt forankret i ledelsen?

Sårbarheten:

15. Hvordan jobber dere for å redusere sårbarheten i virksomheten? Tenker da på sårbarheten i teknologiske systemer IKT.

16. Har NSM gjennomført inntrengningstesting uten forutgående samtykke?

17. Hvordan oppfatter dere at samarbeidet med tilsynsmyndighetene er? Får dere den hjelp og støtte som dere føler at dere trenger får å sikre dere opp mot hendelser innen kriminalitet og/eller terror?

18. Hvor ofte får dere oppdateringer fra PST angende trusselbilde?

Vedlegg 3

Til den det måtte angå:

Forespørsel om intervju i forbindelse med en masteroppgave

Jeg er masterstudent ved Universitetet i Stavanger og holder på med den avsluttende erfaringsbaserte masteroppgaven i risikostyring og sikkerhetsledelse. Temaet for oppgaven er Informasjonssikkerhet i et samfunnsperspektiv. Ønsket er å se hvordan en kan redusere sårbarhetene og øke sikkerheten i kraftforsyningssektoren ved hjelp av risikostyringsverktøy. Ønsker også å se på fordeler og ulemper en finner i risikostyringsverktøyene. Oppgaven er spisset til kraftforsyningssektoren og jeg ønsker å ha fokus på den fysiske sikkerheten ikke den rent tekniske sikkerheten.

For å finne ut av dette ønsker jeg å intervjue de som er med og regulerer bransjen for å få et innblikk i hva forventninger myndighetene anser som god risikostyring for å ha en god sikkerhet opp mot informasjonssikkerhet.

Spørsmålene vil dreie seg om de generelle trekkene som omhandler risikostyring og hvordan en jobber for å bedre og håndtere sikkerheten, for å gjøre virksomheten best mulig i stand til å avdekke sårbarheter og sikre strøm til sine kunder. Jeg vil ikke komme inn på hva tekniske barrierer som blir benyttet i disse virksomhetene, heller ikke spørsmål som kan avdekke sårbarheter i den enkelte virksomhet.

Jeg vil bruke båndopptaker og ta notater mens vi snakker sammen. Intervjuet vil ta omtrent en time, og vi blir sammen enige om tid og sted, ønsker at intervjuet gjennomføres i løpet av juni evt i starten av juli.
Det er frivillig å være med og en har mulighet til å trekke seg når som helst underveis, uten å måtte begrunne dette nærmere. Dersom du trekker deg vil alle innsamlede data med deg bli anonymisert. Opplysningene vil bli behandlet konfidensielt, og ingen enkeltpersoner vil kunne kjenne seg igjen i den ferdige oppgaven. Opplysningene anonymiseres og opptakene slettes når oppgaven er ferdig, innen utgangen av 2017.

Dersom du ønsker å være med på intervjuet, vennligst skriv under på den vedlagte samtykkeerklæringen og returner signert og skannet erklæring til meg.

Hvis det er noe dere lurer på kan du ringe meg på (47) 47 01 18 22, eller sende en e-post til lailarefsland@me.com. Dere kan også kontakte min veileder Sindre Aske Høyland senter for risikostyring og samfunnssikkerhet (SEROS) Det samfunnsvitenskapelige fakultet. Telefonnummer (47) 51 83 37 55.

Med vennlig hilsen

Laila Refsland

Snorres.gt 3

4044 Hafrsfjord

Samtykkeerklæring:
Jeg har mottatt informasjon om studien om informasjonssikkerhet i et samfunnsperspektiv og ønsker å stille på intervju.

Signatur Telefonnummer