Lars Borgos

IKT-sikkerhetsutfordringer i et organisasjons- og samfunnsperspektiv

Casestudie av tre virksomheter under sikkerhetsloven

Masteroppgave i organisasjon og ledelse,
spesialisering i innovasjon og endringsledelse, SOS6901
Veileder: Eirik Albrechtsen
Trondheim, januar 2017

Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for sosiologi og statsvitenskap

NTNU
Kunnskap for en bedre verden

Forord

I det jeg skriver disse linjene er masteroppgaven sluttført ved siden av min fulltidsjobb i NSM. Det har vært en spennende reise som har gitt meg mye ny kunnskap.

Jeg valgte å undersøke IKT-sikkerhetsutfordringer i et organisasjons- og samfunnsperspektiv ettersom temaet omfatter mange interessante problemstillinger, samtidig som IKT-sikkerhet er relativt lite utforsket i et sosio-teknisk perspektiv.

Først vil jeg få takke til min veileder førsteamanuensis Eirik Albrechtsen ved institutt for industriell økonomi og teknologiledelse NTNU for utmerket hjelp, støtte og inspirasjon igjennom studiets mange faser. Takk til professor Per Morten Schiefloe og forsker Petter Grytten Almklov for alle kommentarer og råd.

Takk til min arbeidsgiver som ga tilslutning til prosjektet. Takk til mine kolleger Knut Herje og Lene Bogen Kaland for kommentarer til oppgaven. En ekstra takk til Knut som også bidro med å sette meg i kontakt med mulige informanter.

Takk til alle informantene som tok del i studien, delte av sine erfaringer og utviste et stort engasjement som resulterte i et omfangsrikt empirisk materiale.

Takk til min kjæreste Henriette for råd og tålmodig støtte gjennom arbeidsprosessen. Takk til min kjære sønn Håkon for korrekturlesning av manuskriptet og gode forslag til forbedringer.

29. januar 2017

Lars Borgos

Innhold

Sammendrag

Økende avhengighet til IKT-systemer preger de fleste arenaer i vårt samfunn, og kritiske samfunnsfunksjoner er ifølge NOU 2015:13 (2015) avhengig av lange, sammensatte og uoversiktlige verdikjeder på tvers av sektorer og nasjoner. Trusselbildet preges av hyppige skift, samtidig som IKT-avdelingene ofte møter nye krav om tjenester fra omgivelsene. IKT-systemer passer inn i Perrows (1984) normalulykkesteori om systemulykker som kjennetegnes av høy interaktiv kompleksitet og tette koblinger. Feil ett sted i IKT-systemet kan forplante seg til andre steder i nettverket eller gjennom tilkoblede nettverk.

Nasjonal sikkerhetsmyndighet (NSM) innehar en samfunnsviktig rolle som Norges ekspertorgan for informasjons- og objektsikkerhet. NSMs ansvar omfatter utforming av krav og tiltak, gi rådgivning og veiledning, utstede godkjennelser og å føre tilsyn på bakgrunn av bestemmelser fastsatt i sikkerhetsloven (SL). En rekke offentlige- og private virksomheter er omfattet av sikkerhetskravene for beskyttelse av informasjon, og mange av disse virksomhetene inngår også i kritisk infrastruktur eller leverer samfunnskritiske tjenester. Resultater fra NSMs tilsynsaktiviteter kan tyde på at det er krevende for virksomhetene å opprettholde et IKT-systems sikre tilstand i henhold til SL. Det var derfor av interesse å finne ut mer om hvorfor sikkerhetsarbeidet eventuelt er utfordrende. Det empiriske grunnlaget for studien ble fremskaffet gjennom kvalitative intervjuer med 13 informanter fra tre virksomheter A, B og C underlagt SL.

Pentagonanalysen og drøftingen i kapittel 6 viste for det første at utfordringene omhandlet mer enn bare formelle kvaliteter som formell struktur og teknologi ettersom mange funn omfattet de uformelle kvalitetene kompetanse, verdier og holdninger; interaksjon; sosiale relasjoner og nettverk. For det andre viste analysen at det er avhengigheter mellom formelle og uformelle kvaliteter. Funnene kan derfor ikke betraktes som isolerte fenomener, men må forstås i sammenheng med hverandre. Et tredje moment er at virksomhetene også møtte utfordringer knyttet til eksterne faktorer som politisk nivå, NPM og leverandører.

Flertallet oppfattet sikkerhetskravene for gradert informasjon som relevante; legitime; bra hjelpemiddel, mens halvparten anså kravene til lavgradert informasjon som mindre legitime enn for høygradert informasjon. Halvparten mente preskriptive krav ikke holdt følge med teknologiutviklingen. Det var målkonflikter mellom kravet til administratorroller og –

privilegier og behovet for fleksibilitet og effektiv drift gjennom NPM, noe som gjorde virksomheten mer sårbar.

Stramme økonomiske rammer; latente betingelser; økt interaktiv kompleksitet og tette koblinger; høyt tids- og arbeidspress; undervurdering av kapasitetsbehovet utfordret drift- og vedlikeholdsnivået av IKT-systemene, og resulterte i ad-hoc preget arbeidsform hos to virksomheter. Mangelfull verktøystøtte resulterte i mer manuelt drifts- og vedlikeholdsarbeid, og den menneskelige faktor regnes som det største problemet i forbindelse med vedlikehold. Samfunnskritiske tjenester hadde stanset i forbindelse med vedlikehold.

Målkonflikter mellom sikkerhet og tjenesteleveranser kunne skyldes: sikkerhet ble tatt for gitt; lederne ble målt på leveranser; NPM reduserte sikkerhetsmarginene; politisk bestemte leveranser. Fragmenterte prosjekter utfordret kommunikasjon og koordinering hos en virksomhet. Tidspress var mulig forklaring på svak koordinering, kommunikasjon og samhandling. Stort arbeidspress var mulig forklaring på gradvis frikobling fra etablerte rutiner.

Ansvarsavklaringer ved sammenkoblinger av IKT-systemer er viktig i et samfunnsperspektiv, da koordinering i en beredskapssituasjon hovedsakelig skjer gjennom etablert avtale.

Mens politisk oppmerksomhet ble utløst av tilsynsrapporter og hendelser, kunne hendelser bli utløst av mangelfull informasjon eller feiltolkning. Svikt i sikkerhetsarbeidet og hendelseshåndtering kunne forklares med: menneskelige feil; feiltolkning; manglende forståelse for at feil var inntruffet.

Halvparten av informantene i virksomhetene B og C var fornøyd med kompetansenivået, mens alle andre ønsket en styrkning av kompetansen. Mangelfulle kurstilbud; behovet for kompetanse på både ny og gammel teknologi; turnover representerte organisatoriske sårbarheter. Brukeratferden i forhold til virksomhetens sikkerhetsutstyr ble utfordret av moderne privat utstyr. Brukerinvolvering i grupper er mer effektivt ved innføring av ny teknologi og utforming av brukerprosedyrer.

Studien viste behov for mer relevant ledelsesinformasjon, for å styrke forståelsen og utbedre koordineringen. Informantene ønsket at NSM videreutviklet rapportene, råd- og veiledningsarbeidet. I et organisatorisk- og samfunnsmessig perspektiv viser funnene og drøftingen fra denne studien behov for å videreutvikle det proaktive sikkerhetsarbeidet som da bør forankres helt på toppnivå.

Definisjoner og forkortelser

Ord/forkortelse	Definisjon/forklaring
BUM	Bestiller utfører modell
CC	Common Criteria
CERT	Computer Emergency Response Team
FoA	Forskrift om sikkerhetsadministrasjon
FoI	Forskrift om informasjonssikkerhet
FoO	Forskrift om objektsikkerhet
HRO	High Reliability Organizations
IKT	Informasjons- og kommunikasjonsteknologi
ITIL	Information Technology Infrastructure Library
KI	Kritisk infrastruktur
KIKS	Kritisk infrastruktur – kritiske samfunnsfunksjoner
MTO	Menneske – teknologi - organisasjon
NAT	Normalulykkesperspektivet
NPM	New Public Management
NSM	Nasjonal sikkerhetsmyndighet
RE	Resilience Engineering
SIEM	Security Incident Event Management
SL	Sikkerhetsloven
SPOF	Single Point of Failure

Oversikt over figurer og tabeller

1 Innledning

Gjennom flere år er stigende erkjennelse om samfunnets økende avhengighet til IKT for både privat- og offentlig sektor samt i privat sammenheng belyst i utredninger (NOU 2000: 24, 2000; NOU 2006:6, 2006; NOU 2015: 13, 2015), nasjonale strategier[1] og medier. En velfungerende IKT-infrastruktur er derfor av betydning både for samfunnets- og rikets sikkerhet. I (NOU 2015: 13, 2015) vurderer utvalget at kritiske samfunnsfunksjoner avhenger av lange, sammensatte og uoversiktlige verdikjeder på tvers av sektorer og nasjoner, noe som har betydning for hvordan vi bør forholde oss til tilsiktede og utilsiktede hendelser. Perrows (1984) normalulykkesteori går ut på at systemulykker i sosiotekniske systemer kjennetegnes av høy interaktiv kompleksitet og tette koblinger.

Hyppige teknologiske skift og endringer i trusselbildet utfordrer samfunnets IKT-infrastruktur på nye måter (NOU 2000: 24, 2000; NOU 2006:6, 2006; NOU 2015: 13, 2015). IKT-systemer for behandling av gradert informasjon skal som hovedregel forhåndsgodkjennes av Nasjonal sikkerhetsmyndighet (NSM). NSM er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet. NSMs hovedoppgaver er å utforme krav og tiltak, gi råd og veiledning, utstede godkjenning og føre tilsyn. Den mest sentrale målgruppen er offentlige- og private virksomheter med behov for å beskytte informasjon i henhold til sikkerhetsloven. Mange av disse virksomhetene inngår også i kritisk infrastruktur. Direktoratet er altså delegert myndighet i en samfunnsviktig rolle. NSM leverer i dag også ulike tjenester utenfor sikkerhetslovens område. NSM fremmet i 2015, gjennom sikkerhetsfaglig råd[2] 72 nye satsningsforslag til styrende departementer. Direktoratets rolle kan med ganske stor sannsynlighet forventes å endre seg ytterligere i tiden fremover.

Rammevilkår for IKT-sikkerhet er gitt gjennom Sikkerhetsloven (1998) (SL) med tilhørende forskrifter. De mest sentrale forskriftene i denne sammenheng er Forskrift om informasjonssikkerhet (2001) (FoI), Forskrift om sikkerhetsadministrasjon (2001) (FoA) og forskrift om objektsikkerhet (2011) (FoO). Utfyllende bestemmelser til FoI er gitt i form av

[1] Justis- og beredskapsdepartementet, Fornyings-, administrasjons- og kirkedepartementet, Forsvarsdepartementet og Samferdselsdepartementet. (2012). *Nasjonal strategi for informasjonssikkerhet*, Hentet 08.01.2017 fra https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

[2] NSM. (2015). *Sikkerhetsfaglig råd*. Hentet 08.01.2017 fra https://www.nsm.stat.no/globalassets/rapporter/nsm-sikkerhetsfaglig_raad_2015_web.pdf

generiske- og teknologispesifikke krav. Kapittel 2.1 behandler rammebetingelsene mer inngående. Med bakgrunn i kravene utformer virksomhetene gjennom prosjektorganiserte aktiviteter løsningsspesifikasjoner som danner grunnlaget for godkjenning og senere tilsyn. En slik kommando-kontroll regulering omtales ifølge Skotnes (2015) som instrumentell modell for regulering, deterministisk reguleringsregime, detaljert regulering eller preskriptiv regulering. Kravene som må tilfredsstilles kan muligens virke overveldende på virksomhetene. Ved systemteknisk tilsyn[3] er det avdekket ulike feil, mangler og svakheter, noe som kan indikere at det er utfordrende for virksomhetene å tilfredsstille formelle- og tekniske krav fra sikkerhetsmyndigheten. Omfattende retningslinjer kan også bli en unnskyldning for virksomheter slik at de ikke tar ansvaret for å overvåke og implementere ny og anerkjent ekspertise for særegen bransje (Lindøe og Engen, 2013:200).

Tilsynsrapportene fokuserer på avvik og observasjoner, noe som gjerne omtales som negativ rapportering. Slik rapportering understøtter ideen om at virksomhetene kan lære gjennom økt bevissthet om egne feil, mangler og svakheter. Motsatsen til en slik tilnærming er Resilience Engineering (RE) som legger hovedvekten på erfaringsinnhenting og læring gjennom det som går bra (Hollnagel, Tveiten, og Albrechtsen, 2010), og High Reliability Organizations (HRO) av LaPorte og Consolini (1991) som handler om organisatorisk redundans og feiltolerante organisasjoner som hurtig kan tilpasse seg endringer, noe som er en forutsetning i operasjoner som krever høy pålitelighet. Det gjør blant annet at feil kan korrigeres raskt og før det inntreffer konsekvenser. Det andre forholdet er at det er avvikene som danner eventuelt sanksjonsgrunnlag overfor virksomheten. Skotnes (2015) viser at det er utfordrende å finne riktig balanse mellom preskriptive og funksjonelle krav når det gjelder kontroll av sikkerhetsarbeidet i nettverksorganisasjoner, og at det var spesielt krevende med hensyn til komplekse teknologiske risiki.

Sikkerhet i informasjonssystemer skal ifølge FoI § 5.1, vurderes i forhold til egenskapene autentisitet, konfidensialitet, integritet, tilgjengelighet, ansvarlighet og tillit. Sikkerhetstenkningen har i stor grad vært rettet mot konfidensialitet NOU 2015: 13 (2015). Sikkerhetstiltakene i FoI omfatter de syv prinsippene: Minimalisme, minste privilegium, redundans, forsvar i dybden, selvbeskyttelse, kontrollert dataflyt og balansert styrke.

[3] Systemteknisk tilsyn med IKT-sikkerhet er for tiden en NSM-aktivitet under utvikling der virksomhetenes etterlevelse av bestemmelsene blir undersøkt på både et overordnet og detaljert nivå.

Tradisjonell sikkerhetstenkning innenfor IKT er stor grad teknisk rettet, og prinsippene følger i stor grad Haddon Jr (1970); Haddon (1980) virkemidler for å begrense skade, og Reason (1997a) modell om forsvar i dybden. Eksempler på tiltak er brannmur mellom ulike nettverk eller domener, to-faktor autentiseringsmekanisme. Mange av NSMs sikkerhetskrav fokuserer også på å beskytte IKT-systemene mot brukerne. Brukere ansees både som en venn og en fiende (Albrechtsen, 2008). Flere studier har som nevnt av Schiefloe et al. (2005); Schiefloe og Vikland (2007) vist større erkjennelse for viktigheten av menneske – teknologi – organisasjon (MTO) faktorene i lys av sikkerhetsutfordringenes sammensatte natur.

En eventuell tilsiktet eller utilsiktet svikt hos en virksomhet underlagt SL og som i tillegg er en del av kritisk infrastruktur (KI), kan under gitte betingelser ha konsekvenser for andre virksomheter i infrastrukturen. Et ikke helt utenkelig scenario er at skadevare tilflyter andre systemer eller organisasjoner, enten via sammenkoblete systemer eller via "airgap" og bruk av lagringsmedier. I begge tilfellene kan risikoatferd ett sted ha konsekvenser for andre systemer eller virksomheter. Generelt er IKT-sikkerhetsarbeid ressurskrevende, både i forhold til MTO og økonomi. Virksomheter under SL bør i utgangspunktet kunne være dimensjonert for å drive godt sikkerhetsarbeid.

Påviste avvik etter IKT-tilsyn kan indikere at det er krevende å opprettholde systemets sikre tilstand. Det kan i mange tilfeller synes som om sikkerhetsarbeidet har erodert i tiden etter godkjenning, og senere kommer til kunnskap i forbindelse med tilsyn. Det kan derfor være interessant å finne ut mer om årsakene til endringene i IKT-systemets status.

Det er også et spørsmål om ledelsens forståelse og forankring for å drive sikkerhetsarbeid i virksomheten, og ikke minst hvem driver sikkerhetsarbeid i virksomheten. I denne casestudien er det gjennomført undersøkelser hos tre ulike virksomheter som kjennetegnes ved at de er: 1) underlagt SL; 2) inngår i KI; eller 3) leverer samfunnskritiske funksjoner (tjenester). Som et ledd i casestudien er det også sett på hvordan virksomhetene har organisert IKT-sikkerhetsarbeidet.

1.1 Formål

Gjennom anvendelsen av ulike perspektiver i denne analysen av hvordan dagens rammebetingelser for IT-sikkerhet virker i praksis ute hos virksomhetene, vil det kunne gi nyttig lærdom tilbake til både virksomhetene og NSM selv. Med utgangspunkt i ny kunnskap om virkningen av NSMs rammebetingelser gjennom denne studien, kan resultatene betraktes som

et mulig grunnlag for å kunne jobbe mer målrettet med kontinuerlige forbedringer i enten rammebetingelser eller endrede praksiser for råd, veiledning, godkjenning eller tilsyn. På den annen side kan virksomheter som ikke har deltatt i denne casestudien bruke resultatene til å undersøke om de har tilsvarende utfordringer som bør løses. I neste omgang kan nye måter å forstå sikkerhetsutfordringene på legge grunnlaget for å bedre sikkerhetsarbeidet i et samfunnsperspektiv.

1.2 Forskningsspørsmål

Hvorfor er det utfordrende for virksomheter å beskytte samfunnets kritiske IKT-infrastruktur, og å opprettholde et IKT-systems sikre tilstand i henhold til sikkerhetsloven?

Hvordan har de formelle bestemmelsene virket med hensyn på å sette virksomheten i stand til å drive et godt sikkerhetsarbeid? Hvilke forhold er det som ikke har hatt den ønskede effekt? Eksisterer det tilstrekkelig risikoforståelse hos virksomheten og innehar de kunnskap om kompleksiteten i systemene?

Delspørsmålene kan formuleres som:

- *Hvordan er virksomhetenes oppfatning av IKT-sikkerhetskravene?*
- *Hvordan er virksomhetenes praksis i forhold til NSMs intensjoner om å beskytte samfunnets kritiske IKT-infrastruktur, og hva er årsakene til utfordringene?*
- *Hva kan virksomhetene og NSM lære av dette?*

NSM utformer rammevilkår og regler på den ene side, og fører tilsyn med at reglene blir overholdt på den annen side.

For virksomhetene som skal etterleve bestemmelsene innebærer det både menneskelige, teknologiske, organisatoriske og økonomiske utfordringer og konsekvenser. Det er altså sosio-tekniske sammenhenger som skal undersøkes i denne studien. Casestudien vil dermed også kunne gi indikasjoner på NSMs IKT-sikkerhetsrolle i et organisasjons- og samfunnsperspektiv, og kunne gi grunnlag for læring.

Det er altså et fokus på virksomhetenes opplevde utfordringer med utøvelsen av sikkerhetsarbeidet i organisasjonen og organisatoriske egenskaper for sikker drift som er denne oppgavens tilnærming.

1.3 Definisjon av sentrale begreper

Administrasjon av informasjonssystemsikkerhet defineres av Albrechtsen (2015) som de samlede aktivitetene som gjennomføres på en mer eller mindre kontrollert måte for å kontrollere trusler og sårbarheter for å sikre: beskyttelse av informasjonsressurser og teknologi; trygg og sikker manuell og automatisert prosessering av informasjon; trygg organisering og utførelse av arbeid basert på informasjonsressurser og håndtering

Koordinering defineres av Malone og Crowston (1994) som håndtering av avhengigheter mellom aktiviteter.

Kritisk infrastruktur (KI) defineres i (NOU 2006:6, 2006) som de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse. Elektronisk kommunikasjon er et eksempel på kritisk infrastruktur. Se også samfunnskritiske funksjoner. I St. meld. 10 (2016-2017) (2016) er KI definert som anlegg og systemer som er nødvendige for å opprettholde eller gjenopprette samfunnets kritiske funksjoner.

Informasjonssikkerhet brukes ofte synonymt med: IKT-sikkerhet; IT-sikkerhet; cybersikkerhet. I NOU 2015: 13 (2015) bruks begrepet om sikring av digital eller analog informasjon. Tradisjonelt har sikkerhetstenkningen innen IKT vært teknisk rettet, noe sikkerhetstiltakene i FoI bærer preg av, jf kapittel 1.

I Sverige er definisjonen av informasjonssikkerhet av teknisk karakter:

> Cybersäkerhetsbegreppet är mer strategiskt och fokuserar mer på nationella och internationella nätverk. Därmed har cybersäkerhet en större internationell räckvidd med t.ex. folkrättsliga frågeställningar och normer på cyberområdet än det mer tekniska informationssäkerhetsbegreppet. Det senare har en större tyngdpunkt mot hård- och mjukvara samt standardisering. (SOU 2015:23, 2015:40)

I denne casestudien skal informasjonssikkerhet forstås som noe mer enn kun et teknisk anliggende. For det første vil både begrepene IKT-sikkerhet, IT-sikkerhet og informasjonssikkerhet bli brukt i denne studien. For det andre må begrepene forstås i konteksten MTO.

MTO slik som Petroleumstilsynet forklarer det:

> Samspill mellom menneske, teknologi og organisasjon. (Der hvor menneskelig adferd er en barrierefunksjon, må teknologi og organisasjon legges til rette slik at operatør får den nødvendige støtte for å kunne oppfatte situasjonen korrekt, og handle i tråd med de sikkerhetsmessige forutsetninger). (Schiefloe og Vikland, 2007:3)

Begrepene security og safety kan brukes og forstås på litt ulike måter, og i denne oppgaven skal begrepene forstås på følgende måte:

Security defineres som sikkerhet mot uønskede villede hendelser (terror og kriminalitet). Sikkerhet mot uønskede hendelser som er et resultat av overlegg og planlegging (NOU 2000: 24, 2000:307); (Almklov, Antonsen, og Fenstad, 2011:7).

Safety defineres som sikkerhet mot uønskede tilfeldige hendelser. Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter (NOU 2000: 24, 2000:307); (Almklov et al., 2011:7).

Fra NOU 2006:6 (2006) heter det at Begrepet *"sikkerhet*" kan brukes til å dekke alle uønskede hendelser, uavhengig av om de er utilsiktede eller tilsiktede. *"Sikkerhet*" fremstår på denne måten som et overbegrep, et såkalt hypernym. Sikkerhet mot uønskede utilsiktede hendelser kan settes til *"trygghet*", mens sikkerhet mot uønskede tilsiktede hendelser kan settes til *"sikring»*. Utvalget er på linje med professor Finn-Erik Vinje når han skriver at dette "[...]vil være en vilkårlig konstruksjon – i den forstand at den ikke er oppstått spontant i allmennspråket og neppe imøtekommer noe presserende behov der".

Både *"trygghet»* og *"sikring»* blir i dagligtalen brukt om hverandre for å beskrive sikkerhet mot både uønskede utilsiktede og tilsiktede hendelser.

Utvalget ønsker likevel å understreke betydningen av at ordet *"sikkerhet*" blir benyttet som et hypernym. Etter utvalgets mening burde alt sikkerhetsarbeid omhandle både safety og security. Ved å bruke sikkerhet som et hypernym blir dette understreket. For å beskrive safety på norsk, bruker utvalget *"sikkerhet mot uønskede utilsiktede hendelser*". For å beskrive security på norsk, bruker utvalget *"sikkerhet mot uønskede tilsiktede hendelser*". Ved å benytte seg av en slik tredeling, oppnås ønsket presisjon, samtidig som man unngår å stipulere ord som ikke faller naturlig i norsk dagligtale.

Samfunnskritiske funksjoner er tjenester som understøtter KI. Rapporten DSB (2012) diskuterer blant annet hvilke funksjoner som kan oppfattes som samfunnskritiske og angir

prosess for identifisering av kritisk infrastruktur og virksomheter med ansvar for kritiske samfunnsfunksjoner. Ifølge DSB (2012) forstås kritisk infrastruktur – kritiske samfunnsfunksjoner (KIKS) som en mulig fremtidig overordnet risikostyringsmodell, og modellen utfyller objektsikkerhetsregelverket. I St. meld. 10 (2016-2017) (2016) defineres samfunnskritiske funksjoner som: Funksjoner hvis bortfall vil true befolkningens og samfunnets grunnleggende behov.

Sikkerhetskritisk atferd defineres i denne oppgaven som "atferd der utfallet av atferden kan ha direkte eller indirekte konsekvenser for sikkerheten i en operasjon eller aktivitet" (Schiefloe (2011a:3).

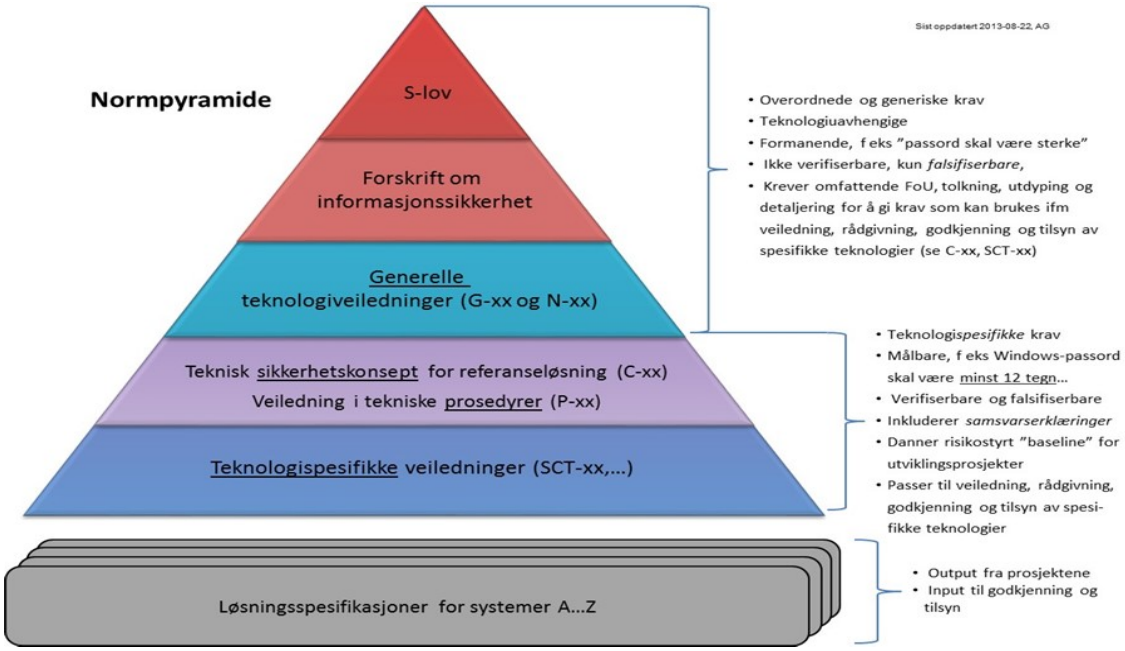
Sikker tilstand er i FoI § 5-2, første punkt definert som: a) Det skal etableres en helhetlig og enhetlig IKT-infrastruktur med nødvendige sikkerhetsfunksjoner, -strukturer og tillitsnivå. b) Det skal implementeres og dokumenteres en sikker tilstand, det vil si at sårbarheter for denne infrastrukturen reduseres til et akseptabelt nivå.

2 Bakgrunn

Ettersom virksomhetene i denne casestudien er underlagt sikkerhetsbestemmelser, er det naturlig først å redegjøre for dagens rammebetingelser i kapittel 2.1, og deretter i kapittel 2.2 omtales studiens omfang og utvalg.

2.1 Rammebetingelser

Formelle rammer er gitt av blant annet: SL[4], og aktuelle forskrifter som kan komme til anvendelse er: sikkerhetsadministrasjon; informasjonssikkerhet; objektsikkerhet; personellsikkerhet; sikkerhetsgraderte anskaffelser. NSM har produsert rammebetingelser som kan virke krevende for en virksomhet å etterleve. Normalsituasjonen i NSMs veiledningsarbeid er å bruke de generelle veiledningene (G-xx, N-xx), men dersom en virksomhet ikke har fortolket kravene på en slik måte at løsningen kan godkjennes pleier veilederne å vise til mer teknologispesifikke krav (C-xx, P-xx, SCT-xx, …) der slike eksisterer. Figur 1 nedenfor viser NSMs normpyramide med utgangspunkt i SL og avgrenset til Forskrift om informasjonssikkerhet (2001) (FoI) med tilhørende veiledninger.



Figur 1 Normpyramide - hentet fra NSM v/AG (2013)

[4] Det er foreslått endringer sikkerhetsloven i NOU 2016:19, *Samhandling for sikkerhet: Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*: utredning fra utvalg oppnevnt ved kongelig resolusjon 27. mars 2015 : avgitt til Forsvarsdepartementet 12. oktober 2016. Hentet fra https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/

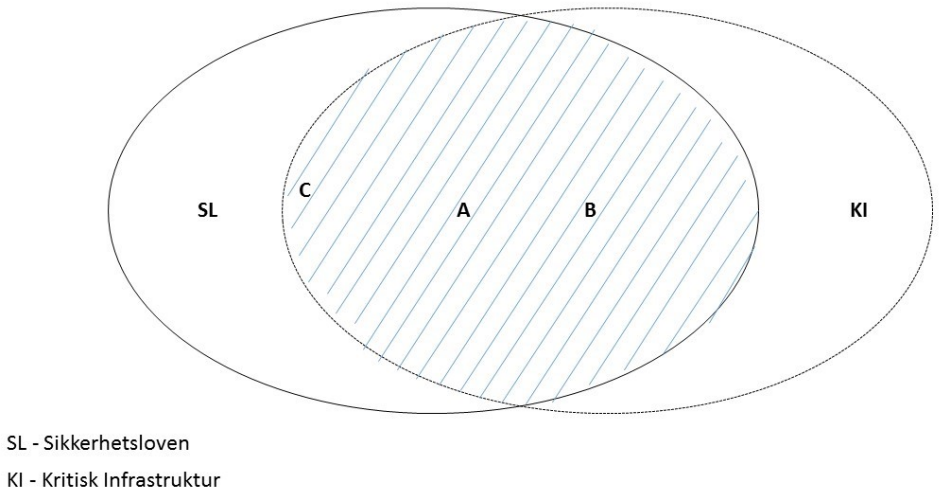
I tillegg kommer Forskrift om sikkerhetsadministrasjon (2001) (FoA) som regulerer hvordan virksomheten skal organisere sikkerhetsarbeidet, herunder blant annet med minimuskrav til sikkerhetsorganisasjon og hvilke roller som må etableres. Forskrift om objektsikkerhet (2011) (FoO) med tilhørende veiledninger er relevant for virksomheter under SL som har skjermingsverdige objekter. IKT-systemer kan inngå i objektsikkerhetsbegrepet. FoO inneholder generelle overordnete krav til informasjonssikkerhet, og det er overlatt til virksomheten å finne passende tiltak. Virksomhetene er ikke pålagt å bruke de tekniske veiledningene som er utformet under FoI. Dersom et informasjonssystem klassifisert som et objekt skal behandle gradert informasjon kommer FoI til anvendelse. Forskrift om personellsikkerhet (2001) er relevant for personell som skal ha tilgang til skjermingsverdig informasjon eller objekter gradert konfidensielt eller høyere. Forskrift om sikkerhetsgraderte anskaffelser (2001) regulerer forhold knyttet til sikkerhetsavtale og leverandørklarering.

Virksomheter er pålagt å konsultere NSM i forbindelse med etablering av visse systemer som skal behandle sikkerhetsgradert informasjon. Det er derfor vesentlig hvilken innsikt virksomheten har fått i det gjeldende rammevilkår fra NSM før utvikling og tiltak blir iverksatt.

FoA og FoI angir krav til organisering av sikkerhetsarbeidet og tekniske sikkerhetskrav. Når det gjelder organisering av driften og hensiktsmessige driftsrutiner henviser NSM eksempelvis til ITIL[5] som ett mulig alternativ. Som nevnt innledningsvis er NSM både kravstiller, godkjennings- og tilsynsmyndighet.

[5] Information Technology Infrastructure Library (ITIL) er et strukturert rammeverk eller antologi for kvalitetssikring av leveranse, drift og support innen IT-sektoren. ITIL går inn i organisasjonsstrukturen, og de faglige ferdigheter til en IT-organisasjon, ved å presentere et utførlig sett managementprosedyrer som en organisasjon kan benytte til å styre sine IT-operasjoner. Hentet 20.12.2016 fra https://no.wikipedia.org/wiki/ITIL

2.2 Studiens omfang og utvalg



Figur 2 Utvalgte virksomheter i casestudien

Figur 2 viser plasseringen av de tre virksomhetene A, B og C som deltar i denne casestudien. Som figuren viser kan virksomheter enten være kun under SL, eller kun KI eller omfatte både SI og KI. I denne casestudien er virksomhetene A og B plassert under både SI og KI. Det var divergerende oppfatninger blant informantene hvorvidt organisasjonen C hørte til under KI, og av den grunn er C plassert på grensen mellom SI og KI. Virksomhet B leverte tjenester som understøttet kritiske samfunnsfunksjoner.

Et fellestrekk ved alle virksomhetene i casestudien er at IKT-utvikling (bestiller) er adskilt fra IKT-drift (utfører) som også noen ganger benevnes henholdsvis forvaltning og drift. Se kapittel 4.6 for nærmere forklaring på organisasjonsmodellen.

Med bakgrunn i forskningsspørsmålet presentert i kapittel 1.2, er valgt forskningsdesign og metodikk for denne studien behandlet i kapittel 3. Introduksjon til de mest sentrale teoriene følger i kapittel 4. Resultatene presenteres i kapittel 5. Analyse og drøfting er fremstilt i kapittel 6, og konklusjon følger i kapittel 7.

3 Metodikk

I kapittel 3.1 følger beskrivelse av egen rolle og forforståelse, kapittel 3.2 redegjør for forskningsdesign og forskningsmetode, kapittel 3.3 omhandler innsamling og bearbeiding av datagrunnlaget, deretter beskrives reliabilitet i undersøkelsen i kapittel 3.4, mens kapittel 3.5 tar for seg studiens validitet, og til sist i kapittel 3.6 følger avhandlingens struktur.

3.1 Egen rolle og forforståelse

Denne forskningsoppgaven fokuserer på sikkerhetsutfordringer med IKT i et organisasjons- og samfunnsperspektiv gjennom en casestudie av tre virksomheter under SL. Som nevnt i kapittel 1 viser funn fra NSMs tilsynsaktiviteter at det ikke er helt enkelt å tilfredsstille alle krav i SL, og virksomhetene oppfordres til selv å finne underliggende årsaker til påviste avvik. Jeg har gjennom min fartstid i NSM[6] siden 2000 jobbet med IKT-sikkerhet og lært mye om hvordan sikkerhetsmyndigheten utøver sine oppgaver, samtidig som jeg har fått mer kjennskap til "kundesiden" av sikkerhetsmyndigheten. I årene før 2000 var jeg gjennom ulike roller i min forrige jobb på kundesiden av sikkerhetsmyndighetens tjenester, altså i en liknende posisjon som virksomhetene i denne casestudien.

Utgangspunktet for denne studien var et ønske om å finne ut mer om årsakene til virksomhetenes utfordringer i sikkerhetsarbeidet gjennom anvendelse av vitenskapelige metoder som beskrevet i kapitlene 3.2 - 3.5 opp mot teorien som beskrevet i kapittel 4.

Datagrunnlaget ble samlet inn slik som beskrevet i kapittel 3.3, og i den senere analysen er det kun det empiriske grunnlaget fra datainnsamlingen som er benyttet. Ved utforming av intervjuguiden har jeg hatt nytte av min forståelse for problemstillingene som skulle undersøkes. Jeg mener derfor det er grunnlag for å si at forforståelsen har bidratt til å spisse studien inn mot temaer det var av særlig interesse å finne svar på.

Temaet IKT-sikkerhet er følsomt og mye informasjon knyttet til informasjonssystemene er gradert på ulike nivåer. I denne casestudien måtte derfor undersøkelsen konstrueres på en måte som gjorde det mulig å belyse problemstillingene uten å måtte eksponere gradert informasjon. Selv om funnene ikke inneholder gradert informasjon, kan resultatene likevel være følsomme av andre grunner som eksempelvis risikoen for at virksomheter eller informanter kan bli

[6] Forsvarets overkommando/sikkerhetsstaben frem til 31.12.2002

gjenkjent. Det er derfor en medvirkende årsak til at virksomheter og informanter er anonymisert i denne studien. Det er også tatt hensyn til sensitiviteten i det empiriske grunnlaget i forbindelse med fortolkningen av transkripsjonene, og av den grunn er informantenes formuleringer og sitater bearbeidet uten at meningsinnholdet er endret. Den andre grunnen er at det er tvilsomt om virksomheter og informanter ville stilt opp i studien uten forsikringer om anonymisering. Jeg vil derfor si at min forforståelse for temaet var både nødvendig og verdifull ved planlegging, utforming og gjennomføring av denne studien.

3.2 Forskningsdesign og forskningsmetode

Forskningsdesignet for denne studien setter rammene for hvordan forskningen er gjennomført, hvilket datagrunnlag som er brukt, hvordan innsamling og analyse er utført. Grunnlaget for valg av forskningsdesign er i stor grad styrt av forskningsspørsmålet, hvilke fenomener som skulle studeres og den teoretiske rammen som er valgt for undersøkelsen. Yin (2014) beskriver casestudier som en studie som undersøker alle samtidige fenomener i dybden i kontekst av den virkelige verden hvor forskningsdesignet altså er planverket for gjennomføring av studien som dermed danner en logisk link mellom forskningsspørsmålet, datainnsamlingen, analysen og funnene som til syvende og sist begrenser de funn som kan komme til syne.

Forskningsdesignet kan betegnes som en kausal studie der hensikten er å finne årsakssammenhenger. Det er en eksplorativ undersøkelse med et fokus på problemløsning i dette studiet.

Undersøkelsen ble gjennomført som en casestudie der tre ulike anonymiserte virksomheter underlagt SL inngår i studien. Av konfidensialitetshensyn er størrelsen på virksomhetene også anonymisert, og virksomhetene blir derfor heretter kun navngitt som A, B og C. Bakgrunnen for at tre virksomheter ble valgt var å se om det etter særskilte likhetstrekk eller forskjeller mellom virksomhetene opp mot de temaene som inngår i studien. Videre bidro tre virksomheter til å få frem et mer valid datagrunnlag for den senere analysen og drøftingen.

Bevisene i et multiple-case studie betraktes ifølge Herriott og Firestone (1983) som mer robust enn i et single-case studie. Et single-case studie er mer sårbart, ettersom man *"*plasserer alle eggene i en kurv" (Yin, 2014). Bruk av to eller flere case gir ifølge Yin (2014) vesentlige analytiske fordeler.

I dette studiet ble det vurdert som mest aktuelt å foreta en kvalitativ undersøkelse. Det er en deskriptiv undersøkelse som handler om å kartlegge variabler. Empirien for studien ble hentet inn ved gjennomføring av kvalitative intervjuer basert på åpne spørsmål. Det vil si at informanten stod fritt til å bruke sin egen beskrivelse i besvarelsen av spørsmålene. En kvantitativ undersøkelse er til sammenlikning mer låst i formatet i forhold til en kvalitativ studie, ettersom svaralternativene i en kvantitativ undersøkelse er gitt på forhånd. Den kvalitative undersøkelsen i dette studiet kan kategoriseres som semistrukturert, ettersom det var behov for å sikre at visse tema ble belyst i undersøkelsen. Det vil si at rekkefølgen, tema og selve spørsmålene kan varieres, men undersøkelsen bygger på en overordnet guide (Johannessen, Christoffersen, og Tufte, 2010). Samtidig vil det være åpne spørsmål, slik at det blir mulig å få belyst komplekse sammenhenger og ukjente spørsmål, samt gi et godt utgangspunkt for læring (Argyris og Schön, 1996). Med bruken av åpne spørsmål kunne selve intervjuene også som nevnt over beskrives som en eksplorativ undersøkelse.

Noen av fordelene med en kvalitativ undersøkelse er ifølge Johannessen et al. (2010) at informantene får større frihet til å formulere seg; muliggjør rekonstruksjon av hendelser; kan få frem situasjonsbestemt kunnskap; kan få frem nyanser og belyse kompleksitet; kan anvendes som supplerende metode og få frem nye perspektiver.

Bakgrunnen for at det ble valgt en kvalitativ studie er at det fremstod som mest hensiktsmessig for denne undersøkelsen. IKT-sikkerhet er et komplekst felt som involverer mange aktører på ulike beslutningstrinn. IKT-sikkerhet, forhold som er knyttet til feltet eller rammevilkår kan derfor oppfattes ulikt av personer, noe som kan være vanskelig å fange opp gjennom en kvantitativ studie. En tilnærming som også fokuserer nedenfra og opp, vil kunne gi bedre legitimitet til resultatene som kommer frem i undersøkelsen.

En ulempe ved kvalitative undersøkelser er at resultatene ikke kan generaliseres statistisk, slik kvantitative undersøkelser som er basert på tilfeldig utvalg kan gi grunnlag for Kvale, Anderssen, og Rygge (1997). Kvalitative studier kan imidlertid som Schiefloe (2011b) foreslår generaliseres substansielt gjennom teoretisk og logisk argumentasjon for at tilsvarende fenomener også gjelder for liknende case, noe som da må besvares ved empirisk etterprøving. Kvale et al. (1997) bruker begrepet analytisk generalisering som omhandler i hvilken grad funnene fra en studie gir en rettesnor for hva som kan inntreffe i en annen situasjon. Når det gjelder virksomheter som opererer under tilsvarende betingelser som virksomhetene A, B og C i denne casestudien, så kan ifølge Corbin og Strauss (2015) resultatene gi grunnlag for læring.

Kvale, Brinkmann, Anderssen, og Rygge (2009, 2015) legger vekt på at hensikten med intervjuene er å innhente kjennskap til informantenes dagligliv for å kunne tolke betydningen av de fenomenene som beskrives. Intervju er en særlig velegnet metode til å gi informasjon om hvordan personer som intervjues, opplever og forstår seg selv i sine omgivelser.

Utvalg av informanter karakteriseres ifølge Thagaard (2009, 2013) som tilgjengelighetsutvalg. Metodevalget ble gjort i visshet om at IT-sikkerhet er et følsomt tema og at det dermed kunne by på utfordringer å finne frem til personer som var villige til å stille opp i studien. En god kollega bidro med å introdusere prosjektet overfor aktuelle miljøer, og det ble deretter etablert kontakt mellom flere mulige informanter. I tillegg har studiens problemstilling vært førende for hvilke informanter som ble forespurt om deltakelse i prosjektet, noe som ifølge Thagaard (2009, 2013) betegnes som strategisk utvalg. Thagaard (2009, 2013) utdyper med at deltakere velges ut fra de egenskaper og kvalifikasjoner som er strategiske i forhold til problemstillingen og de teoretiske perspektivene som inngår i undersøkelsen.

For å få et tilstrekkelig antall informanter til undersøkelsen var det nødvendig å ta i bruk en ny metode for å finne informanter. Det ble rettet henvendelser til noen av informantene om hvilke andre personer som kunne forespørres om å ta del i undersøkelsen. Denne metoden betegnes ifølge Thagaard (2009, 2013) som *"Snøballmetoden*". Utvalget av informanter og fordeling av informanter på organisasjonsnivåer er vist i tabellene 1 og 2 nedenfor.

Virksomhet	**Informanter**
A	5
B	2
C	6

Tabell 1 Utvalg av informanter fordelt på virksomheter

Høyere ledernivå	**Ledelse og/el fag (sikkerhetspersonell)**	**Fag (operativt)**
1	11	1

Tabell 2 Utvalg av informanter fordelt på roller og organisasjonsnivåer

To innvendinger mot tilgjengelighetsutvalg ifølge Thagaard (2009, 2013) er at informanter i slike utvalg representerer personer som er vant til forskning; kan gi en skjevhet som innebærer mer innsyn i mestring av ulike situasjoner enn konfliktfylte forhold, mens de som kanskje kunne sagt noe om det siste forholdet kanskje ikke er representert i undersøkelsen. Til det er det å si at feltet som er studert er av spesialisert karakter hvor majoriteten av informantene har spesialisert bakgrunn, mens øvrige har høy kompetanse av mindre spesialisert art. I den forstand kan man si utvalget har visse skjevheter, men det vurderes ikke å ha resultert i negative konsekvenser ettersom studien omfattet et felt med høy kompleksitet. Et annet forhold er studiens sensitive karakter, noe som dels resulterte i at beskyttelsesverdig informasjon er utelatt. Det andre poenget er som nevnt i kapittel 3.1 relatert til utfordringene med å få tak i informanter, noe som da kan knyttes til studiens sensitive karakter og som dermed begrenset tilgjengeligheten på informanter. Studiens utforming ansees å nøytralisere de to innvendingene som er nevnt foran.

Kategoribasert utvalg ved at informanter som representerer den *"*butte*"* (*"blunt end"*)[7] og *"*spisse*"* (*"sharp end"*)[8] enden av organisasjonen inngår i studien, i tillegg representerte informantene både høyere og lavere nivåer når det gjelder autoritet. Et kategoribasert utvalg etter de prinsippene som er beskrevet over kan ut i fra Thagaard (2009, 2013) betegnes som kvoteutvelging. Bredden i utvalget er representert gjennom den butte og spisse enden av organisasjonen samt de ulike autoritetsnivåene, men bredden ble smalere enn ønsket ettersom det bød på utfordringer å få flere informanter fra den butte og spisse enden av virksomhetene som fremstilt i tabell 2. Undersøkelsen ble imidlertid konstruert slik at den butte og den spisse enden av virksomhetene er dekket gjennom perspektivene fra de informantene som deltok i studien.

[7] Med den *"*butte*"* enden av virksomheten eller *"*blunt end*"* menes slik som designere, planleggere, analytikere og regulerende myndigheter, en gruppe beslutningstakere som ikke er tett på det operative nivået og har høyere myndighet enn operativt nivå.*

[8] Med den "spisse" enden av virksomheten eller "sharp end" menes slik som piloter, offshore inspektører, vedlikeholds personell for fly, flygeledere, en gruppe beslutningstakere i det operative miljøet som er tett på farer eller hendelser. Oppgavene preges av å være mer hendelsesdrevet med kortere tidshorisonter mesteparten av tiden. Personell har også mer oppdatert og detaljert førstehåndskjennskap til systemene enn personell i den spisse enden av virksomheten.* Begge forklaringene er hentet fra (Rosness et. al. 2010). I IKT-sammenheng menes med den "spisse" enden slik som IKT-drift, CERT-miljøet, brukere.

3.3 Innsamling og bearbeiding av datagrunnlaget

Som et ledd i forberedelsene ble det utformet en intervjuguide. Hensikten med intervjuguiden var å sikre at ønskede tema i forhold til problemstillingen ble belyst, og at det var et egnet hjelpemiddel for å kunne strukturere intervjuet. Intervjuguiden ble prøvd ut i en pilottest før selve undersøkelsen startet. Pilottesten avdekket behov for å innarbeide enkelte mindre justeringer. Intervjuguiden ble kvalitetssikret av veileder før undersøkelsen startet. Intervjuene ble tatt opp elektronisk og deretter transkribert til tekst. Transkripsjonene ble deretter gjennomgått av de enkelte informantene for kommentarer og eventuelle korreksjoner. Hensikten var todelt: å avklare om informantene fikk uttrykt det de hadde ment å formidle og oppklare eventuelle uklarheter; verifisere og sikre at det ikke var skjermingsverdig informasjon i datamaterialet. Svarene fra intervjuene ble deretter bearbeidet, kategorisert og konsentrert til et mer håndterbart format før analysen og drøftingen startet. Transkripsjonene ble kodet og lagt inn i programmet NVivo Pro, versjon 11, som er ett av flere verktøy for analyse av kvalitative data. Under bearbeidingen av svarene ble det sett etter om bestemte mønstre i svarene gikk igjen. Svarene ble fortolket av forskeren både under datainnsamlingen og bearbeidingen.

Følgende fremgangsmåte ble benyttet for intervjuene i denne casestudien hos tre ulike virksomheter hvor i alt 13 informanter stilte opp til intervju: Etter utført pilottest og kvalitetssikring av intervjuguiden ble det avtalt tid for intervjuene med informantene to uker i forveien. Intervjuguiden ble deretter formidlet til informantene, slik at de skulle få rimelig tid til tenke igjennom temaene på forhånd og eventuelt andre forhold som de måtte ønske å ta opp. Noen dager før intervjuene fant sted ble det sendt en påminnelse om avtalen. Intervjuene startet med å gå igjennom samtykkeerklæringen hvor det blant annet er presisert at det var frivillig å delta samt at alle svarene skulle anonymiseres i avhandlingen.

3.4 Reliabilitet i undersøkelsen

Reliabilitet knyttes til spørsmålet om forskningens pålitelighet (Thagaard, 2009), og i en kvalitativ studie handler om hvorvidt resultatene lar seg reprodusere av andre. Det handler om forskningsresultatenes konsistens (Kvale et al., 1997) og troverdighet (Kvale et al., 2009). Thagaard (2009, 2013) kobler spørsmålet om reliabilitet til forskningens pålitelighet. Det er ikke nødvendigvis så lett ettersom IKT-sikkerhet er et komplekst felt hvor forutsetningene for studiet kan endre seg over tid fra undersøkelsen gjennomføres første gang til øvelsen repeteres.

I en kvalitativ undersøkelse kan ifølge Johannessen et al. (2010) studiens reliabilitet (pålitelighet) styrkes gjennom å beskrive konteksten og forskningsprosessens fremgangsmåte på en inngående, åpen og detaljert måte. Det innebærer ifølge Silverman (2011) (Referert fra Thagaard (2013)) at forskningsprosessen er transparent både med hensyn til forskningsstrategi, analysemetoder og teoretisk grunnlag. Gode retningslinjer for gjennomføring av casestudie er som Yin (2014) beskriver å utføre forskningen på en slik måte at en revisor kan repetere prosedyren og forhåpentlig komme frem til samme resultat.

Denne studiens reliabilitet er derfor søkt underbygget i de foregående avsnittene gjennom fremstillingen av formålet med studien, detaljert beskrivelse av hvordan denne studien er bygget opp, hvilke metoder som er brukt og hvordan prosjektet er gjennomført. Forskningsdesign, forskningsmetode, datainnsamling, hvordan datagrunnlaget er tolket og hvilke verktøy som er brukt i bearbeidingen av datamaterialet er beskrevet detaljert i kapitlene 3.2 - 3.3. Resultatene fra undersøkelsen er fremstilt i kapittel 5. Intervjuguiden er presentert som vedlegg A i kapittel 8. Samlet sett bidrar fremstillingen i denne studien til å gi et troverdig bilde av undersøkelsens innretning og resultatene som er fremskaffet. Kravene til transparens som nevnt hos Silverman (2006); Thagaard (2013) ansees dermed tilfredsstilt.

3.5 Studiens validitet

Validitet er knyttet til spørsmålet om forskningens gyldighet (Thagaard, 2009), og i en kvalitativ studie handler om undersøkelsens troverdighet. Både Corbin og Strauss (2008, 2015); Silverman (2006) peker på troverdighet eller sannferdighet som et uttrykk for forskningens kvalitet. Corbin og Strauss (2015) diskuterer hva som menes med kvalitet i forskningen, noe som blant annet beskrives som at forskningen har substans, gir innsikt, viser sensitivitet og ikke bare repeterer de *"*samme gamle tingene*"* som kan leses i avisen. Corbin og Strauss (2015) foretrekker begrepet kredibilitet i kvalitativ forskning fremfor validitet og reliabilitet. I samfunnsvitenskap omhandler spørsmålet om validitet i samband med intervjuer ifølge Kvale (2007) hvorvidt undersøkelsesmetoden passer til formålet med undersøkelsen, mens en bredere fortolkning av validitetsbegrepet går ifølge Kvale et al. (1997); Kvale et al. (2009) ut på i hvilken utstrekning en metode undersøker det den er ment å undersøke. Thagaard (2009, 2013) kobler spørsmålet om validitet til forskningens gyldighet. I kvalitative studier er det også vanlig å snakke om overenstemmelse. Det er vanlig å skille mellom begrepsvaliditet som handler om spørsmålene som tas opp i undersøkelsen gjenspeiler begreper som brukes; intern validitet som

handler om hvorvidt det er støtte for resultatene opp mot innsamlet datagrunnlag; ekstern validitet handler om generalisering, altså om resultatene er overførbare til andre situasjoner.

Det første punktet om begrepsvaliditet omfatter kommunikasjon og fortolkning mellom informantene og forskeren. Yin (2014) trekker frem de tre strategiene: bruke flere beviskilder; etablere en beviskjede; få nøkkelinformantene til å gjennomgå utkast til rapport. Det er lagt stor vekt på å fange opp eventuelle uklarheter i intervjusituasjonen og sørge for å få utdypet hva informanten mener. For å unngå at misforståelser oppstår er det lagt vekt på å bruke kjente begreper i intervjuguiden, foruten definisjon av begreper det er vanskelig å finne gode synonymer for. For å verifisere at det er overenstemmelse mellom det informanten har ment og sagt under intervjuet, ble transkripsjonene som nevnt i kapittel 3.3 gjennomgått og godkjent av informantene. Det er forskerens vurdering at informantenes gjennomgang og stadfesting dermed styrker det empiriske grunnlaget for casestudien ved at informantene har kvalitetssikret transkripsjonene.

Det andre punktet om intern validitet gjelder forskerens fortolkning av det datamaterialet som er samlet inn. Intern validitet er ivaretatt dels gjennom bruk av verktøyet NVivo Pro 11 i analysen av transkripsjonene fra intervjuene, og dels ved at bearbeidingen av materialet fokuserte både på detaljert og overordnet nivå opp mot forskningsspørsmålene.

Det tredje punktet om generalisering er normalt vanskeligere å oppfylle fra en casestudie. Valget av tre virksomheter bidrar som nevnt om forskningsdesignet i kapittel 3.2 til å styrke funnene med tanke på overførbarhet til tilsvarende case. Det er ikke dermed sagt at det er mulig å generalisere resultatene fra studien, men snarere at det kan indikere mulige kilder til sammenfall innen tilstøtende områder. Sentrale kriterier i et konstruktivistisk paradigme er kredibilitet og overførbarhet.

Kvale et al. (2009) tilnærming er kvalitetskontroll gjennom alle stadier av kunnskapsproduksjonen fremfor å ta kontrollen i sluttfasen av prosjektet. Det er også en metode som er praktisert i denne casestudien, noe som dermed skulle sørge for god validitet i alle faser av forskningen. Når en vurderer om tolkninger som er basert på en enkelt undersøkelse også kan gjelde for andre situasjoner handler det om overførbarhet ifølge Thagaard (2013).

3.6 Avhandlingens struktur

Kapittel 1 inneholder overordnet beskrivelse av IKT-sikkerhetsarbeidet sett i et organisasjons- og samfunnsperspektiv, forskningsspørsmålene og til slutt definisjon av sentrale begreper. Kapittel 2 presenterer først de mest sentrale rammebetingelsene og beskriver deretter omfanget av casestudien. Kapittel 3 beskriver metodikken som er anvendt i casestudien og hvordan forskningsprosjektet er gjennomført. Kapittel 4 introduserer kort tidligere forskning av relevans, mens resten av kapitlet omhandler den teoretiske rammen som avgrenser omfanget av denne casestudien. Kapittel 5 inneholder resultatene fra den kvalitative intervjuundersøkelsen som deretter er analysert og drøftet i kapittel 6 mot teorien fra kapittel 4. Kapittel 7 presenterer konklusjonen fra dette forskningsprosjektet på bakgrunn av forskningsspørsmålene i kapittel 1.2, teorien i kapittel 4, resultatene i kapittel 5 og analysen og drøftingen i kapittel 6. Til slutt foreslås videre forskning innenfor dette emnet.

4 Teoretisk fundament

Valg av teori ble forankret i to forhold: for det første la det valgte temaet for casestudien føringer på valg av teorier; for det andre var de empiriske resultatene førende for det endelige valget av teorier. Som nevnt i kapittel 1 har IKT-sikkerhet blitt betraktet som et teknisk anliggende. Det er imidlertid økende erkjennelse for at sikkerhet i komplekse industrielle systemer må forstås innenfor andre rammer der både teknologiske, menneskelige og organisatoriske ifølge Schiefloe og Vikland (2007) er viktige. Sosio-tekniske teorier er derfor et sentralt utgangspunkt for å kunne forstå utfordringene i et MTO-perspektiv, og i kapittel 4.3 er det utdypet nærmere hvorfor teorien er relevant for IKT-sikkerhet. IKT-sikkerhetsarbeidet er underlagt omfattende regulering som omtalt i kapittel 2.1, og for å få bedre forståelse for hvordan bestemmelsene virker overfor individer, organisasjoner og i et samfunnsperspektiv er det nødvendig å kjenne til hovedprinsippene i reguleringsteorien. Siden samfunnsperspektivet er en del av denne casestudiens tilnærming, og flere studier som nevnt i kapittel 1 viser både økt avhengighet til IKT og økt kompleksitet i infrastrukturene er det naturlig å trekke inn teorier om samfunnssikkerhet i kritiske infrastrukturer. For å få bedre forståelse for de formelle og uformelle kvalitetene i virksomhetene er det nødvendig å trekke inn organisasjonsteorier. Alle forannevnte teorier anvendes ved hjelp av den generelle Pentagonmodellen i en systemteoretisk og handlingsteoretisk tilnærming gjennom å dekomponere den organisatoriske konteksten for deltakernes atferd (Schiefloe og Vikland, 2007:6).

I fortsettelsen presenteres først en kort oppsummering av tidligere forskning av relevans for denne casestudien i kapittel 4.1. Kapittel 4.2 fremstiller analyseverktøyet pentagon-modellen og organisatoriske forutsetninger for sikker drift. Kapittel 4.3 beskriver IKT-sikkerhet i et sosio-teknisk perspektiv. Kapitel 4.4. handler om reguleringsteorier. Kapittel 4.5 tar for seg samfunnssikkerhet og kritisk infrastruktur. Til slutt omtales organisering og ledelse av sikkerhetsarbeidet i kapittel 4.6.

4.1 Tidligere forskning

IKT-sikkerhet er et relativt ungt fagområde sammenliknet med safety-feltet. Mye av den tidligere forskningen som er gjort på IKT-sikkerhet har hatt et teknisk fokus ifølge Siponen og Oinas-Kukkonen (2007). Det er ikke gjort mange studier av IKT-sikkerhet i et safety-perspektiv, men det finnes noen: Albrechtsen (2008); Almklov et al. (2011); Skotnes (2015). Innen safety er det utviklet flere ulike teorier som på hver sin måte kan bidra til å gi interessante

perspektiver på forskningsspørsmålene i denne oppgaven. Det å belyse en problemstilling ved hjelp av flere perspektiver gir det et godt grunnlag for læring. Det er derfor nærliggende å bruke safety-teorier til å analysere, drøfte og forklare resultatene i denne undersøkelsen opp mot forskningsspørsmålene.

Studien i forbindelse med SAMRISK-prosjektets[9] problemstilling: *"Hva er konsekvensene av reorganiseringen av offentlig sektor (og funksjoner som tidligere var utført av offentlig sektor) for kritiske infrastrukturer og derav samfunnssikkerheten?"* av Almklov et al. (2011) omhandlet utfordringene i kraftsektoren, vannforsyning og IKT som følge av omstruktureringen og innføringen av styringsprinsippene New Public Management (NPM) og hvilke mulige konsekvenser det kunne ha for samfunnssikkerheten.

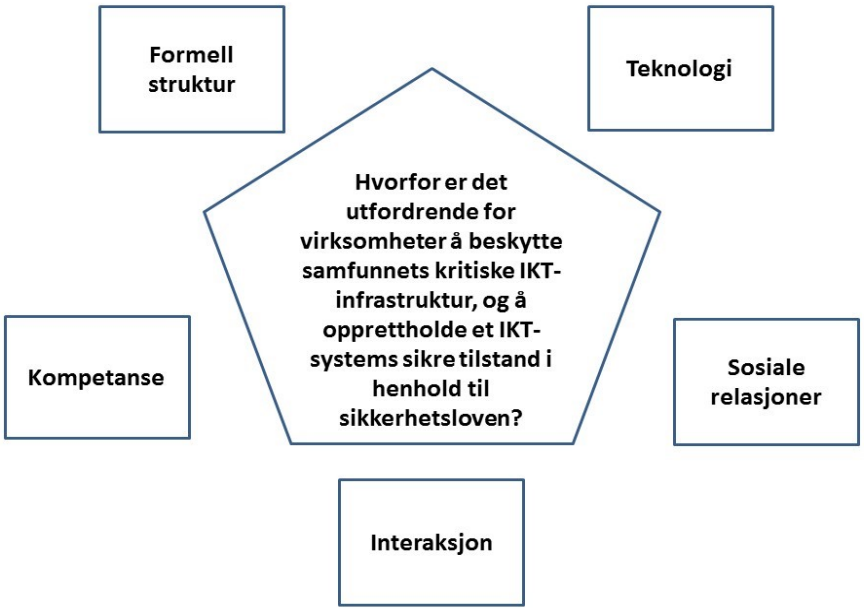
En videreføring av SAMRISK-prosjektet så nærmere på blant annet hvordan tilsyn og beredskapsmyndigheter skal forholde seg til at IKT har blitt en KI for andre kritiske infrastrukturer[10].

4.2 Pentagon-modellen og organisatoriske forutsetninger for sikker drift

Resultatene fra undersøkelsen er analysert ved hjelp av Pentagon-modellen som er utformet av Schiefloe (2013, 2014); Schiefloe og Vikland (2007). Pentagon-modellen er et fleksibelt og skalerbart verktøy som kan brukes til analyse både i et systemperspektiv, organisatorisk perspektiv eller individperspektiv. Verktøyet kan brukes både til innsamling, bearbeiding og analyse mellom ulike formelle- og uformelle faktorer og sammenhengen mellom disse, kategorisert som formell struktur, teknologi, kultur, interaksjon og sosiale relasjoner. Pentagon-modellen representerer altså et utvidet MTO perspektiv ifølge Almklov et al. (2011).

[9] Forskningsrådets program for Samfunnssikkerhet og risiko (SAMRISK) ble ferdigstilt i juni 2011. Det er igangsatt et nytt forskningsprogram ved navn SAMRISK II. Hentet 03.01.2017 fra http://www.forskningsradet.no/prognett-samrisk/Om_programmet/1228296552890

[10] Publisert i notatet *Offentlige etaters rolle i å sikre robusthet i komplekst organiserte og tett koblede infrastruktursektorer* fra NTNU Samfunnsforskning AS, September 2011. Hentet 07.01.2017 fra http://samforsk2.no/oer/docs/SluttrapportOER.pdf



Figur 3 Pentagon-modellen – hentet fra (Schiefloe og Vikland, 2006; Schiefloe, 2013, 2014)

Formell struktur handler om ansvar, myndighet og roller slik det er angitt i SL, forskrifter, veiledninger, retningslinjer for sikker konfigurasjon, jf. kapittel 2.1. IKT-systemer betraktes i NOU 2000: 24 (2000); NOU 2015: 13 (2015) som bærebjelker i samfunnet. Teknisk tilstand på IKT-plattformen er én faktor som påvirker mulighetsrommet for å opprettholde et IKT-systems sikre tilstand i henhold til SL, og de fire grunnsikringstiltakene[11] anbefalt av NSM er eksempelvis en viktig del av den forebyggende beskyttelsen både i graderte og ugraderte systemer. Sosiale relasjoner omhandler blant annet nettverkene i virksomhetene, organisasjonens sosiale kapital, makt, allianser, vennskap og konflikter. Slike relasjoner er viktige for å kunne skape tillit mellom partene eksempelvis i samband med sammenkobling av IKT-systemer mellom virksomheter, og det er viktig for å finne frem til gitte ressurspersoner ved hendelseshåndtering. Interaksjon omfatter kommunikasjon, samarbeid, utøvelse av ledelse og koordinering mellom flere parter. Det siste punktet om kompetanse er en delmengde av kultur som i Schiefloes modell som foruten kunnskap også omfatter språk, symboler, verdier/attributter, normer og arbeidsmåter. I denne studien er det et fokus på kompetanse, verdier og holdninger blant annet fordi SL fastsetter minimumskrav til kompetanse til ulike

[11] 1) Oppgrader program- og maskinvare, 2) Installer sikkerhetsoppdateringer så fort som mulig, 3) ikke tildel sluttbrukere administratorrettigheter, 4) blokker kjøring av ikke-autoriserte programmer, NSM. (udatert). *Fire tiltak stopper opp mot 90 prosent av dataangrep*. Hentet 17.12.2016 fra https://nsm.stat.no/virksomhetssikkerhet/fire-enkle-tiltak-stopper-90-prosent-av-dataangrep/

formelle roller og ansvar. Det betyr ikke at de øvrige momentene er mindre viktige, men kulturbegrepet favner såpass bredt at det ville by på utfordringer å dekke temaet tilfredsstillende innen rammen av denne casestudien. Denne studien berører likevel atferd til brukere.

Analysen vil formodentlig kunne si noe om virksomhetenes kapabiliteter (bruke: kapasitet), ytelse og sikkerhetskritisk adferd når det gjelder organisatoriske egenskaper for sikker drift.

Schiefloe (2011a) har på bakgrunn Reason (1990) energi-barriereperspektiv, Perrows (1999) normalulykkesperspektiv, Turners (1978) menneskeskapte katastrofer, LaPorte& Consolini (1991) høypålitelige organisasjoner og Hollnagel, Woods, og Leveson (2006) robusthet, laget en modell for organisatorisk sikkerhet. Ifølge Schiefloe (2011a) må de fem organisatoriske egenskapene pålitelig, sensitiv, proaktiv handlingsdyktighet, reaktiv handlingsdyktighet og evne til læring utvikles for at en organisasjon skal operere sikkert over tid. I (Almklov et al., 2011) CISS-prosjekt[12] ble infrastrukturenes robusthet undersøkt ved hjelp av tilsvarende modell for organisatorisk sikkerhet.

Figur 4 Organisatoriske egenskaper for sikker drift – hentet fra (Schiefloe, 2011)

[12] SAMRISK Critical infrastructures, public sector reorganization and societal safety (CISS). Hentet 07.01.2017 fra https://samforsk.no/Sider/Prosjekter/SAMRISK-Critical-Infrastructures,-Public-Sector-Reorganisation-and-Societal-Safety-(CISS).aspx

Det kan argumenteres for at virksomheter som skal forvalte sikkerhetsgodkjente IKT-systemer og levere over tid bør ha tilsvarende egenskaper. Drøftingen baseres derfor på Schiefloe (2011a) modell om organisatoriske egenskaper for sikker drift.

Virksomhetene og NSM må i sikkerhetsarbeidet forholde seg til lover og forskrifter, veiledninger, organisasjoner, mennesker, roller, teknologi, budsjetter, verdier, trusler og målkonflikter. Endringer i ett eller flere momenter kan ha konsekvenser for sikker IKT-drift i organisasjonen. Hendelser i den skarpe enden av organisasjonen er i mange tilfeller nokså fjernt fra beslutningstakere høyere opp i organisasjonen, også kjent som den butte enden av virksomheten som vist i figurene 5 og 7. Videre kan beslutninger som er tatt i andre forvaltningsnivåer ha utilsiktede eller uønskede virkninger i den skarpe enden av virksomheten. Det handler altså om forstå sammenhengene og samspillet mellom MTO. Det betyr at det er viktig, både for NSM og for virksomhetene, å forstå hvordan sikkerhetsbestemmelsene NSM er satt til å forvalte virker hos organisasjoner som er underlagt et slikt sikkerhetsregime. I samband med tilsyn anmodes virksomhetene selv å finne frem til underliggende årsaker til avvik. Det er fornuftig om regulator også lærer mer om hvorfor ulike former for svikt oppstår, noe som i neste omgang kan gi grunnlag for mulige endringer i enten rammebetingelser eller rådgivningstjenesten overfor virksomhetene.

4.3 IKT-sikkerhet i et sosio-teknisk perspektiv

IKT-sikkerhet er som nevnt i kapittel 1 tradisjonelt oppfattet som et teknisk anliggende, men denne studien har et bredere fokus hvor temaet er belyst i et MTO-perspektiv. Det er ifølge Albrechtsen (2008) viktige likhetstrekk mellom informasjonssikkerhet og industriell sikkerhet, noe som gjør erfaringsoverføring mulig ettersom begge omhandler skadeforebygging. Albrechtsen (2008) påpeker at industriell sikkerhet er et mer modent felt når det gjelder sosio-teknisk tilnærming og dermed gir bedre muligheter for læring. Teorigrunnlaget bør derfor også være et godt utgangspunkt for å besvare delspørsmål 3 om læring. Albrechtsen og Hovden (2007) kom frem til at sikkerhetsstyring av IKT fokuserte mest på tekniske barrierer, menneskelige feil og administrative prosedyrer, som svarer til de tre første av i alt fem utviklingstrinn innenfor industriell sikkerhet. Line og Albrechtsen (2016) fant at IKT-sikkerhetsstyring nå anvendte flere ideer fra det fjerde utviklingstrinnet innenfor industriell sikkerhet, som blant annet omfatter lederskap og ansvar, organisatoriske aspekter av

sikkerhetsarbeid, samt taksonomier med sikkerhetskultur som virkemidler for bedret sikkerhet. Sosio-tekniske teorier er derfor relevant i et IKT-sikkerhetsperspektiv.

Reason (1997a) fokuserer på organisatoriske ulykker og skiller mellom latente betingelser og aktive feil når han omtaler svikt i barrierefunksjonene. Aktive feil kan ifølge Reason (1997b) lede til uventede hendelser, mens latente betingelser trenger ikke føre til en umiddelbar ulykke. Det første forholdet kan skyldes operatørfeil i datasentralen, mens det andre forholdet kan ha sammenheng med dårlig designet IKT-system eller skadevare for å nevne noen eksempler. Reason (1997a) konstaterer at ulykker kan utvikles som følge av at barrierene ikke er intakte, ettersom barrierer og beskyttelsesmekanismer kan forvitre over tid på grunn av at en eller flere barrierer er fjernet som følge av redesign, vedlikehold, testing, feil, brudd eller tilsvarende.

Ifølge Perrow (1984) normalulykkesperspektiv (NAT) er enkelte ulykker praktisk talt uunngåelige på grunn av strukturelle egenskaper i visse systemer, og de kan inntreffe overraskende på folk. Mindre hendelser er etter Perrow (1984) syn typisk forårsaket av feil på en eller to komponenter i et system uten at det leder til uventet gjensidig påvirkning. Det er langt på vei mulig å beregne sannsynligheten for ulykker som følge av komponentsvikt gjennom risikoanalyse. Vanskeligere er det å forutse systemulykker ettersom de omfatter gjensidig påvirkning av en rekke latente og aktive feil i et komplekst system. Det er enda vanskeligere å kontrollere et system med høy interaktiv kompleksitet som eksempelvis et kjernekraftverk eller komplekse IKT-systemer. Det oppstår et dilemma i systemer med høy interaktiv kompleksitet og tette koblinger, ettersom det første krever desentralisert ansvar og myndighet, mens det andre forholdet krever sentralisert styring. Begge forholdene kan ikke realiseres samtidig, og et alternativ er å unngå å etablere systemer med høy interaktiv kompleksitet og tette koblinger. Lineære barrieremodeller fanger ikke opp kompleksitet, noe som gjør at ulykker kommer overraskende på folk og dermed vanskeliggjør forberedelser på denne type hendelser.

En kritikk mot NAT er at det i praksis er vanskelig å finne organisatoriske årsaker til svikt i lineære systemer. Begrepsbruk "*interaktiv kompleksitet*" og *"tette koblinger*" betraktes ifølge Rosness et al. (2010) som vag; det er vanskelig å måle *"interaktiv kompleksitet*" eller *"desentralisering*"; for pessimistiske forslag å kassere komplekse teknologier som blant annet kjernekraftverk; påstanden om at en organisasjon ikke kan være sentralisert og desentralisert samtidig som unødvendig repetisjon; noen kritikere antar NAT er relevant kun for systemer kjennetegnet med ekstremt interaktiv kompleksitet og tette koplinger.

Turner (1978) fremhever betydningen av informasjonssvikt eller feiltolkning av informasjon fra sin studie av en rekke alvorlige ulykker betraktet som menneskeskapte kriser. Turner (1978) modell omfatter seks trinn fra antatt normalsituasjon, inkubasjonsperioden, utløsende hendelse, begynnende krise, krisehåndtering og til slutt gjenoppretting av kontroll. Det er prosessene forut for ulykken som representerer viktige forutsetninger i teorien. I følge Turner (1978), Turner og Pidgeon (1997), Pidgeon og O'Leary (2000) er det et paradoks at ulykker gjennomgående oppfattes som en overraskelse på involverte organisasjoner og media, mens etterpåklokskap gjerne avdekker at eksistensen av tidlige signaler og varsler ikke ble fanget opp eller forstått av involverte parter før hendelsen. Betegnelsen organisatoriske ulykker brukes gjerne om denne typen ulykker. Detaljerte funn fra revisjonsprosessen bør ifølge Turner og Pidgeon (1997) sammenstilles for å bedømme hvordan informasjon relatert til sårbarheter blir håndtert i organisasjonen. Forfatterne vektlegger også sikkerhetskultur som en nøkkelfaktor for å ta tak i og kontinuerlig overvåke risiko, samt organisatorisk læring som hjelp til å bedre risikoforståelsen blant personell og med det overvinne dårlig tiltro, normer og informasjonsflyt i organisasjonen. Begge forholdene nevnt foran kan sies å fokusere på forbedringer av eksisterende praksiser. Noen ganger kan det imidlertid være fornuftig å stille spørsmål om de riktige målene er i fokus, noe som da ifølge Argyris og Schön (1996) kan betegnes som dobbeltkretslæring. Et eksempel på det siste er spørsmålet om virksomheten har tatt i bruk de riktige tiltakene for å sikre IKT-driften med hensyn på pålitelighet, sensitivitet, samt proaktiv og reaktiv handlingsdyktighet i daglige operasjoner som vist i Figur 4.

I Turner (1978) modell beskrives fire former for informasjonssvikt: fullstendig ukjent informasjon; Tilgjengelig informasjon blir ikke tatt hensyn til, noe som kan skyldes høyt arbeidspress eller sikkerhetsnivået oppfattes som godt nok tross manglende realisme; eksisterende informasjonselementer blir ikke kombinert og satt i sammenheng; tilgjengelig informasjon blir mistolket eller neglisjert ettersom det ikke samsvarer med rådende fortolkningsrammer.

Akkumulering av mer data per se forhindrer ikke ulykker. Det er derfor nødvendig å fokusere på prosessene der informasjon blir satt sammen og fortolket. En rekke komponenter i IKT-systemer kan settes opp til å loggføre mange ulike hendelser etc. når det gjelder sikkerhet, både viktige og mindre viktige. Samlet sett blir det store datamengder pr dag, uke, måned og år. For å lette arbeidet med innsamling, sammenstilling og fortolkning av data eksisterer det en rekke

administrative verktøy kalt *Security Incident Event Management* (SIEM). For at slikt verktøy skal gi noen mening, må man vite hva man skal se etter og filtrere bort støy.

En kritikk mot informasjonsperspektivet er at advarsler om opptrappende hendelser og kommunikasjonsproblemer sees i retrospekt. En grunn til det vurderer Turner (1978) kan være at biter av informasjon eller tidlige signaler om hendelser er forsvunnet i mengden av informasjon. Den kanskje største innvendingen mot informasjonsperspektivet er det Rosness et al. (2010) nevner om utfordringen når det gjelder å vise at påstander er meningsfulle og gyldige overfor aktører som ikke sitter med de fordelene etterpåklokskap gir, eller for å låne uttrykket til sårbarhetsutvalget: "… en viktig side av arbeidet med sikkerhet og beredskap er å bli mer "etterpåkloke på forhånd". Utfordringene er betydelige" NOU 2000: 24 (2000:5).

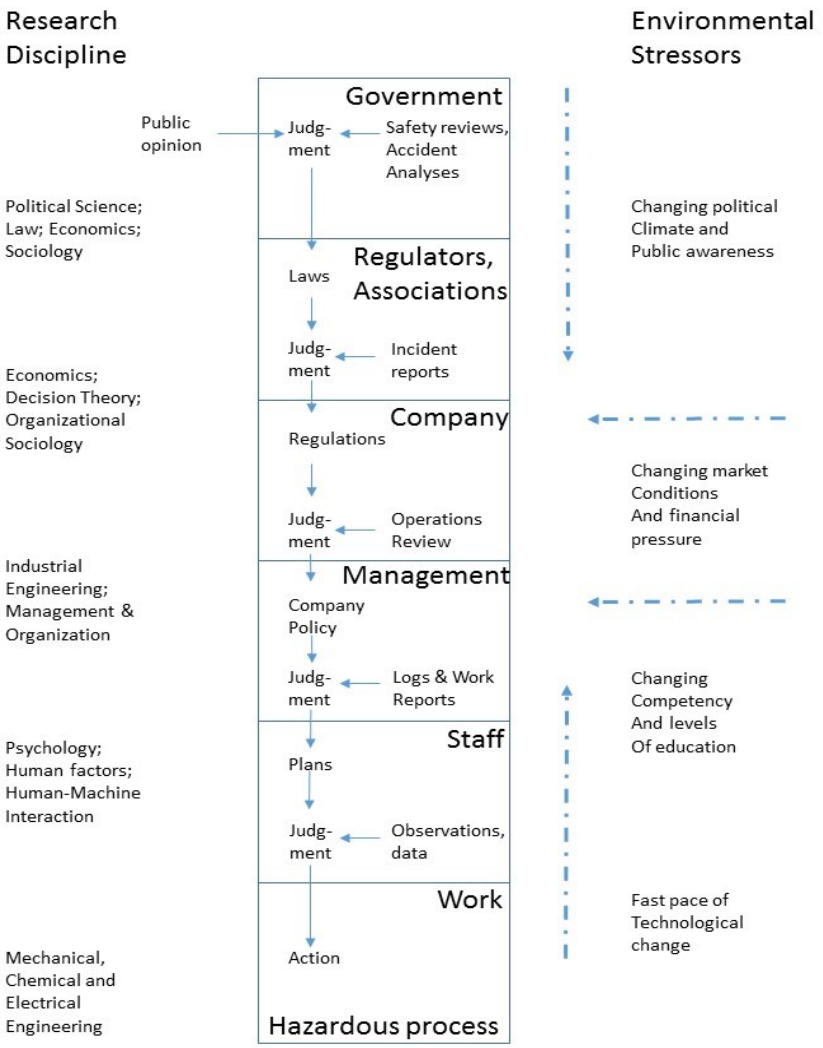
Det er en lang kjede av beslutningstakere fra politisk nivå, ulike forvaltningsnivåer, virksomheter, ledelse, til operativt nivå hvor oppgavene faktisk blir utført. Figur 5 illustrerer i den hierarkiske strukturen i Rasmussen (1997) modell for sikkerhet og risikostyring i et sosio-teknisk system. Det betyr at vi da kan få det Rasmussen (1997) omtaler som en lite dynamisk modell med ovenfra og ned kommandokjede, der høyere myndighet fastsetter bestemmelser. Forslag til lov eller forskrift skal blant annet i henhold til utredningsinstruksen[13] alltid forelegges berørte departementer. I følge Rasmussen (1997) settes bestemmelsene ut i praksis gjennom blant annet fortolkninger hos lavere myndighetsnivå som vist i nedre del av figuren, noe som både påvirker arbeidsprosesser og har konsekvenser for økonomien som følge av anskaffelser av utstyr. Risiko kan i et slik perspektiv som Rasmussen (1997) vurderer, forstås og oppfattes på en annen måte av lovgiverne på høyeste beslutningsnivå, ofte omtalt som *"blunt end*", enn eksempelvis IKT-driftspersonell som har det praktiske arbeidet med å beskytte virksomhetens informasjon. Operativt personell befinner seg i det området Rasmussen (1997) kaller *"sharp end*". Figur 7 viser hvordan begrepene skal forstås. Eksterne faktorer er blant annet et skiftende trusselbilde med terror, spionasje, sårbarheter i program- og maskinvare og hyppige teknologiske endringer, noe som dermed utfordrer en slik kommando- og kontrollkjede når det gjelder tilpasninger og evne til rask respons. En utfordring for regulerende myndigheter er dermed å finne passende virkemidler for IKT-sikkerhet på tvers av ulike bransjer innen et felt preget av stor dynamikk, hyppige teknologiske skift, endringer i trusselbildet og

[13]Finansdepartementet. (2016). *Instruks om utredning av statlige tiltak (utredningsinstruksen)* Hentet 13.01.2017 fra https://lovdata.no/dokument/INS/forskrift/2016-02-19-184?q=utredningsinstruksen

teknologifikserte brukere. NSMs veiledninger som ble omtalt i kapittel 2.1 åpner for hurtigere tilpasning til endrede betingelser enn det som er mulig i kommando- og kontrollkjede. Reguleringsteorier behandles nærmere i kapittel 4.4. Leverandørenes strategiske beslutninger om design, utviklingspraksis og kvalitetskontroll er andre eksterne faktorer som har innvirkning på virksomhetenes organisering og håndtering av sikkerhetsarbeidet.

Kompetanse og utdanningsnivå er en ekstern faktor av betydning for å kunne møte endringer i omgivelsene

Rasmussens (1997) modell i Figur 5 illustrerer også tilbakekoblingssløyfer nedenfra og opp. Det er viktig at erfaringer fra operativ anvendelse av rammebetingelsene kommer høyere myndighetsnivåer til kunnskap, ettersom det først og fremst er operativt ledd som møter utfordringene med hurtige skift, nye teknologier og nye trusler.

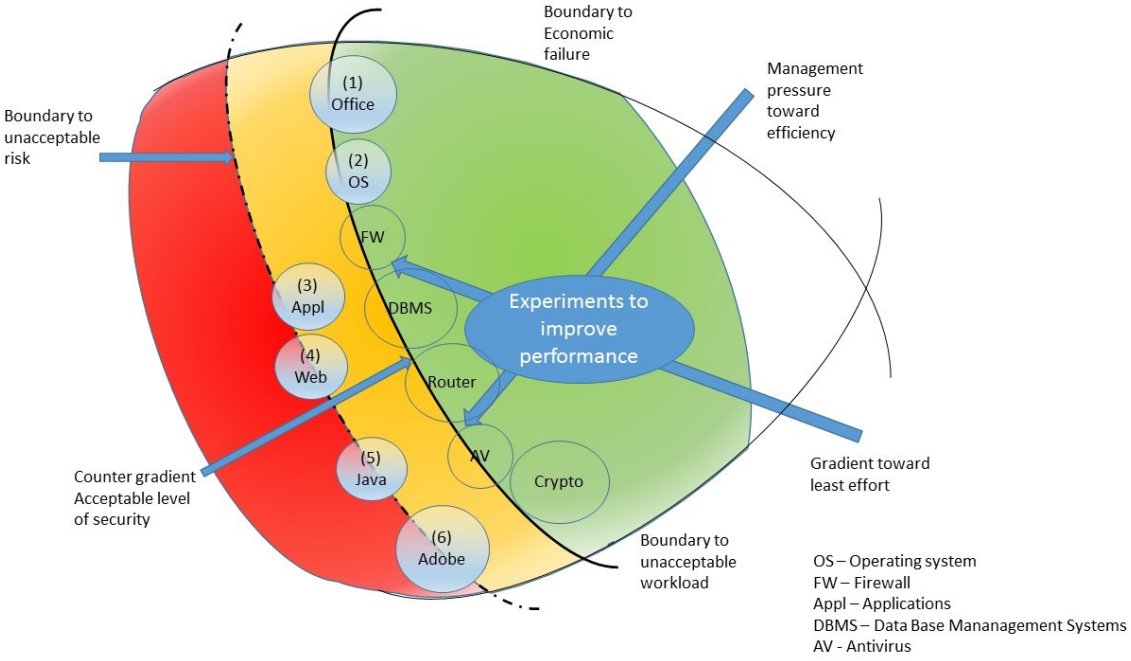


Figur 5 Sikkerhet og risikostyring i sosio-teknisk system - hentet fra Rasmussen (1997)

Det kan dermed oppstå målkonflikter i forhold til arbeidsbelastning, effektivitet og risiko, se Figur 6. Rasmussen (1997) foreslår å se på målkonfliktene som aktiviteter som flyttes mot grensen for akseptabel ytelse. De tre grensene definerer dermed handlingsrommet for effektivitet, kvalitet og sikkerhet. Rasmussen (1997) bruker også begrepet *"Practical drift"* når aktivitetene gradvis opererer mer usikkert eller som Snook (2000) omtaler som at man sakte men sikkert beveger seg lengre vekk fra skrevne prosedyrer. Behandling av sikkerhetsgradert informasjon er underlagt preskriptive bestemmelser som omtalt i kapittel 4.4. Krav til sikkerhetsbarrierer kan dermed komme i konflikt med leveranser, resultatkrav og økonomiske rammer. Behovet for kompetanse vil dermed, gitt stram økonomi, utfordre tekniske- og

organisatoriske barrierer ytterligere. De tekniske barrierene og annen standard programvare som vist i Figur 6 installeres, konfigureres, driftes- og vedlikeholdes av spesialiserte individer eller grupper som ikke nødvendigvis har bred oversikt på andre områder. Programvare som representerer en forholdsvis stor angrepsflate er i Figur 6 illustrert på grensen for uakseptabel risiko, mens produkter som har bedre designede sikkerhetsfunksjoner og i større grad kan herdes er lagt på grensen for akseptabelt sikkerhetsnivå. Hvilken risiko som er knyttet til produktene vil kunne variere over tid og med grad av herding, samt med hvilke andre tekniske eller administrative sikkerhetstiltak som tas i bruk. Krypto er plassert innenfor akseptabelt sikkerhetsnivå, og ettersom en rekke krav må være oppfylt for å få godkjent en kryptoinstallasjon betyr det også at det er lagt større innsats i å få frem et sikkerhetsmessig robust produkt. Det er derfor grunn til å ha høyere grad av tillit til et produkt som er designet og implementert i tråd med anbefalt eller beste praksis på feltet. Teknologiområdene som er nummerert fra 1 - 6 i Figur 6 representerer hovedsakelig NSMs fire anbefalte tiltak[14] i programvare for å stoppe potensielle angrep, mens oppdatering av maskinvare omfatter både skraverte og ikke-skraverte områder. Figur 6 tar ikke hensyn til teknologiområdenes plassering langs grensene for økonomiske svikt eller uakseptabel arbeidsbelastning.

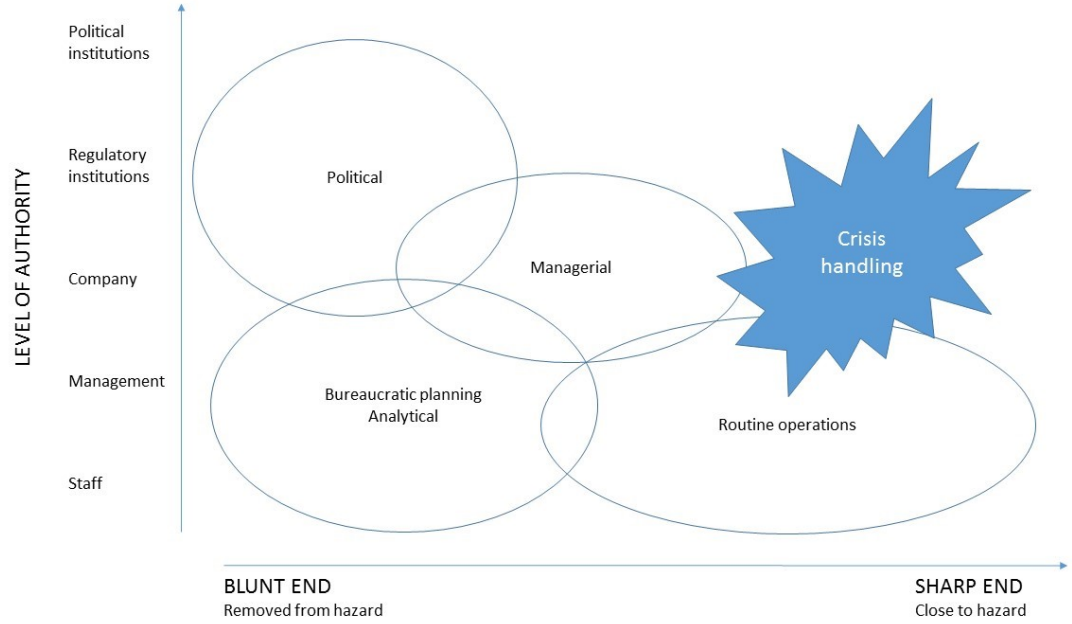
[14] NSM. (udatert). *Fire tiltak stopper opp mot 90 prosent av dataangrep*. Hentet 17.12.2016 fra https://nsm.stat.no/virksomhetssikkerhet/fire-enkle-tiltak-stopper-90-prosent-av-dataangrep/



Figur 6 Målkonflikter - modifisert figur - hentet fra Rasmussen (1997)

Beslutningsprosessene som ble fremstilt i Figur 5 inngår i Figur 7 nedenfor som er hentet fra Rosness (2001). NOU 2015: 13 (2015) beskriver 10 sentrale aktører[15] med oppfølgingsansvar for IKT-sikkerhet i tillegg til fylkesmannen og kommunene. Modellen illustrerer spennvidden mellom den butte enden (*"blunt end"*) av organisasjonen hvor de mer overordnede beslutningene fattes til den spisse enden (*"sharp end"*) av virksomheten hvor mer eller mindre rutinepregede oppgaver som eksempelvis drift- og vedlikehold utføres. Det er derfor den spisse enden av organisasjonen som vanligvis er de første til å håndtere ulike typer IKT-hendelser.

[15] Statsministerens kontor; Justis- og beredskapsdepartementet; Forsvarsdepartementet; Utenriksdepartementet; Samferdselsdepartementet; Kommunal- og moderniseringsdepartementet; Nasjonal sikkerhetsmyndighet; Direktoratet for samfunnssikkerhet og beredskap; Direktoratet for forvaltning og IKT; Datatilsynet.



Figur 7 Forholdet mellom målkonflikter og sikkerhet - hentet fra Rosness (2001)

NSM utgir regelverk for sikkerhetsgraderte IKT-systemer, og har myndighet til å ilegge virksomheter/virksomhetsledere sanksjoner dersom reglene ikke følges. Politisk behandling og utforming av rammebetingelser skjer langt fra det operative miljøet, mens personell i den skarpe enden av organisasjonen skal følge bestemmelsene. I følge Rosness (2001) må en forvente at operatører har mer oppdatert og detaljert førstehåndskunnskap om systemet som skal driftes enn aktører i den "butte enden". Rosness (2001) forventer derfor at beslutningskriteriene, prosedyrer og resultater er relatert til a) hvor nært en aktør eller et beslutningsforum befinner seg i forhold til faren (risikoen) og b) hvilken autoritet aktøren eller forumet har.

Regjeringens sikkerhetsutvalg (RSU) vil typisk håndtere hendelser som IKT-angrep med nasjonale konsekvenser NOU 2015: 13 (2015).

4.4 Reguleringsteorier

Bruken av harde eller myke[16] virkemidler for å regulere IKT-sikkerhet er forbundet med ulike fordeler og ulemper. Kapittel 2.1 beskriver prinsippene for dagens ordning og hvilke hierarkier

[16] Kommando og kontroll regulering betegnes også som "harde" virkemidler. Motsatsen til kommando og kontroll regulering er selvregulering, også kategorisert som "myk" regulering ifølge Lindøe og Engen (2013).

som gjelder i rammebetingelsene fra NSM vedrørende FoI, FoO samt øvrige relevante forskrifter som berører arbeidet med informasjonssikkerhet.

Ved eventuelle brudd på SL og underliggende bestemmelser risikerer den regulerte part straff og sanksjoner dersom bestemmelsene ikke etterleves. Denne typen hard regulering er ifølge Lindøe og Engen (2013) også kjent som kommando og kontroll med detaljerte preskriptive lover og reguleringer, og det representerer en asymmetri mellom regulator og regulerende part.

> Command and control regulation is invariably presented as a compulsory form of government intervention. Government literally *commands* industry to meet specific environmental standards, either directly through legislation or indirectly through delegated authority, and *controls* its behaviour through the threat of negative sanctions. (Sinclair, 1997:534)

"Within a command and control regime, prescriptive rules will be legally binding to all safety elements" (Lindøe og Engen, 2013:201).

Detaljert regulering av et dynamisk felt som IKT-sikkerhet er både utfordrende og ressurskrevende, likeså er tilsynsoppgavene. Hyppige teknologiske skift kan være krevende å følge opp i tide for myndigheten med nye detaljerte reguleringer, ettersom det kreves mye FoU-rettet forarbeid.
Mange detaljerte krav kan på den ene side by på utfordringer for virksomheter som er underlagt bestemmelsene, men kan på den annen side muligens også være et bra hjelpemiddel for å organisere arbeidet i virksomhetene.

Motsatsen til kommando og kontroll er selvregulering, også kjent som myk regulering ifølge Lindøe og Engen (2013), noe som karakteriseres ved ytelses og risikobasert regulering. Ideen er at virksomhetene selv definerer hvilke tiltak som er de rette til å oppfylle formålet ifølge Lindøe og Engen (2013). Meningen er da at tiltakene kan tilpasses type virksomhet. Det innebærer altså at virksomhetene selv utfører internkontroll og iverksetter tiltak for å oppfylle intensjonene.

FoI kan etter dette betraktes som preskriptive krav med innslag av selvregulering, mens FoO fremstår som selvregulerende med funksjonelle krav. Årsaken til det første er dels kravet om egne risikovurderinger, og dels meldeplikten til regulerende myndighet dersom virksomheten planlegger eller har gjennomført vesentlige endringer i sikkerhetsgodkjente systemer.

Kritikken mot kommando og kontrollregulering er ifølge Sinclair (1997) høye kostnader; ineffektivt; hemmer innovasjon; inviterer til å fremtvinge vanskeligheter; fokuserer på *"end-of-pipe"* løsninger. Kommando og kontrollprinsippet gir ifølge Sinclair (1997) ikke incentiver til å gjøre flere forbedringer enn å tilfredsstille spesifiserte minimumskrav, og i de fleste tilfellene vil hverken selv-regulering eller kommando-kontroll være den foretrukne løsningen.

> By contrast, in a purpose and performance regime, the use of legal-binding norms are minimized but connected by legal standards to relevant and applicable technical standards. In practice the challenges will be to find the balance between the two extremes. (Lindøe og Engen, 2013:201)

4.5 Samfunnssikkerhet og kritisk infrastruktur

Virksomhetene i denne casestudien er som nevnt i kapittel 2.2 enten en del av KI og/eller leverer samfunnskritiske tjenester. Fellestrekkene for virksomhetene A, B og C er viktigheten av en velfungerende IKT-plattform som sikkerhetsmessig er ivaretatt i henhold til definerte behov og gitte krav. Egan (2007) mener økt teknologiavhengighet også betyr flere *"*kritisk infrastruktur-liknende*"* teknologier. En velfungerende IKT-infrastruktur eller stabile tjenesteleveranser forutsetter blant annet intakt strømforsyning. Almklov et al. (2011) vurderer pålitelig leveranse av el-kraft er avgjørende for samfunnssikkerhet, noe som også er årsaken til benevnelsen KI for kraftsektorens del.

Et forhold som gjør at sikkerhetsmodellen på samfunnsnivå blir mer komplisert enn på organisasjonsnivå, er at de fleste elementene i modellen forutsetter koordinering mellom ulike offentlige etater og organisasjoner, og at slik koordinering alltid er vanskelig å få til (Schiefloe, 2011a).

Virksomhetene i dette casestudiet er dels tjenesteytere i egen organisasjon og dels til andre organisasjoner, noe som kan innebære både teknologiske, organisatoriske, mellommenneskelige utfordringer eller det kan oppstå ulike hendelser. Ifølge Kruke (2012) må ett eller flere av følgende kriterier være oppfylt for å kunne si at hendelsen truer samfunnssikkerheten:

- Ekstraordinære påkjenninger og tap
- Kompleksitet og gjensidig avhengighet
- Tillit til vitale samfunnsfunksjoner

4.6 Organisering og ledelse av sikkerhetsarbeidet

Rammevilkårene fra sikkerhetsmyndigheten legger store føringer på hvordan virksomhetene skal organisere og lede sikkerhetsarbeidet. Blant annet er det krav til egen sikkerhetsorganisasjon med sikkerhetsleder, datasikkerhetsleder og eventuelt ansvarlige for krypto dersom virksomheten benytter det. Vi kan karakterisere organisasjonsformen knyttet til sikkerhetsarbeidet som byråkratisk. Ifølge Mintzberg (1983) handler byråkratiet om formalisering av atferd for å oppnå koordinering. Clegg, Kornberger, og Pitsis (2011) definerer byråkrati som en organisasjonsform bestående av hierarkier av differensiert kunnskap og ekspertise hvor regler og disipliner er avtalt ikke bare hierarkisk i forhold til hverandre, men også i parallell. Som vist i kapittel 2.1 er sikkerhetsmyndighetens rammevilkår omfattende.

Samtidig fordrer sikkerhetsarbeidet i virksomhetene kompetente medarbeidere som skal forholde seg til hyppige teknologiske endringer og skiftende trusselbilde, noe som kan være utfordrende i en byråkratisk organisasjon der arbeidet i stor grad koordineres gjennom rutiner og regler. Ledelse beskriver Clegg et al. (2011) som en prosess med å kommunisere, koordinere og ferdigstille oppgaver i bestrebelsene med å nå organisasjonens mål, mens man samtidig ivaretar forbindelsene med interessenter, teknologier og andre artefakter, både innenfor så vel som utenfor organisasjonen.

Organiseringen og styringsmekanismene i offentlig sektor preges av ideer fra privat sektor som *New Public Management* (NPM) som blant annet omfatter balansert målstyring og revisjoner, noe som i denne sammenheng er relevant siden majoriteten av virksomheter underlagt SL er en del av offentlig sektor. En viktig driver for endringene i styring og ledelse av offentlig sektor var ifølge Clegg et al. (2011) mer effektivitet og bekymringer for transaksjonskostnader, og man mente NPM kunne implementeres på tvers av sektorene med inkrementelle justeringer. Et annet forhold er at NPM innebærer en annen måte å koordinere aktiviteter på enn tradisjonell ledelse hvor Mintzberg (1983) definerer koordinering som å samordning av aktiviteter ved fem ulike måter: gjensidig tilpasning; direkte tilsyn; standardisering av arbeidsprosesser; standardisering av kunnskap; standardisering av resultater.

Transparens og etterprøvbart ansvar er ifølge Almklov et al. (2011) argumenter for NPM. Andre typiske trekk ved NPM har Almklov and Antonsen (2010) definert som modularisering av organisasjoner og kommodifisering av arbeidsoppgaver. En variant av NPM er bestiller-utfører-modell (BUM) beskriver Almklov et al. (2011) som mer forretningsmessige grenser mellom de

som bestiller og utførende ledd. Virksomhetene i denne casestudien er organisert slik som vist i kapittel 2.2, men det er ikke undersøkt hvorvidt man faktisk driver med internfakturering. Veiledningene under FoI anbefaler eksempelvis å bruke ITIL for organisering av driften, noe som kan sies å innebære det Almklov, Antonsen, og Fenstad (2010) omtaler som standardisering av arbeidsprosessene. Sikkerhetsgodkjenninger, som er gebyrbelagt, kan sies å tilhøre samme kategori.

Desentraliseringer og måleparametere som balansert målstyring i NPM står på mange måter i motstrid med den samhandling som virksomhetene gjerne oppfordrer til. Det er spesielt de fire barrierene Hansen (2009) omtaler som: *"not invented-here*"; *"hoarding*"; *"search problems*"; *"transfer problems*". Barrierene handler ifølge Hansen (2009) henholdsvis om: uvilje mot å gå ut over egen gruppe for å få synspunkter og hjelp fra andre; uvilje mot å hjelpe andre og dele kunnskap og erfaring; vanskelig å finne relevant informasjon og riktige personer; folk strever med å formidle informasjon fra en enhet/person til en annen, og én enkelt barriere er nok til å hindre godt samarbeid. Disiplinert samarbeid beskriver Hansen (2009) som vurdering av hvorvidt samarbeid er hensiktsmessig og det å utvikle vilje og evne til samarbeid når det trengs. Han beskriver videre hvordan man kan: evaluere mulighetene; identifisere barrierene; implementere løsningene. Virksomhetene i denne casestudien hadde behov for både intraorganisatorisk, interorganisatorisk samhandling nasjonalt og internasjonalt.

Som nevnt tidligere innebærer IKT-sikkerhetsarbeidet at virksomhetene må forholde seg til blant annet hyppigere teknologiske skift enn i andre infrastrukturer. Det gjør at organisasjonen må være rustet for å takle flere hyppige endringer og gjøre tilpasninger. Det er ikke nødvendigvis bare teknologiske konsekvenser å innføre noe nytt i virksomheten. Å tilfredsstille sikkerhetsmål kan betraktes som å skape endringer, og de enkelte utfordringene kan slik sett også forstås på tilsvarende måte som organisasjonsendringer. En grunn til det er endringene som må skapes for å utvikle organisasjonen fra en tilstand hvor sikkerhet ikke er på et tilfredsstillende nivå til et akseptabelt nivå. For å bringe sikkerhetsinnsatsen fra god til bedre tilstand foreslår Hagen, Albrechtsen, og Hovden (2008) at informasjonssikkerhet fokuserer på den menneskelige faktor. Et annet forhold poengtert av Almklov et al. (2011) som sammenligner den fysiske infrastrukturen og utbyttbarheten IKT med andre typer KI, og viser til at der andre kritiske infrastrukturer er preget av lav utskiftningshastighet og lange investeringshorisonter (ledningsnett for framføring av vann og strøm, veinett) er det både økonomisk og teknisk mulig å skifte ut komponenter i IKT-infrastrukturen. NSMs krav for

informasjonssikkerhet har lagt til rette for utskifting av komponenter i IKT-systemene gjennom modulbaserte krav. Virksomhetene i denne casestudien benyttet enten standardiserte IKT-komponenter og/eller skreddersøm.

Meyer og Stensaker (2011) diskuterer blant annet virksomhetenes utfordringer og kapasitet i forbindelse med store omorganiseringer, omstillinger og endringer. Temaet er relevant i denne casestudien ettersom flere av virksomhetene blant annet pekte på ressursmessige utfordringer ved innføring nye systemer. Innføring av eller utvidelser av IKT-systemer innebærer endringer som påvirker organisasjonens leveranseevne.

5 Resultater

Resultatene i denne casestudien bygger på en kvalitativ intervjuundersøkelse blant 13 informanter fordelt på tre ulike virksomheter. Formålet med studien var å finne svar på forskningsspørsmålet: *"Hvorfor det er utfordrende for virksomheter å beskytte samfunnets kritiske IKT-infrastruktur og å opprettholde et IKT-systems sikre tilstand i henhold til sikkerhetsloven.*" En naturlig innfallsvinkel for å besvare forskningsspørsmålet var da å se nærmere på virksomhetenes oppfatninger av IKT-sikkerhetskravene, virkninger av kravene og tiltakene i lys av NSMs intensjoner om å beskytte samfunnets kritiske IKT-infrastruktur, samt finne læringspunkter for både virksomhetene og NSM. I intervjuguiden omtalt i kapitlene 3.1, 3.3, 3.4 og 3.5, ble forskningsspørsmålene dekomponert ytterligere for blant annet å få frem flere perspektiver på problemstillingene som er reist her. Hovedfunnene fra denne studien er primært strukturert ut i fra intervjuguidens oppbygning, og resultatene er presentert i kapitlene 5.1 - 5.3.

5.1 Virksomhetenes oppfatninger av sikkerhetskravene

Flertallet av informantene oppfattet generelt IKT-sikkerhetskravene under SL som relevante og legitime, og de fleste virksomhetene sa de prøvde å etterleve kravene så godt som mulig. Kravene var gode og ofte nødvendige å vise til for å få truffet beslutninger om sikkerhetstiltak og investeringer, mens fravær av krav kunne resultere i at sikkerhet ble ignorert. Noen informanter mente kravene i SL også var relevante for ugraderte systemer. En informant var usikker på om veiledningene skulle oppfattes som krav eller ikke.

Det var imidlertid noen nyanser i svarene ettersom syv informanter mente kravene enten var for strenge, for gammeldagse eller for lite fleksible og skalerbare. Årsakene ble forklart slik:

- for store likheter mellom kravene for høygraderte og lavgraderte systemer, noe som ble oppfattet som både krevende og strengt for lavgraderte systemer;
- at kravene ikke var i takt med teknologiutviklingen som eksempelvis virtualisering og nyeste Windowsversjoner;
- at regelverket ikke understøttet økte krav til mobilitet.

En informant mente SL ikke var tilpasset dagens praksis der virksomheten stod i en kunderelasjon med leveranse av driftstjenester, fordi det da ble oppfattet som noe uklart hvem som hadde ansvaret for å ivareta enkelte av sikkerhetskravene.

Flere informanter pekte på at virksomhetene også var underlagt mange sikkerhetskrav gjennom flere andre lovverk, i tillegg til standarden ISO/IEC 27001. Tre informanter oppfattet SL som den enkleste å forholde seg til på grunn av flere konkrete krav sammenliknet med sikkerhetskrav i øvrige regelverk. Et par informanter trakk frem mulighetene for mer tolkningsrom i andre lovbestemmelser som blant annet personopplysningsloven og sektorreglene.

5.1.1 Virkningen av kravene ift beskyttelse av samfunnets kritiske IKT-infrastruktur

Halvparten av informantene fordelt på alle virksomhetene mente kravene hadde bidratt til enten bedring, fungerte etter hensikten eller var et bra hjelpemiddel til beskyttelse av samfunnets kritiske IKT-infrastruktur, mens den andre halvparten hadde litt mer nyansert og kritisk syn.

En informant syntes ikke arbeidet var godt nok, men mente de tre sikkerhetstjenestene og andre parter bidro til at det fikk fokus hos maktapparatet. Kravene i FoO og en påfølgende ROS-analyse[17] bidro ifølge en informant til nok politisk oppmerksomhet til å kunne sikre objekter på en bedre måte.

En informant pekte på paradokset med at virksomhetens IKT-infrastruktur på den ene side ble regnet som ganske samfunnskritisk og på den annen side var ugradert. En annen informant rapporterte at virksomhetens informasjonssystem i sin tid ble vurdert innmeldt i henhold til FoO, men ifølge NSM var selve informasjonssystemet ikke å betrakte som et objekt.

En virksomhet manglet gode verktøy å kunne ta imot og behandle informasjon på tvers av landegrensene. Bakgrunnen var at politikerne vedtok å endre behandlingsreglene på den ene siden av grensen før samarbeidende part hadde fått på plass egnede løsninger. Det var på tidspunktet for intervjuet uklart hvordan virksomheten skulle forholde seg til endringene og

[17] Med ROS-analyse menes risiko- og sårbarhetsanalyse. NSM og NTNU har i samarbeid utviklet en fem-trinnsmodell som er beskrevet i NSMs veileder i risiko- og sårbarhetsanalyse for virksomheter underlagt SL. NTNU. (udatert). *Risikoanalyse. Teori og metoder*. Hentet 12.01.2017 fra http://frigg.ivt.ntnu.no/ross/slides/risikoanalyse/kap16_ROS.pdf; Rausand og Utne (2009), *Risikoanalyse: Teori og metoder*, Tapir akademisk forlag, Trondheim, ISBN: 9788251924467

hvordan man skulle løse saken. Informanten mente NSM burde vært mer på tilbydersiden i denne typen saker.

En informant mente det forebyggende arbeidet ikke fungerte for tiden og at man ikke gjorde noe med mindre man var nødt, eksempelvis som følge av hendelser med konsekvenser. Informanten mente årsaken var at SL ikke ble fulgt.

5.2 Virksomhetenes praksis for å beskytte samfunnets kritiske IKT-infrastruktur og årsaker til utfordringer

I kapitlene 5.2.1 - 5.2.11 presenteres årsaker til utfordringene fra den kvalitative intervjuundersøkelsen hos de tre virksomhetene. Temaene er inndelt på følgende måte: kapittel 5.2.1 omhandler proaktiv innsats, kapittel 5.2.2 om innføring av ny teknologi, kapittel 5.2.3 om ledelsesforankring og forståelse for sikkerhetsarbeidet, kapittel 5.2.4 IKT-investeringer og ressurser, kapittel 5.2.5 systemteknisk nåtilstand, kapittel 5.2.6 kompetanse, kapittel 5.2.7 bruk av risikoanalyse – effekt på risikoforståelsen – forståelse for kompleksitet i IKT-systemene, kapittel 5.2.8 Sammenkoblinger, kapittel 5.2.9 Organisering av sikkerhetsprosjekter, kapittel 5.2.10 Samhandling, kapittel 5.2.11 Svikt i sikkerhetsarbeidet og hendelseshåndtering.

5.2.1 Praksis for drift- og forvaltning og årsaker til utfordringer

Virksomhetene A og C hadde et organisatorisk skille mellom drift- og forvaltning, mens i virksomhet B var drift- og forvaltning underlagt samme avdeling. Driftspersonell tok i større eller mindre grad del i utviklingsoppgaver, dels avhengig av prosjektets art og prosjektleder. I virksomhetene B og C var driftspersonellets involvering i prosjekter redusert for å kunne fokusere på drift- og forvaltning. Adskilt drift- og forvaltning forutsatte et klart ansvar mellom partene, men en informant sa det i praksis var uklare ansvarsforhold og man var usikre på hvordan arbeidet burde organiseres. Et tilsvarende fenomen om ansvarsforhold var i følge en annen informant tilfelle der driftsorganisasjonen ytet tjenester til eksterne parter.

Virksomhet B praktiserte utstrakt bruk av ekstern bistand til ulike tekniske oppgaver, mens virksomhet C hadde egne eksperter som støttet driftspersonell. Målsettingen var å kunne ha overlappende kompetanse med 3-5 personer.

En informant sa vedlikehold av IKT-løsningen ble gjort ut fra systemets dokumenterte sikre tilstand i henhold til gjeldende prosedyrer for anskaffelser og designendringer. Kvalitetskontroll

ble gjennomført både for løsningsdesign og endring i sikkerhetskonfigurasjoner. Det var egne varslingsrutiner mot kunder i forbindelse med vedlikehold eller innføring av nye tjenester.

Arbeidet med vedlikehold av tekniske barrierer i IKT-systemene var krevende av flere ulike årsaker:

Flere informanter viste til komplekse systemer som blant annet vanskeliggjorde mulighetene for å oppdage og forstå sammenhenger i: tjenester; komplekse trafikkmatriser som innebar risiko for å åpne opp for mer trafikk enn planlagt ved sammenkobling mellom virksomheter; manglende kompetanse eller erfaring gjorde ifølge informanter begge forholdene enda mer krevende. Dessuten var det var vanskelig for én person alene å ha oversikt over systemene ifølge en informant.

Kritiske systemendringer hos én virksomhet ble foretatt uten bruk av dublert bemanning. Flere personer kunne imidlertid være involvert i endringsprosessen ettersom en rekke barrierer oftest måtte endres samtidig. En annen virksomhet praktiserte bruk av endringsmeldinger som deretter ble kontrollert av nærmeste leder. Hastverksendringer kunne kontrolleres av kollega ved leders fravær.

I følge en informant kunne sikkerhetsnivået bli svekket ved innføring av ny funksjonalitet ettersom det kunne være nødvendig å omgå en sikkerhetsbarriere. Patching[18] kunne ifølge informanter resultere i ustabilitet i nettet, noe som dermed utfordret tilgjengelighetskravene. Et liknende hendelse resulterte følge en annen informant i lavere robusthet i nettet. Årsaken var applikasjoner som feilet fordi man forsøkte å tilfredsstille tekniske krav. Sikkerhetsoppdateringer kunne ifølge en informant stoppe samfunnskritiske tjenester på grunn av kompatibilitetsproblematikk, fordi man ikke helt skjønte sammenhengene i systemet og dermed kunne forutse konsekvensene. Under intervjuet ble eksempler på hendelser belyst.

Et forhold som ble trukket frem av flere informanter var knapphet på menneskelige og økonomiske ressurser, og dermed også manglende investeringer. Det første punktet kunne også ifølge flere informanter sees i sammenheng med tidspress i forhold til å gjøre drifts- og vedlikeholdsoppgaver. Lavt fokus fra toppledelsen var ifølge en annen informant årsak til at

[18] A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. Patch (computing). (udatert). Hentet 20.12.2016 fra https://en.wikipedia.org/wiki/Patch_(computing). Norsk begrep er sikkerhetsoppdateringer.

man ikke fikk tilstrekkelig med ressurser til vedlikehold og kompetansebygging. Årsaker til utfordringer med vedlikeholdsarbeidet kan oppsummeres slik:

- Kompatibilitetsproblemer	- Sikkerhetsoppdateringer
- Kompleksitet	- Mangelfull planlegging
- Verktøy	- Mangelfull risikovurdering
- Konfigurasjonsfeil	

Tabell 3 Årsaker til utfordringer med vedlikeholdsarbeidet

5.2.2 Noen årsaker til utfordringer ved innføring av ny teknologi

Halvparten av informantene trakk frem kompetansebygging som utfordrende ved innføring av ny teknologi. Mer spesifikt handlet det ifølge informantene i virksomhet A om hvilken kompetanse man burde ha på hvilket nivå i organisasjonen, samt kompetanse til drift- og vedlikehold av ny teknologi. Årsakene til man ikke rakk å bygge opp nødvendig kompetanse var: høyt arbeidspress; stadig nye krav; kapasitetsutfordringer hos drift grunnet flere oppgaver, og i noen tilfeller også flere manuelle oppgaver; mangel på kompetansemidler og urealistiske tidsfrister i prosjekter.

Andre årsaker til utfordringer var ifølge alle virksomhetene at ny teknologi oftest ble integrert med gammel teknologi, noe som dermed økte kompleksiteten ytterligere og hvordan teknologien gjensidig påvirket hverandre i forhold til sårbarheter. Ingen av informantene pekte på utfordringene med ny teknologi og dynamikken i IKT-sikkerhetsfeltet som er preget av både hyppige endringer i trusselbildet og fremvekst av nye sårbarheter.

En informant betraktet ny teknologi som fordelaktig, fordi det kunne lukke gamle kjente sårbarheter og dermed bidra til økt robusthet i systemene. Samtidig var informanten bevisst på at ny teknologi også kunne åpne for sårbarheter. En annen informant mente man burde avvente innføring av ny teknologi til den var mer utprøvd, ettersom ny teknologi ofte inneholdt feil.

Flere informanter i virksomhet C opplevde den forutgående godkjenningsprosessen som både langvarig og vanskelig av følgende årsaker: manglende godkjenning på diodeteknologi; ikke-oppfylte tempestkrav; at NSMs veiledninger ikke dekket nyere teknologier/versjoner som eksempelvis virtualisering og operativsystemer. En informant beskrev bivirkningene med lang utviklingstid for visse sikkerhetsprodukter omtrent slik: Brukeren måtte da forholde seg til

"gammel teknologi" i jobbsammenheng, mens vedkommende privat var godt vant med tilgang på moderne teknologi; tilkoblingsmuligheter; deling av informasjon. Ifølge informanten var det en mulig forklaring på vanskeligheter med å skille jobbrelaterte arbeidsvaner og adferd fra privat vaner. I tabellene nedenfor er årsakene utfordringer ved innføring av teknologi og manglende kompetanseoppbygging oppsummert.

- Høyt arbeidspress	- For lite kompetansemidler
- Nye krav (til leveranser)	- Prosjektets ferdigstillelsesdato

Tabell 4 årsaker til manglende kompetanseoppbygging før innføring av ny teknologi

- Økt kompleksitet (integrasjon mellom ny og gammel teknologi)	- Manglende godkjenning av komponenter
- Feil i ny teknologi	- brukeratferd

Tabell 5 årsaker til utfordringer ved innføring av ny teknologi

5.2.3 Ledelsesforankring og forståelse for utøvelse av sikkerhetsarbeid

Hovedinntrykket fra intervjuene var at forståelse og forankring av sikkerhetsarbeidet var: bra forståelse hos én på høyt nivå, ellers under bedring i virksomhet A, selv om man ikke var helt i mål enda; økt i virksomhet B og ble dermed ble prioritert noe høyere enn tidligere; rimelig god på avdelingsnivå og høyeste ledernivå hos virksomhet C.

Omtrent alle informantene trakk frem tilsyn fra NSM som den viktigste årsaken til bedret oppmerksomhet rundt sikkerhetsarbeidet, og hos to virksomheter var negativ hendelse en faktor som stimulerte til økt fokus på sikkerhetsarbeidet. Alle virksomhetene hadde erfart at resultater fra tilsyn, risikovurderinger eller negative hendelser også medførte politisk oppmerksomhet.

En informant mente interessen for sikkerhetsarbeidet falt etter 2-3 måneder, mens en annen mente interessen kunne holde seg oppe inntil ett år. En tredje informant mente det nok måtte skje noe for å få fornyet oppmerksomhet.

Andre årsaker til økt fokus på sikkerhetsarbeidet var ifølge informanter i virksomhet B gradvis erkjennelse og modning av sikkerhetsbehovet, økt kompetanse, samt ny ledelse hvorav flere med IKT-bakgrunn. En av informantene la til at med ny ledelse måtte man begynne forfra med reetablering av forståelsen. En informant begrunnet økt forståelse med ledelsens ansvar for

formell risikoaksept, sikkerhetsgodkjenninger, internkontroller og at synergier i forhold til funksjonelle områder ble synliggjort.

En grunn til at sikkerhetsarbeidet tidligere ikke hadde nødvendig fokus var ifølge informanter i virksomhet A at komplisert teknisk informasjon ikke ble fremstilt på forståelig måte for øverste ledelse og at man ikke var gode nok til å formidle kun relevant informasjon. En årsak til bedring var at de ansvarlige for utforming av ledelsesinformasjon hadde gjort en god innsats med å plukke ut riktig informasjon. Årsaken til behovet for relevant ledelsesinformasjon om IKT-sikkerhet var ledelsens tidspress og fokus på mange andre saker utover IKT-feltet.

Underliggende årsaker til begrenset forståelse for sikkerhetsarbeidet hos virksomhet B ble ifølge en informant synliggjort ved en IKT- leveranse hvor det ikke var planlagt med sikkerhet i løsningen, leveransedato var politisk bestemt og kontroll av sikkerhet var siste sjekkpunkt før lansering. I tabellene nedenfor oppsummeres årsakene til henholdsvis økt og manglende fokus på sikkerhetsarbeidet:

- Gradvis erkjennelse og modning,	- Ny ledelse,
- Kompetanseøkning,	- Formell risikoaksept,

Tabell 6 Årsaker til økt fokus på sikkerhetsarbeidet

- For dårlig kommunikasjon og informasjon (det å formidle komplisert teknisk informasjon til ikke-teknologer),

Tabell 7 Årsaker til mangelfullt fokuks på sikkerhetsarbeidet

- Ikke planlagt med sikkerhet i utviklingsfasen,	- Politisk bestemt lanseringsdato for løsningen,
- Sikkerhet ble kontrollert som siste sjekkpunkt før lansering av løsning,	

Tabell 8 Underliggende årsaker til mangelfullt fokus på sikkerhetsarbeidet

5.2.4 Årsaker til utfordringer mellom IKT-investeringer og ressurser

En av årsakene til utfordringene mellom IKT-investeringer og tilgjengelige ressurser var ifølge informanter at sikkerhet var dyrt og kombinert med budsjettkutt fikk det ytterligere

konsekvenser for planlagte investeringer i IKT-infrastrukturen og sikkerhet. En bakenforliggende årsak var i tillegg at man undervurderte kostnadene på IKT-anskaffelser og IKT-sikkerhet. En annen informant var inne på noe liknende og mente det manglet forståelse helt opp på embetsnivå i ett av departementene for hva som var nødvendig av IKT-investeringsmidler. Ettersom politikere kommer og går, måtte forståelsen være tilstede på embetsnivå. Ifølge informanten var investeringsplaner til liten nytte dersom ministeren ikke fikk nødvendige tildelinger i budsjettforhandlingene. Tre informanter i virksomhet A omtalte også begrensede budsjetter som en av årsakene til utfordringene.

Et annet forhold ifølge en informant var at IKT-investeringene var linket til politiske krav om effektivisering og kostnadsreduksjoner hos IKT-organisasjonen, noe som vanskelig kunne oppnås. Årsakene var kompleks infrastruktur og høye lisens- og driftskostnader. Innføring av nye IKT-verktøy økte derfor kostnadene. Informanten la til at andre deler av virksomheten muligens kunne oppnå innsparinger.

En annen grunn til utfordringer som halvparten av informantene var inne på handlet om at man undervurderte kapasitetsbehovet for å drifte nye løsninger, noe som ifølge en informant skyldtes at drift ikke fikk tilført personell, driftsstøtteverktøy eller ikke stengte ned gamle tjenester. Konsekvensene av manglende driftsverktøy var da flere manuelle operasjoner. Et tilsvarende syn ble understøttet av en annen informant hvor det fremgikk at prosjektene ikke vurderte levetidskostnadene på IKT, og årsaken til det var fokus på investeringer og ikke like mye på driftskostnader. Bortsett fra selve anskaffelsesreglene så var ifølge en informant selve investeringen i utstyr det enkleste, men det var mange andre krevende forhold: på brukersiden; i organisasjonen som skulle bruke utstyret; organisasjonen som skulle drifte- og forvalte løsningen. Informanten sa det slik: *"Det hjelper ikke med investeringsbudsjett i mangemillionersklassen, hvis det ikke følger med midler på driftsbudsjettet*".

En informant bekreftet at organisasjonen hadde nødvendig utstyr, men det var 3-4 ubesatte stillinger på drifts- og sikkerhetsoppgaver. Årsaken til ubesatte stillinger var i dette tilfellet omorganiseringer. Konsekvensene av underbemanning kunne eksempelvis være at prosedyrer ikke ble fulgt og at patching ikke ble dokumentert.

En utfordring som ble fremhevet av en informant var de høye kostnadene på sikkerhet i forhold til effekten man fikk av verktøyet, mens en annen informant kommenterte at den graderte

løsningen hovedsakelig ble brukt til administrative og regulative funksjoner som ikke var synlige i form av tjenester til publikum.

Ifølge en informant fikk politiske beslutninger om krav til nye tjenester ofte prioritet og sikkerhet var ikke nødvendigvis en styringsparameter, men ble tatt for gitt at det var på plass på samme måte som eksempelvis økonomisystemer. Årsaken mente informanten, var at lederne ble målt på om: *"virksomheten leverte det den skulle*". I avveiningen mellom bruk av midler på den graderte løsningen eller utvikling av ny tjeneste, var det ifølge informanten lett for at man landet på det siste. I tabellen nedenfor oppsummeres årsakene til utfordringer mellom IKT-investeringer og ressurser:

- begrensede budsjetter og høye kostnader på sikkerhetsløsningene,	- undervurderte kapasitetsbehovet for å drifte nye løsninger,
- undervurderte kostnadene på IKT-anskaffelser og IKT-sikkerhet,	- investeringsfokusert og ikke så driftsfokusert,
- kompleks infrastruktur,	- lederne ble målt på leveranser og ikke sikkerhet.
- høye lisens- og driftskostnader,	

Tabell 9 Årsaker til utfordringer mellom IKT-investeringer og ressurser

5.2.5 Systemteknisk nåtilstand

For å få et overordnet bilde av systemteknisk status og hvordan virksomhetene jobbet med det NSM omtaler som grunnsikring av IKT-systemer, ble informantene spurt om hvorvidt man: anvendte oppgradert maskin- og programvare i virksomheten; installerte sikkerhetsoppdateringer raskt; blokkerte administratorrettigheter for sluttbrukere; blokkerte kjøring av ikke-autorisert programvare.

Det var noe avvikende svar mellom informantene og da spesielt hos en virksomhet, noe som nok kunne tilskrives både rolle og plassering i organisasjonen, eller ulike systemer i virksomhetene. Indikasjonene i sammendraget nedenfor er ikke nødvendigvis et komplett bilde av virksomhetene.

Første virksomhet: tilstanden på maskin- og programvare ble vurdert som rimelig bra, men var samtidig et vanskelig punkt. Årsaken til det var mye gammelt virksomhetskritisk utstyr; Det

var gode rutiner for sikkerhetsoppdateringer, men de ble ikke nødvendigvis lagt inn med en gang. Årsaken til det var behovet for kvalitetssikring, for å minimere risikoen for driftsproblemer på virksomhetskritisk utstyr; Det var behov for å rydde i administratortilganger. Årsaken til det var utviklerbehov og et uklart skille mellom test og produksjon; Status for blokkering av ikke-autoriserte programmer var uklart.

Andre virksomhet: tilstanden på maskin- og programvare ble vurdert som rimelig bra, men kunne vært bedre. Man hadde fortsatt gamle systemer i drift som eksempelvis Windows 2003. Årsaken var at budsjettene ikke muliggjorde fornying i den takt man burde; Det var bra rutiner for sikkerhetsoppdateringer, men det kunne ta noe tid. Årsaken var behov for kvalitetssikring i forhold til funksjonalitet før oppdateringene ble distribuert i hele organisasjonen; Det var kun driftspersonell som hadde administratortilganger. Det var imidlertid visse utfordringer knyttet både til antall administratorer og administratorroller. En årsak til det var måten virksomheten var organisert på, og hvordan rollene burde fordeles for å sikre både rasjonell drift og overlappende kompetanse; Status for blokkering av kjøring av ikke-autoriserte programmer var rimelig bra, og det var en pågående prosess med å innføre dette tiltaket på øvrige systemer.

Tredje virksomhet: maskin- og programvarestatus ble ansett som bra, ble oppdatert jevnlig og brukte verktøy for å kartlegge og prioritere oppgraderingsbehovene. Det kunne også skje at systemer ble opprettholdt til slutten av livstidssyklus. Årsaken til utskiftingstakten hadde sammenheng med finansieringen; Sikkerhetsoppdateringer ble utført i henhold til etablerte prosedyrer og forutgående vurderinger av kritikalitet. Mindre kritiske oppdateringer ble testet før distribusjon. For oppdateringer som ikke rutinemessig ble varslet fra produsenten, kunne det oppstå forsinkelser med å få disse på plass. Årsaken var at ressurser var opptatt på med andre saker; Ingen sluttbrukere hadde administratortilganger, og for driftspersonell var granulerte administratortilganger redusert til et minimum; Det pågikk et prosjekt for blokkering av ikke-autoriserte programmer, men prosjektet var ikke ferdigstilt enda. Til tross for at det ikke var tillatt å laste ned programmer på klientene hadde det forekomment, men det ble oppdaget ved hjelp av deteksjonsmekanismer. I tabellen nedenfor oppsummeres årsaker til systemteknisk nåtilstand:

- Gammelt virksomhetskritisk utstyr, budsjettene tillot ikke høyere utskiftingstakt,	- Avgrenset til driftspersonell, hos enkelte gjenstående avklaringer (forholdet mellom test og produksjon eller rasjonell drift og overlappende kompetanse),
- Implementert prosedyrer, ble normalt kvalitetssikret før distribusjon, personell var opptatt med andre saker,	- Innført eller under innføring, men til dels avhengig av 1,

Tabell 10 Årsaker til systemteknisk nåtilstand

5.2.6 Kompetanse

Hos virksomhet A mente alle informantene at kompetansebehovet ikke var tilfredsstilt bra nok, og at det derfor var behov for mer kompetanse. Minimumskravene var ifølge to informanter tilfredsstilt for sikkerhetsledere og datasikkerhetsledere. To informanter sa det var sertifiseringskrav for å inneha bestemte roller. Informanter mente det var: for mange kompetansehull; behov for mer personell med kompetanse på risikovurderinger innen IKT; behov for mer spesialisert utdanning. Sistnevnte mente også erfaring var sentralt grunnet stadig mer kompleks dokumentasjon, noe som forutsatte totalforståelse for hvordan systemet virket i tillegg til lokalkunnskap.

Andre årsaker til kompetansegapet var ifølge flere informanter turnover; konkurranse om sikkerhetspersonell; det ble gjennomført for lite opplæring på sjefsnivå; begrensinger i budsjettene, som ble gjort fordi det ikke fikk direkte konsekvenser for driften.

En av årsakene var ifølge informanter at IKT-utdanningene ikke dekket spesifikke behov, samtidig som det ikke var eksplisitte kompetansekrav til risikovurderinger innen IKT for sikkerhetsledere og datasikkerhetsledere. En annen årsak var manglende tilgjengelighet på de aktuelle kursene på ønsket tidspunkt, og det kunne derfor ta lang tid før kompetansen var på plass.

Hos virksomhet B var synet delt mellom informantene. I følge en informant var ikke problemet hvorvidt man hadde riktig kompetanse eller ikke, men snarere utnyttelsen av kompetansen til å gjøre de riktige tingene. Dagens kompetansenivå var et resultat av: systematisk satsning gjennom flere år; etablerte roller og rutiner, slik at man ikke lengre var helt avhengig enkeltpersoner i samme grad som tidligere. Det var imidlertid ikke så mye dublert kompetanse i virksomheten.

Det var ifølge en informant et samarbeid med en av utdanningsinstitusjonene innen IKT-sikkerhet. Virksomheten var underbemannet og det ble tilsatt for få med den riktige bakgrunnen, noe som gjorde virksomheten sårbar. Årsaken mente informanten var manglende forståelse for kompetansebehovet hos ledelsen, og at det var gjentatte kamper om å få nødvendige ressurser til ansettelser. Sett bort i fra bruken av eksterne konsulenter var denne delen av virksomheten tynt bemannet.

Omtrent halvparten av informantene i virksomhet C mente kompetansenivået var bra, mens fem informanter så behovet for ytterligere styrking av kompetansen gjennom eksempelvis kurs fra NSM, SANS eller mer generelle kurs. En informant var usikker på kompetansebehovet på teknisk nivå og brukernivå, mens en fra teknisk side bekreftet behovet.

Noen av årsakene til dagens kompetansenivå var: aksept hos ledelsen; at det ble satt inn nok personell; at det ble satt av tid; tildelt nødvendige midler.

En informant pekte på ytterligere kompetansebehov hos driftspersonell. Årsaken var endret bruksmønster på systemet til mer operativ bruk og økte tilgjengelighetskrav og behov for flere operatører. I tabellene nedenfor følger oppsummering av årsaker til utfordringer knyttet til kompetansebehov, samt årsaker til positiv utvikling av kompetansen:

- Mer kompleks (sikkerhets)dokumentasjon, - Kurs- og utdanningstilbud var enten ikke tilgjengelige eller dekket behovet, - Begrensede budsjetter, - Turnover i virksomheten,	- Ikke eksplisitte kompetansekrav i regelverket om IKT-risikovurderinger for sikkerhetsledere datasikkerhetsledere, - Manglende forståelse hos ledelsen for kompetansebehovet, - Endret bruksmønster på IKT-systemet.

Tabell 11 Årsaker til utfordringer kompetansebehov

- Systematisk satsning på kompetansebygging, - Satt av nok personell, tid og budsjetter,	- Aksept hos ledelsen,

Tabell 12 Årsaker til nåværende kompetansenivå

5.2.7 Årsaker til bruk av risikoanalyse – effekt på risikoforståelsen - forståelse for kompleksiteten i IKT-systemene

Nesten alle informantene nevnte det ble gjennomført ulike typer risikoanalyser[19] i virksomhetene. Årsaken var ifølge halvparten pålagte krav. Andre årsaker var: nødvendigheten av å forstå risikoen; erkjenne risikoen; forstå konsekvensene; finne hvilke tiltak man eventuelt skulle sette inn. Risikoanalysene ble brukt som styringsinformasjon.

Som en informant sa det: *"... en oppvåkning på sikkerhet og at sikkerhets- og sårbarhetsanalyser var en forutsetning for å forstå hvordan problemet skulle gripes an*".

Hovedinntrykket hos informantene var at risikoanalysen bidro til økt bevisstgjøring og bedre risikoforståelse hos virksomhetsansvarlige. En informant la til at analysen også resulterte i bedre forståelse for komplekse forhold. En annen informant syntes det manglet en aggregert fremstilling, og at rapportene kunne videreutvikles for å gi bedre styringsinformasjon til ledelsen. En informant registrerte imidlertid at forståelsen var svakere på operativt nivå og hos utviklingsavdelingen, mens en annen antok analysen kunne illustrere risikoen for de med økonomisk makt. To informanter sa aktiv deltakelse fra lederen bidro til økt forståelse. En informant mente analysen kunne bidra til utvikling og mer proaktiv atferd.

En informant var usikker på om forståelsen økte på øverste ledernivå i forhold til gradert løsning, fordi det graderte systemet var IKT-avdelingens ansvar. Risikoanalysen var ikke nødvendigvis den katalysatoren som bidro til økt forståelse, men det var snarere en hendelse på ugradert som også fikk fokus høyere opp.

Et fellestrekk for alle virksomhetene var rimelig god forståelse for kompleksiteten hos ansvarlige ledere i IKT-avdelingene, men svakere i øvrige avdelinger og høyere oppover i makthierarkiet til politisk nivå. Hos to organisasjoner hadde imidlertid direktørnivået god innsikt, noe som ifølge to informanter skyldtes ledernes interesse for detaljer. En informant pekte på komplisert språk som en barriere mot forståelsen, men vedkommende løste dette ved å snakke med sine medarbeidere og ba om forklaringer. En annen informant var inne på det samme om evnen til formidling av komplekst stoff. Hos den tredje virksomheten hvor forståelsen var svakere oppover i hierarkiet, var sikkerhetsansvaret for IKT og objekter spredt

[19] Risikovurdering ble brukt synonymt med risikoanalyse hos flere informanter.

mellom ulike avdelinger og seksjoner. Årsaken til svakere forståelse oppover var at avdelingene ikke snakket så mye sammen.

En informant syntes kunnskapen var totalt fraværende på departementsnivå, og det var liten forståelse i ledergruppen. *"Det mangler fortsatt forståelse for datasikkerhet i maktapparatet.*"

En informant med IKT-bakgrunn syntes det var komplekst, og trodde ikke de ansvarlige ledere hadde stor forståelse for kompleksiteten:

"De kjenner til at det er komplekst, men har kanskje ikke full kjennskap til eksisterende kompleksitet, sammenhenger og avhengigheter. Det er først når konsekvensene blir synlige, at man får ny forståelse."

Ifølge en informant gjennomførte en leder på høyere nivå med bakgrunn fra drift aktiv veiledning av sine ledere og bidro slik til økt forståelse i temaet. Informanten mente driftsmessig bakgrunn var årsaken til økt forståelse for kompleksiteten.

Ifølge en informant hadde enkelte en veldig forenklet tilnærming, og vedkommende mente årsaken var divergerende oppfatninger når det gjaldt verdivurderingen av informasjonen.

En annen informant mente forståelsen var tilstede, men at det ikke alltid var mulig å følge nødvendig praksis. Årsaken var at det måtte gjøres forenklinger av hensyn til tjenesteleveranser.
I tabellene nedenfor oppsummeres først årsakene til manglende forståelse for risiko/kompleksitet, deretter vises årsakene til bruk av riskoanalyse, og hvorfor forståelsen for risikovurdering og kompleksitet økte:

- manglende kommunikasjon/samhandling,

Tabell 13 Årsaker til manglende forståelse for risiko - kompleksitet

- Lovpålagte krav,	- å forstå og erkjenne risikoen, konsekvensene og hvilke tiltak man eventuelt skulle sette inn,

Tabell 14 Årsaker til bruk av risikoanalyse

- aktiv deltakelse fra lederen,	- hendelse på IKT-system,

Tabell 15 Årsaker til økt forståelse for risikovurdering

- leder aktivt veiledet andre ledere,	- ledernes interesse for detaljer,
- kompetanse (fra drift),	- dialog mellom leder og medarbeidere.

Tabell 16 Årsaker til økt forståelse for kompleksiteten i IKT-systemene

5.2.8 Noen årsaker til utfordringer med sammenkoblinger

Resultatene fra intervjuene viste mange ulike årsaker til utfordringer med sammenkoblinger av informasjonssystemer mellom: ulike graderingsnivåer; virksomheter; nasjoner; *"air-gap"*-løsning. Sammenkoblingene kunne også omfatte ulike graderingsnivåer på tvers av virksomheter og nasjoner. Flere informanter kjente til ulike utfordringer som hadde inntruffet, og av eksempler som kan gjengis her var: tidkrevende avtaleinngåelse; systemtilpasninger; behov for kompetansebygging hos samhandlingspart; tilkobling av ikke godkjent utstyr; avklaringer av hvilken informasjon som skulle deles mellom parter; ulike typer informasjon på tvers av landegrenser.

Sammenkobling mellom ulike graderingsnivåer forutsatte at tilliten til sammenkoblingen var etablert i et eget system. Tabellen nedenfor oppsummerer årsaker til utfordringer med sammenkoblinger:

- teknisk utfordrende og økte kompleksiteten på IKT-systemet,	- avklaring av ansvarsforhold mellom partene,
- ressurskrevende å drifte- og vedlikeholde,	- ressurskrevende sikkerhetsgodkjenning,
- interessekonflikter,	- ressurskonflikter,
- økt risikoeksponering,	- kostnadsdrivende,
- filtrering av informasjon,	- manuelle integrasjonstiltak,
- mange aktører,	- manuelle kontrolltiltak.

Tabell 17 Årsaker til utfordringer med sammenkoblinger

For sammenkoblinger mellom virksomheter var resultatene fra informantene nokså tilsvarende som for sammenkobling mellom ulike graderingsnivåer, men det var to forhold som ble

fremhevet som utfordrende. Det første var at sammenkoblinger mellom virksomheter og nasjoner handlet mye om tillit mellom partene, og det andre var det å skulle forholde seg til mange aktører i flere ulike organisasjoner på tvers av landegrensene. Det siste punktet ble utfordret ytterligere ettersom informasjonsutvekslingen var politisk bestemt på den ene siden av grensen, mens man på norsk side ikke hadde etablert et hensiktsmessig mottaksapparat for den aktuelle forbindelsen.

De fleste utfordringene knyttet til sammenkoblinger hadde hovedsakelig sammenheng med virksomhetens uformelle kvaliteter, i tillegg til noen få formelle og tekniske kvaliteter. Funnene drøftes nærmere i kapitlene 6.1, 6.2 og 6.3.

5.2.9 Virksomhetenes praksis for organisering av sikkerhetsprosjekter

Kun en virksomhet hadde pågående sikkerhetsprosjekter. To virksomheter orienterte om gjeldende praksis.

Den ene virksomheten hadde et organisatorisk skille mellom utvikling- og drift. Funksjonelle sikkerhetskrav ble utformet av virksomheten, og prosjektorganisasjonen fikk deretter ansvaret for å levere løsningen. Øvrige interessenter i prosjektorganisasjon kunne være fra andre miljøer i virksomheten, industrien og NSM. Driftsorganisasjonen satte frem funksjonelle krav til drift av systemet ut i fra et sikkerhetsmessig fokus og krav til dokumentasjon.

Hos den andre virksomheten ble prosjektene organisert på ulik måte avhengig av type prosjekt, men normalt fulgte man de fem fasene for sikkerhetsgodkjenning når det handlet om graderte systemer. Vanlige prosjekter besto av interessentene: prosjektleder, forvalter, teknikere, dokumentasjonsansvarlig og arkitekter, mens man i større prosjekter også satte inn prosjektsikkerhetsleder, teknisk prosjektleder og styringsgruppe. Fra drift hentet man inn ressurser etter behov, men ifølge en informant varierte graden av involvering avhengig av prosjektlederen. Prosjekter ble ledet av systemeiere, mens det tidligere også ble benyttet ekstern bistand. På ugradert var operativ sikkerhet nå mer involvert fra start i forhold til tidligere praksis, men av kapasitetshensyn var deltakelsen avgrenset til kortere tidsrom.

Flere informanter poengterte at dagens praksis ikke var like godt egnet av følgende årsaker:

- IKT-arbeidet var fragmentert over flere avdelinger med mange bestillere og manglet én IKT-sjef for virksomheten,	- Politisk nivå besluttet at industrien skulle utvikle løsning for virksomheten, men uten organisasjonens deltakelse,
- For rigide krav i samband med teknologisk utvikling vanskeliggjorde arbeidet med referansegodkjenningene[20], fordi systemene endret seg hele tiden,	- Fremdriften ble hemmet pga kapasitetsproblemer ettersom personell utførte både drifts- og prosjektoppgaver,
- Ferdigstilte prosjekter oppnådde ikke nødvendig godkjenning,	- Prosjekter ble fragmentert pga manglende overbygning.

Tabell 18 Årsaker til utfordringer med sikkerhetsprosjekter

Sikkerhetsfolk ble ifølge informanter involvert sent i prosjektene og det ble dermed marginalt med tid igjen til å løse saken. En løsning var ifølge en informant å fokusere mer på risiko, slik at det ble mer dynamisk.

5.2.10 Samhandling

Alle virksomhetene hadde lagt ned innsats i å styrke interaksjonen og informasjonsflyten både internt og mellom organisasjoner, men flere informanter mente det kunne bli bedre. Årsakene til bedre interaksjon mellom partene var dels leders innsats og tilsyn fra NSM.

Ansvaret for sikkerhetsarbeidet var ulikt organisert i de tre virksomhetene, og gjeldende praksis for informasjonsflyt og koordinering av IKT-sikkerhetsoppgaver slik det kom frem under intervjuene er kort oppsummert i det følgende:

Hos virksomhet A lå ansvaret til driftsavdelingen, mens sikker drift ble håndtert av en annen avdeling. Arbeidet ble regulert gjennom instrukser for sikker drift, interne rutiner og direktiv for håndtering og rapportering av hendelser.

I situasjoner hvor sikker drift oppdaget noe vedrørende utstyr i en annen avdeling der personell tilhørte en tredje avdeling var det uklart hvem som da hadde ansvaret for å informere og håndtere selve hendelsen. Sikker drift fikk ikke nødvendigvis tilbakemelding om innrapporterte saker, men de hadde heller ikke kapasitet til å følge opp eventuelle tilbakemeldinger.

Hos virksomhet B var sikkerhetsansvaret fordelt på flere organisasjoner underlagt en felles sikkerhetsleder, noe som hadde bedret informasjonsflyten ettersom disse snakket sammen i

[20] En referansegodkjenning innebærer at man kan gjenbruke evalueringsresultater på bakgrunn av standardiserte systemmoduler, NSM G-02 (2014), *Explaining Infosec Directive §5.6 - §5.9*

større grad enn tidligere. Det forelå etablerte rutinebeskrivelser, nødvendige verktøy og definerte roller var besatt. Det var innført en prosjektmodell som satte minimumskrav til dokumentasjon i ulike faser av prosjektet.

Hos virksomhet C var det på operativt nivå etablert rutiner, samt flere elektroniske systemer for å understøtte informasjonsflyt og koordinering i virksomheten. Det var etablert flere fora for å understøtte arbeidet med informasjonssystemsikkerhet, og det ble holdt jevnlige koordineringsmøter både på teknisk nivå og stabsnivå. Koordinering mot kunder fant sted etter behov. Det var imidlertid enkelte tette skott mellom avdelingene, så samarbeidet var nok ikke så bra som det burde vært ifølge en informant. I tabellen nedenfor oppsummeres årsakene til at dagens praksis kunne ha betydning for sikkerhetstilstanden i virksomhetene:

- At saker ble løftet opp til høyere ledernivåer, og jo høyere opp desto lengre beslutningsveier i forhold til investeringer, - At det ikke forelå korrekt styringsinformasjon, mangel på informasjon, - At mindre ting ble håndtert tilfeldig avhengig av leders kapasitet, - Manglende vilje til koordinering på tvers av enheter (horisontalt), - Mangel på dublerte roller, - Rutiner ikke ble fulgt, - mangel på kommunikasjon,	- At man ikke dokumenterte godt nok og dermed ikke fikk tilstrekkelig status på hendelser, iverksatte tiltak, risikoeksponering, manglende dokumentasjon understøttet ikke virksomhetens læring tilstrekkelig og man ble dermed ikke gode nok på verdivurderinger, - Knapphet på tid til å formidle sikkerhetsmessige kommentarer, - Menneskelige feil som ikke ble tolket som feil og dermed ikke ble rapportert. - Mangel på ressurser, - At hendelser ikke ble håndtert korrekt, - utilsiktede sikkerhetsbrudd.

Tabell 19 Årsaker til at sikkerhetstilstanden utfordres i samhandling

En underliggende årsak som utfordret sikkerhetstilstanden var at man satte i drift systemer som manglet de riktige papirene, og informanten mente derfor at sikkerhetstilstanden kunne blitt påvirket ytterligere i positiv retning ved at man praktiserte strengere etterlevelse av kravene før idriftsetting. En vanlig underliggende årsak til at rutiner ikke ble fulgt var tidspress. Andre underliggende årsaker var: at det ikke ble vurdert som viktig nok; at man automatisk fulgte tidligere praksis (gikk på autopilot); latskap; menneskelig svikt; for dårlig kultur.

Konsekvensene av ressursmangel var at man jobbet ad hoc hele tiden og ikke fikk anledning til proaktiv innsats. Andre mulige konsekvenser var: tap av konfidensialitet; tap av tilgjengelighet; uønskede situasjoner; fravær av rapporter; nedsatt arbeidslyst og moral. Det var lang behandlingstid for saker som ble løftet til høyere nivåer, både på grunn av lange beslutningskjeder og mange iterasjoner for å komme frem til endelige konklusjoner. Andre konsekvenser var sårbarheter som ikke ble lukket som følge av manglende herding av løsningen, på grunn av uteblitt analyserapport etter reaktiv håndtering av et detektert angrep. Det kunne bli åpnet porter i nettverket som ikke burde ha vært åpnet.

Det var altså mange utfordringer knyttet til flere av organisasjonens uformelle kvaliteter.

Empirien fra dette kapitlet drøftes i kapitlene 6.1, 6.4 og 6.5.

5.2.11 Årsakene til svikt i sikkerhetsarbeidet og håndtering av hendelser

Alle informantene, med ett unntak, kjente til at det hadde vært svikt i sikkerhetsarbeidet eller med hendelseshåndtering av i løpet av det siste året. Den ene virksomheten hadde hundrevis av rapporterte hendelser månedlig. I en annen del av organisasjonen var det bare et fåtall rapporter, noe som virket litt for godt til å være sant. Den andre virksomheten hadde mange rapporterte sikkerhetshendelser uten at det ble tallfestet, mens den tredje virksomheten opplyste om flere registrerte sikkerhetshendelser.

Felles for virksomhetenes praksis var at sakene ble løst ved bruk av forhåndsdefinerte og skalerbare prosedyrer. Egne ekspertteam var ansvarlige for ulike tekniske spørsmål, noe som da krevet koordinering mellom teamene.

Årsakene til svikt i sikkerhetsarbeidet og hendelseshåndteringen var sammensatt. Felles for virksomhetene var ulike former for tekniske- eller menneskelige svikt. Teknisk svikt handlet om at systemene: manglet nødvendige barrierer, deteksjonsmuligheter og verktøy; hadde konfigurasjonsfeil og sikkerhetshull (nulldagssårbarheter). Tabellen nedenfor oppsummerer årsaker til svikt i sikkerhetsarbeidet og hendelseshåndteringen som gikk igjen hos to virksomheter:

- dårlig informasjonsflyt slik at involverte ikke var klar over hva som ble gjort (koordineringssvikt mellom drift og CERT),	- manglende personellressurser eller at ressursene var overbelastet med andre oppgaver,
- ikke fulgte sikkerhetsbestemmelsene og avvek fra etablerte rutiner. Det var tre forhold som gjorde at rutinene sviktet: tidspress; manuelle rutiner; mangelfulle rutiner eller hendelse som ikke var dekket av rutinebeskrivelsene,	- feiltolkning eller manglende forståelse for at det hadde oppstått en hendelse. (driftsmessige forhold ble detektert, men feiltolket som ikke-sikkerhetsrelatert, og følgelig ikke rapportert til CERT),
- manglende lederforankring og underprioritering av ressurser,	- manglende eller for lav kompetanse, herunder ikke-dublert kompetanse.

Tabell 20 Årsaker til svikt i sikkerhetsarbeidet og hendelseshåndteringen

Kompleksitet i systemene og manglende redundans (SPOF) var ifølge en av virksomhetene årsaker til svikt i sikkerhetsarbeidet. Strømbrudd ble nevnt som en årsak til IKT-sikkerhetshendelser, men som informanten sa: *"Det var ikke opplagt at alle betraktet tilgjengelighet som sikkerhet.*"

IKT-systemets sikre tilstand var ukjent på grunn av manglende eller mangelfull dokumentasjon ifølge en informant.

De fleste årsakene til svikt i sikkerhetsarbeidet eller hendelseshåndtering var knyttet til virksomhetenes uformelle egenskaper, med unntak av SPOF, strømbrudd og dokumentasjon. Funnene drøftes i kapitlene 6.1, 6.2, 6.4 og 6.5.

5.3 Informantenes syn på læring

Ledelsen kunne på den ene side bli bedre til å forstå sikkerhetsutfordringene, noe som på den annen side utløste behov for bedre styringsinformasjon. Læringen var også ifølge flere informanter en modningsprosess som ble styrket gjennom: ledelsesinvolvering ved risikoanalyse av objekter; undersøkelser av hendelser og sikkerhetsbrudd; sikkerhetsarbeid generelt. Tilsynsrapporter ga ideer til internkontroller.

Det var behov for kompetansetiltak på risikoanalyse for IKT-systemer. Risikovurderinger for objekter var ikke sammenfallende med vurderinger for IKT-sikkerhet. Et informasjonssystem ble ikke vurdert som objekt etter tolkning av regelverket, men senere ble én virksomhet kjent med at informasjonssystemer hos andre virksomheter var klassifisert som objekt. Fragmentert

kompetanse og mangelfull dokumentasjon utløste ved hendelser behov for å samle team som kunne bidra til å løse problemet.

Modulariseringen kunne resultere i problemer med å se helheten, noe som i neste omgang utfordret godkjenningen. Flere mente kravene var vanskelige å etterleve fullt ut og at NSM burde: fokusere mer på tilsyn som hjelp til virksomheten; bedre balansen mellom kontroller og veiledning; oppdatere veiledningene hyppigere; tilby spesialtilpassede kurs om SL, tilby DSL-kurs. En tredjedel ønsket mer strukturerte rapporter og forenklet oppfølging; halvparten ønsket mer: rettledning, veiledning, samt kurs i teknologiveiledninger. Det var også ønskelig med en oppdatert godkjent produktliste via NSM. Det hadde vært fordelaktig med en felles portal for informasjon.

Informanter reflekterte omkring samordnet regelverk for både gradert / ugradert, og kravene til gradert ble i enkelte tilfeller gjenbrukt også på ugraderte systemer. Videre mente enkelte informanter undersøker om informasjonssikkerhet eller sikkerhetsadministrasjon burde samordnes med øvrige tilsynsmyndigheter på området.

Resultatene fra kapittel 5 analyseres og drøftes i kapittel 6 mot teorien fra kapittel 4.

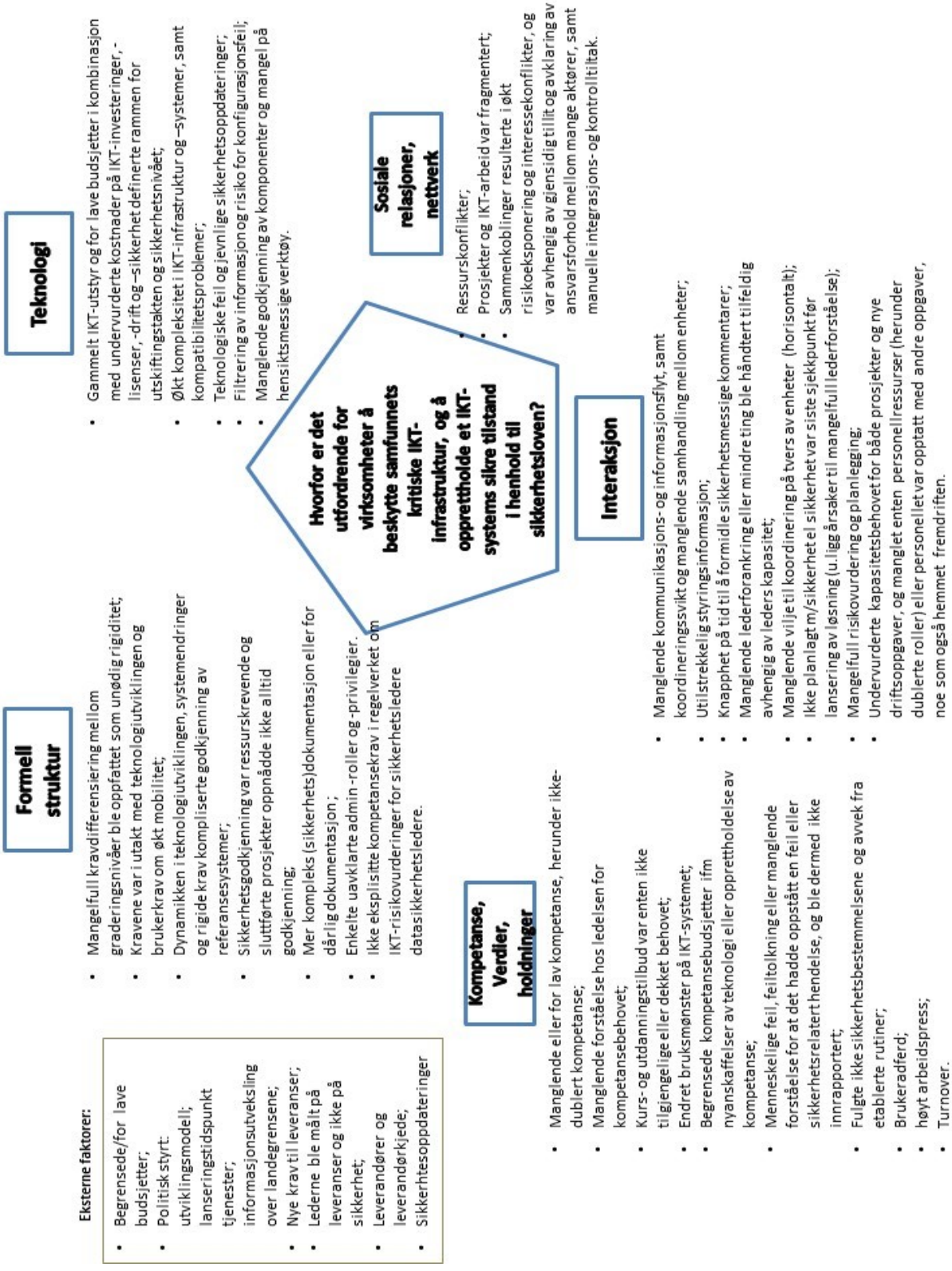
6 Analyse og drøfting

I dette kapittelet er funnene fra kapittel 5 brutt ned, systematisert, strukturert og analysert ved hjelp av pentagon-modellen omtalt i kapittel 4.2. Resultatene fra pentagonanalysen er fremstilt i Figur 8, og det er disse resultatene som brukes og drøftes videre i dette kapitlet mot teorien i kapittel 4 mot forskningsspørsmålet i kapittel 1.2. *"Hvorfor er det utfordrende for virksomheter å beskytte samfunnets kritiske IKT-infrastruktur, og å opprettholde et IKT-systems sikre tilstand i henhold til sikkerhetsloven?*"

Et interessant fenomen i denne casestudien er de mange funn under alle områdene i pentagonet slik det er vist i Figur 8 herunder uformelle kvaliteter, i tillegg til seks eksterne faktorer. Det viser for det første at informasjonssikkerhet må forstås som noe mer enn formell struktur og teknologi. Tradisjonelt er arbeid med informasjonssikkerhet oppfattet som et teknisk anliggende. Et forhold som kan illustrere det var eksempelvis utsagn fra informanter om: *"... ansvaret for det graderte systemet lå hos IKT-avdelingen og at virksomhetens ledelse ikke var ...*". Et annet poeng var at de som jobbet med drift ikke betraktet driftsoppgavene som en del av sikkerhetsarbeidet. I denne casestudien er det interessant nok relativt få funn under kapittel 6.3 sosiale relasjoner og nettverk. En mulig forklaring på det fenomenet kan være måten sikkerhetsarbeidet er organisert og forankret i virksomhetene på, og at funnet dermed indikerer at sikkerhetsarbeidet foregår litt isolert fra resten av virksomhetens aktiviteter. På den annen side er denne casestudien avgrenset til 13 informanter, hovedsakelig fra sikkerhetsorganisasjonen. Det blir dermed et fokus på sikkerhetsarbeidet fra innsiden av sikkerhetsorganisasjonen.

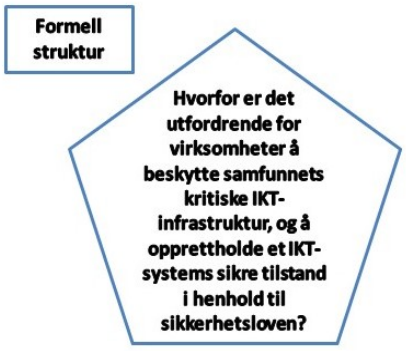
Figur 8 viser for øvrig eksistensen av mange ulike sammensatte årsaker til utfordringer med sikkerhetsarbeidet. Vi skal se litt nærmere på hvordan dette henger sammen i de påfølgende avsnittene.

Drøftingen tar utgangspunkt i formell struktur i kapittel 6.1, deretter behandles teknologi i kapittel 6.2. I fortsettelsen drøftes og analyseres de tre uformelle organisatoriske kvalitetene i kapitlene 6.5 kompetanse, verdier og holdninger, 6.4 interaksjon og 6.3 sosiale relasjoner og nettverk. Som et ledd i drøftingen i dette kapitlet er deler av empirien fra kapittel 5 utdypet og presisert nærmere.



Figur 8 Sosio-tekniske faktorer som forklarer utfordringer med å opprettholde IKT-systemers sikre tilstand iht. SL og beskyttelse av samfunnets kritiske IKT-infrastruktur (Ref. Pentagonmodellen, Schiefloe og Vikland, 2007; Schiefloe, 2013, 2014)

6.1 Formell struktur



I dette kapitlet analyseres og drøftes følgende resultater fra kapittel 5: Mangelfull kravdifferensiering mellom graderingsnivåer ble oppfattet som unødig rigiditet; Kravene var i utakt med teknologiutviklingen og brukerkrav om økt mobilitet; Dynamikken i teknologiutviklingen, systemendringer og rigide krav kompliserte godkjenning av referansesystemer; Sikkerhetsgodkjenning var ressurskrevende og sluttførte prosjekter oppnådde ikke alltid godkjenning; Mer kompleks (sikkerhets)dokumentasjon eller for dårlig dokumentasjon; Enkelte uavklarte admin -roller og -privilegier; Ikke eksplisitte kompetansekrav i regelverket om IKT-risikovurderinger for sikkerhetsledere og datasikkerhetsledere.

Flertallet oppfattet kravene som gode og nødvendige å vise til ved investeringsbeslutninger i sikkerhet, fravær av krav kunne lede til at sikkerhet ble ignorert. Omtrent halvparten av informantene oppfattet at kravene enten var: for lite differensiert for systemer beregnet for Hemmelig (H)[21] og Begrenset (B)[22]; i utakt med teknologiutviklingen (virtuelle systemer og nyeste Windows); ikke understøttet mobilitet; ikke var tilpasset relasjonen tjenesteleverandør og kunde. Kravene ble altså oppfattet som: for strenge; for gammeldagse; for lite fleksible og skalerbare. I fortsettelsen drøftes funnene nærmere.

Mangelfull kravdifferensiering mellom lavere- og høyere graderingsnivåer ble oppfattet som unødig rigid. Det var sammenfallende god forståelse for kravene på høyere graderingsnivå, men det var altså informantenes oppfatning at kravene på lavere graderingsnivå var tilnærmet de samme som for høyere graderingsnivå. En komparativ studie mellom Norge, England og US innen safety offshore viser både kompleksiteten i de regulatoriske ordningene og hvor viktig det er å utvikle regler som har legitimitet og som kan håndteres av involverte parter (Lindøe og Engen, 2013).

[21] altså informasjonssystemer godkjent for bruk til sikkerhetsgradert informasjon opp til og med Hemmelig. I denne avhandlingen brukes også begrepet høyere graderingsnivå.

[22] altså informasjonssystemer godkjent for bruk til sikkerhetsgradert informasjon opp til og med Begrenset. I denne avhandlingen brukes også begrepet lavere graderingsnivå.

Konsekvensene var dermed at kravene for lavere graderingsnivå ikke ble oppfattet som like legitime som for høyere graderingsnivå. Jo flere regler og tekniske reguleringer fra myndighetene, desto større er bevisbyrden som er pålagt utenfra ifølge Lindøe og Engen (2013). Det er vanskelig å se hvordan safety-kritiske problemstillinger i tilknytning til ledelse, organisasjon og teknologi ikke kan forbedres ved å bruke ytterligere eller mer detaljerte myndighetsregler. Jo flere preskriptive regler og tekniske standarder myndighetene tar opp som juridisk bindende, desto mer ansvar påtar de seg selv (Lindøe og Engen, 2013:211).

Informantenes oppfatning var stort sett at regelverket hadde understøttet sikkerhetsarbeidet i positiv retning, og flere brukte ord som: *"… bra å vise til for ledelsen"; "de gjeldende kravene er udiskutable"; "det er helt nødvendige krav"; "...blir bare mer og mer aktuelt."* En virksomhet var i gang med å bruke modifiserte sikkerhetskrav på et ugradert system som hadde for mange svakheter og for dårlig dokumentasjon. Kravene var altså et hjelpemiddel til å sikre systemene på bedre måte enn det man ellers fikk til. Majoriteten av sikkerhetspersonellet hadde som nevnt tidligere god nytte av detaljerte retningslinjer for å implementere sikkerhet i systemene, mens fravær av retningslinjer eller veiledninger gjorde at virksomhetene ikke kunne lansere tilbud om virtualisering. Det samsvarer bra med Skotnes (2015) funn om at mellomledere og ansatte med ansvar for innføring av internkontrollsystemer ønsket seg mer konkrete og detaljerte bestemmelser. Altså ifølge Skotnes og Engen (2015) var etterspørselen etter preskriptive reguleringer større i tett koblede og komplekse systemer hvor risikoen ble oppfattet som uforutsigbar og usikker. Motsatt var funksjonelle krav det foretrukne i styringen av løst koblede systemer hvor risikoen ble oppfattet som kontrollerbar og forutsigbar ifølge Skotnes og Engen (2015).

Kommando kontroll-prinsippet utfordrer dermed regulerende myndighets kapasitet til oppfølging, mens selvregulering etter frivillige tekniske standarder ifølge Lindøe og Engen (2013) overlater bevisbyrden til virksomhetene. På bakgrunn av kravene, kostnadene og arbeidet med å få på plass en godkjent lavgradert løsning, kunne byrdene ifølge flere informanter resultere i at virksomheten unnlot å skaffe til veie løsning for å behandle lavgradert informasjon; unnlot å gradere informasjon; behandlet informasjon på ikke godkjente systemer. Teorien om avskrekking som strever etter kommando og kontrollregulering, bygger ifølge Tietenberg i 1992 (som sitert av Sinclair (1997), s. 534) på antakelsen om at firmaer opptrer som rasjonelle kalkulerende aktører klare til å utforske enhver mulighet til å unnslippe regulatoriske krav dersom det fører til finansiell belønning. Virksomheten kan derfor muligens

falle for fristelsen til først og fremst å prioritere det de blir målt på, og hvis sikkerhet ikke er en måleparameter vil virksomheten underlagt NPM-prinsippene kunne se seg best tjent med å sørge for tjenesteleveransen som de faktisk blir målt på.

Skotnes (2015) argumenterer for at kombinasjonen av funksjonelle og preskriptive regler tar bedre hensyn til den naturlige utviklingen med nye teknologier og operative behov enn detaljerte regler, men komplekse teknologier krever samtidig både mer detaljerte retningslinjer, overvåkning og støtte.

> What regulators often lack, however, are the tools, training and the resources to confront the all important human and organizational factors and to monitor the insidious accumulation of the latent conditions that can subsequently combine to penetrate the system's defences. The same also applies to the policy-makers. (Reason, 1997b:183)

Det er altså ikke nødvendigvis regulerende part som prioriterer vekk sikkerhet som Tietenberg er inne på, men i IKT sammenheng innebærer for det første avstanden mellom regulerende myndighet, regulerende part og utviklerne av teknologien utfordringer med hensyn på å se alle relevante faktorer i sammenheng, noe som dermed har konsekvenser for beslutningene og resultatet. For det andre viste empirien at IKT-drift ikke alltid fikk nødvendige verktøy til å understøtte driftsoppgavene som dermed gjorde at de ikke hadde de samme forutsetningene for å kunne følge med på de latente betingelsene i de tekniske barrierene. Det bringer oss over til et annet fenomen som handlet om at sikkerhetsgodkjenningen var ressurskrevende og sluttførte prosjekter oppnådde ikke alltid godkjenning. Sammenkoblinger var en av grunnene til ressurskrevende godkjenningsprosesser. Større endringer krever ekstra ressurser i den tiden endringen pågår ifølge Meyer og Stensaker (2011), noe som kan skje gjennom å frigjøre kapasitet, øke kapasiteten eller utvikle ressurser. Et annet forhold det er naturlig å se nærmere på er organiseringen av utviklingsprosjektene.

For systemer som ikke fikk godkjenning ble det søkt om midlertidig brukstillatelse, noe som gjerne ble innvilget gitt at det kunne godtgjøres bruk av kompenserende tiltak frem til gjenstående krav ble oppfylt innen gitte frister. "Kundene" forventet dermed at det var mulig å finne løsninger selv om reglene ikke ble tilfredsstilt fullt ut, men tilsvarende forventning er observert også på myndighetsnivå: *"Authorities in many jurisdictions are often prepared to regard licence conditions as merely aspirational, and to waive the rules"* (Sinclair, 1997:535). Det normale ble på mange måter midlertidig brukstillatelse, selv om det altså strengt tatt ikke

var godt nok ifølge godkjenningsmyndigheten NSM. Rosness et al. (2010) kaller det for normalisering av avvik. Virksomheten var selv klar over at man ikke opererte fullt ut i henhold til rammebetingelsene. Under granskningen av Challenger-ulykken i 28. januar 1986 fant man ifølge Vaughan (1996) tilsvarende normalisering av avvik, ettersom O-ring problemet ble identifisert allerede i forbindelse med oppskytingen av STS-2 i 1981. I senere oppskytninger ble ifølge Vaughan (1996) stadig større avvik akseptert, og i tillegg sendte NASA opp nesten dobbelt så mange romferger i 1985[23] som året før tross større problemer med O-ringene. Grensene for akseptabelt risikonivå ble som Rasmussen (1997) vurderer det flyttet stadig nærmere uakseptabelt nivå, jf. Figur 6. Det at nødvendig barrierer ikke var på plass slik som de burde, innebar at informasjonssystemet hadde latente betingelser som kan lede til ulike sikkerhetshendelser eller sikkerhetsbrudd.

Prosjektene ble organisert på litt ulike måter avhengig av type prosjekt, og interessentenes involvering varierte. Virksomhetene fulgte de fem fasene for godkjenning i henhold til FoI. Det varierte hvilke interessenter som tok del i prosjektene. Prosjekter hadde blitt stanset som følge av: manglende deltakelse fra drift eller sikkerhet; manglende innspill; sikkerhetskrav ikke var tilfredsstilt. En viktig årsak til at prosjekter feiler er ifølge Cleland (1986, 2008); Jergeas, Williamson, Skulmoski, og Thomas (2000); Karlsen (2002) manglende kartlegging og ledelse av interessenter. Dersom ikke alle relevante interne og eksterne interessenter er representert i prosjektene, kan det derfor lede til at prosjekter feiler. Det er imidlertid mange andre mulige årsaker til at prosjekter enten feiler eller kommer i mål, og de fem viktigste slik Groth (2005) ser det er: Lederstøtten; Avklaringer av mål og forventninger; Kravspesifikasjonen; Bemanning og kompetanse; Prosjektorganisasjonen. Som vi ser passer de meddelte feilsituasjonene fra interessentene bra med Groths empiri, men for å få tegnet et fullstendig bilde av hvorfor sikkerhetsprosjekter feilet er det nødvendig med en egen undersøkelse. Poenget her er at det å oppnå sikker tilstand i et IKT-system starter allerede når utviklingsprosjektet ligger på tegnebrettet, og de funn som ble gjort i denne casestudien tydet på at ikke alle relevante interessenter var representert. Svakheter ved organiseringen av prosjekter kan derfor være en medvirkende årsak til at resultatene ikke ble som ønsket, men det var også indikasjoner på at eksterne faktor som økonomi spilte inn. Tidlig deltakelse fra driftspersonell kunne samtidig

[23] STS 51-C, STS 51-D, STS 51-B, STS 51-G, STS 51-F, STS 51-I, STS 51-J, STS 61-A, STS 61-B

bidratt til kompetansebygging på systemer driftsorganisasjonen senere skulle overta ansvaret for, noe som er diskutert i kapittel 6.5.

Kravene var i utakt med teknologiutviklingen og brukerkrav om økt mobilitet; Dynamikken i teknologiutviklingen, systemendringer og rigide krav kompliserte godkjenning av referansesystemer. Som nevnt i kapittel 2.1 utgir NSM ulike typer generelle og spesifikke teknologiske veiledninger om hvordan kravene skal etterleves. Dette understøtter det som er sagt i kapittel 4.4 om kommando og kontroll prinsippet. Informantene savnet imidlertid retningslinjer for nyere teknologier. En utfordring sett fra myndighetenes side er å følge opp teknologiutviklingen med nye og oppdaterte krav, og fra den regulerende parts side kan det derfor oppstå tvil om hvilke krav som skal legges til grunn, noe følgende sitat illustrerer:

"In rapidly expanding industries, particularly those with high rates of technological turnover, regulatory authorities are unlikely to be able to keep abreast of technical developments that form the basis of prescriptive regulations." (Sinclair, 1997:542)

Informantene sto da overfor dilemmaene: valget mellom nyere teknologi som ikke var dekket av kravene, eller holde seg til kravene og bruke gårsdagens teknologi.

Et annet spørsmål som melder seg er hvorvidt det er tilrådelig å bruke ny teknologi i komplekse systemer og kritiske infrastrukturer, som kanskje ikke har blitt grundig nok forhåndsundersøkt av eksperter. Ifølge de Bruijne og van Eeten (2007) er infrastruktursektorene utfordret gjennom fragmentering og konkurranse, slik at prinsippene om fullstendig informasjon, sentralisert planlegging og kommando og kontroll har fått redusert betydning til fordel for mer sann-tids operasjoner ifølge Roe et al, (2002) (som sitert av de Bruijne og van Eeten (2007), s. 21). Ideen om sanntids operasjoner som en viktig løsning for drift av kritiske IKT-systemer forutsetter da at feil kan korrigeres fra operasjonssenteret. Mange feil avhenger imidlertid av eksterne faktorer som leverandører, leverandørkjede mv., noe som da kan innebære reparasjonstid av uønsket varighet. Lysneutvalget viste i NOU 2015: 13 (2015) til sårbarhetslivssyklus i programutviklingen som er preget av flere feil, sårbarheter og mangler i tidlig utviklingsfase enn i senere fase. Programutviklingens sårbarhetslivssyklus og informantenes signaler om at kravene var gode hjelpemidler for beslutninger og gjennomføring av sikkerhetstiltak, bør sees i sammenheng med de systemene som faktisk skal beskyttes. Av den grunn kan det være formålstjenlig å velge godt designede, robuste og pålitelige systemer som ikke nødvendigvis er de nyeste på markedet, selv om det ifølge reguleringsteorien påfører myndighetene en større

byrde. Et annet spørsmål er om krav nærmere selvreguleringsprinsippet ville påføre regulerende part en mindre byrde ettersom virksomheten i større grad må bruke ressurser på å finne ut hvilken løsning som er god og sikker nok for formålet med tanke på at løsningene isolert sett er komplekse og oppkoblet som en del av infrastrukturen øker avhengighetene og kompleksiteten ytterligere, se også diskusjon i kapittel 6.2. Virksomheten bør i tillegg etablere sensitivitet til å kunne oppdage unormale forhold, og dermed handle gjennom både proaktive og reaktive tiltak som vist i figur 4.

Informanter opplevde godkjenningen av referansesystemer som utfordrende på grunn av endringer underveis og rigide krav.

Mer kompleks sikkerhetsdokumentasjon eller for dårlig dokumentasjon skapte utfordringer for virksomhetene. Betydningen av formell dokumentasjon, utover det å tilfredsstille rammevilkårene, har i andre sammenhenger vist seg å være vesentlig for den organisatoriske kompetansen. De formelle strukturene la dermed også føring for samhandlingen i virksomheten.

En informant viste til et tilfelle der sikkerhetsgodkjenning av informasjonssystem omfattet et hundretalls dokumenter. En annen informant mente sikkerhetsdokumentasjonen burde bestå av felles overbygning og struktureres på en slik måte at senere systemendringer og påfølgende oppdateringer i dokumentasjon kunne forenkles. I granskningen av Challengerulykken fant man ifølge Reason (1997b); Vaughan (1996) at mange interne dokumenter fortsatt klassifiserte en sammenføyningskomponent på faststoffrakettene med C1-R, selv om det tidligere var vedtatt å endre klassifiseringen fra C1-R til C1. C1 betød høyeste kritikalitet og mulig tap av liv eller fartøy, mens R betød at det eksisterte redundans eller backupsystem for mulig feil. Hos NASA var det i dette tilfellet ikke foretatt tekniske endringer i systemene som skulle dokumenteres, men det var endret klassifisering av tekniske komponenter som ikke ble dokumentert korrekt. Ifølge Reason (1997b); Vaughan (1996) medførte feildokumenteringen at enkelte ledere i NASA og personell i NASAs internkontroll[24] trodde det var et redundant forsvarssystem (sikring) på plass. Kompleksitet eller mangler i dokumentasjon kan derfor være medvirkende årsaker til at hendelser oppstår eller byr på utfordringer ved gjenoppretting, slik som eksempelvis et IKT-systems sikre tilstand. Forholdet til styrende dokumentasjon eller strukturelle faktorer var ifølge Brattbakk, Østvold, van der Zwaag, og Hallvard (2004);

[24] Safety, Reliability and Quality Assurance Program (SR & QA)

Schiefloe et al. (2005) og Schiefloe og Vikland (2007) én av årsakene til hendelsen på Snorre A.

For å få reetablert sikker tilstand må man vite eksakt hva som var systemets sikre tilstand. Som nevnt i kapittel 5.2.1 ble vedlikehold gjort ut fra IKT-løsningens dokumenterte sikre tilstand, og robustheten i systemet hvilte dermed i stor grad på at dokumentasjon viste korrekt status. Tatt i betraktning systemenes kompleksitet, samt omfattende og kompleks dokumentasjon for de graderte systemene, illustrerer det utfordringene for virksomhetene. Flere virksomheter opplyste at ugraderte systemer hadde hull i dokumentasjonen, og ved gjenoppretting etter hendelser ble det satt ned team av eksperter som i fellesskap tegnet opp systemet. Bruk av slike ekspertteam er bra for å skape felles forståelse for hvordan et system er satt opp og virker, men et slikt reaktivt tiltak vil påvirke reparasjonstiden i ulik grad avhengig av hendelsens karakter. Det betinger at ekspertene er tilgjengelige når man trenger de.

Det ble også vurdert som viktig å ha god kunnskap om lokale forhold i forbindelse med utforming av sikkerhetsdokumentasjon, se drøfting i kapittel 6.5.

Det var ikke stilt eksplisitte kompetansekrav i regelverket om IKT-risikovurderinger for sikkerhetsledere og datasikkerhetsledere. Dersom man ikke vet hva man skal se etter, så blir det også vanskelig å oppdage svakheter og mangler. FoI og FoO inneholder imidlertid bestemmelser om at risikovurderinger skal utføres. For førstnevnte bestemmelse var det innarbeidet praksis hos virksomhetene. Ettersom FoO trådte i kraft i 2011 var det ganske nytt for virksomhetene å gjennomføre risikovurderinger av objekter, men samtlige rapporterte at det var nyttig og lærerikt. Det er altså ikke bare myndigheten som har ansvar for å kontrollere virksomhetene, men virksomhetene har selv et ansvar for å gjøre risikovurderinger; vurdere hvorvidt de oppfyller kravene; melde fra til sektormyndigheten; sette inn tiltak. Det kan forstås som at virksomheten har overtatt det funksjonelle ansvaret for etterlevelse av sikkerhetskravene, noe som ifølge Olsen og Lindøe (2009) åpner for at interessentene kan samarbeide om implementeringen av sikkerhet.

Bruken av administratorroller og –privilegier var i all hovedsak etablert hos alle virksomhetene i henhold til gjeldende rammevilkår. Det var imidlertid ikke helt enkelt å løse alle forhold slik rammebetingelsene la opp til, noe som innebar at det for systemteknisk nåtilstand forelå enkelte uavklarte punkter ned hensyn på administratorroller og –privilegier. Årsaken hadde

sammenheng med: måten virksomhetene organiserte arbeidet på; bruk av ekstern bistand; bruk av testsystemer.

Ett av prinsippene i FoI handler om færrest mulig administratorer med de høyeste privilegiene. I praksis var det ikke så enkelt å etterleve kravet, fordi fravær av nøkkelpersonell med høyeste privilegier da kunne gjøre virksomheten mer sårbar. Det var derfor nødvendig å gjøre visse avveininger med tildeling av roller opp mot behovet for fleksibilitet og effektiv drift. De formelle sikkerhetskravene kom dermed i konflikt med kravene til NPM.

NOU 2015: 13 (2015) er inne på liknende forhold og anbefaler at funksjonsbasert regelverk vurderes i forbindelse med kravstilling til IKT-sikkerhet, og begrunner dette med raske teknologiske endringer og behovet for sikkerhetstiltak er tilpasset den enkelte virksomhet. I USA er trenden ifølge Rasmussen (1997) at lovgivning og reguleringer innen flere risikoområder går bort fra preskriptive regler og over til ytelsesbaserte regler.

Informanter mente regelverket burde praktiseres strengere enn det som var tilfelle nå under henvisning til at sanksjoner knapt hadde blitt anvendt. I kjølvannet av Challenger-ulykken undersøkte en forsker ifølge Reason (1997b) den regulatoriske prosessen og kom frem til at utøvelse av myndighetsrollen ikke skjedde på fritt grunnlag siden det var uunngåelige intraorganisatoriske relasjoner mellom myndigheten og virksomheten som var underlagt regulering. Dette resulterte ifølge forskeren til relasjoner som var mer tuftet på forhandlinger og kompromisser enn trusler og sanksjoner. Slike intraorganisatoriske relasjoner kan kanskje også forklare at sluttførte prosjekter uten sikkerhetsgodkjenning kunne få innvilget midlertidig brukstillatelse. Ytre press som nevnt i kapittel 5.2.3 om å få ta i bruk løsningen er andre mulige forklaringer på at kompromisser ble inngått.

6.1.1 Sammendrag formell struktur

Kravene for lavgradert ble ikke oppfattet som like legitime som for høygradert, noe som ifølge Lindøe og Engen (2013) var viktig. Det er vanskelig å si at bruk av preskriptive bestemmelser ikke virker positivt på sikkerhetsarbeidet ifølge Lindøe og Engen (2013), men samtidig påtar myndigheten seg større ansvar. Det beste var å finne balansen mellom bruk av preskriptive og funksjonelle krav ifølge Sinclair (1997); Skotnes (2015).

Ressursbehovet i prosjekter ble undervurdert og interessenter fra drift ble ikke alltid koblet inn i tide. Normalen var at sikkerhetsgodkjenning resulterte i midlertidig brukstillatelse ved bruk av kompenserende tiltak.

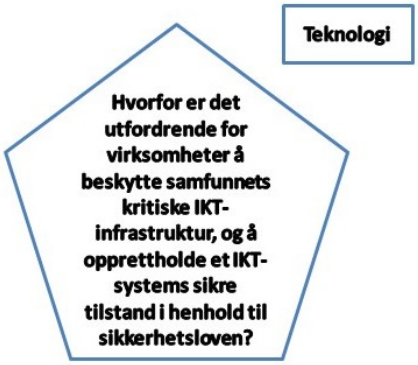
Halvparten av informantene mente preskriptive krav var i utakt med den dynamiske teknologiutviklingen og vanskeliggjorde tilfredsstillelse av nye brukerkrav. Godkjenning av referansesystemer ble komplisert på grunn av systemendringer underveis og rigide krav.

Kompleks eller for dårlig sikkerhetsdokumentasjon representerte fallgruver ved kritiske operasjoner eller fare for feilaktige beslutninger, noe som var tilfelle hos blant annet NASA og på Snorre A.

Det var ikke stilt eksplisitte kompetansekrav i regelverket om IKT-risikovurderinger for sikkerhetsledere og datasikkerhetsledere.

Det var fare for at kravet til administratorroller og –privilegier gitt i FoI gjorde virksomheten mer sårbar, da kravene kom i konflikt med behovet for fleksibilitet og effektiv drift gjennom NPM.

6.2 Teknologi



I dette kapitlet analyseres og drøftes følgende resultater fra kapittel 5: Gammelt IKT-utstyr og for lave budsjetter i kombinasjon med undervurderte kostnader på IKT-investeringer, - lisenser, -drift og –sikkerhet definerte rammen for utskiftingstakten og sikkerhetsnivået; Økt kompleksitet i IKT-infrastruktur og –systemer, samt kompatibilitetsproblemer; Teknologiske feil og jevnlige sikkerhetsoppdateringer; Filtrering av informasjon og risiko for konfigurasjonsfeil; Manglende godkjenning av komponenter og mangel på hensiktsmessige verktøy.

Resultatene fra kapittel 5.2 viste at ønsket utskiftingstakt på IKT-utstyr ikke var realisert hos noen av virksomhetene. Den viktigste årsaken var stramme budsjettrammer og høye kostnader, mens én part vurderte det som utfordrende å bytte virksomhetskritisk utstyr. Utskiftingstakten påvirket igjen mulighetene for å implementere sikkerhetsfunksjonen blokkering av ikke-

autoriserte programmer som finnes i nyere versjoner. To virksomheter var i gang med innføring av nevnte sikkerhetsfunksjon, mens status var uklar i den siste virksomheten.

Hyppige teknologiske skift, endringer i trusselbildet og krav om ny funksjonalitet er noen faktorer som påvirker behovet for utskifting av utstyr, og resultatene fra casestudien viste først og fremst fokus og stort press på det siste punktet. Samtidig anbefaler NSM at maskiner- og programvare bør holdes oppdatert til nyeste versjoner for ugraderte systemer, mens det er et krav for graderte systemer. Granskningsrapporten etter gassutblåsningen på Snorre A viste ifølge Schiefloe og Vikland (2007) at forebyggende vedlikehold og tekniske oppgraderinger hadde vært nedprioritert gjennom flere år, samtidig som høy produksjon ble opprettholdt, i tillegg pågikk mange nye prosjekter og det var stort aktivitetsnivå.

Arbeidsformen hos to av virksomhetene var preget av en ad-hoc tilnærming, noe én informant beskrev som at man befant seg på *"slagmarken*" med stadig nye krav. Man fikk ikke muligheter til å jobbe mer proaktivt, noe som dermed hadde betydning for sikkerhetstilstanden. Det samme var også tilfelle på Snorre A, hvor driftspraksisen var preget av høyt arbeidspress, hyppige avbrytelser og stadige behov for improvisasjoner og *"brannslokking*" (Schiefloe og Vikland, 2007).

Ny teknologi var beheftet med tekniske feil, noe som blant annet gjorde det nødvendig med jevnlige sikkerhetsoppdateringer. Disse to forholdene hadde dermed konsekvenser både for systemteknisk nåtilstand, og hvordan virksomhetene skulle ivareta drift- og vedlikeholdsoppgavene. Mangler og svakheter i teknologien ble av informanter beskrevet som: *"... systemene var ikke feilfrie ..."; "... selv om ny teknologi var testet, gjenstår det nesten alltid feil"; "... det trenger ikke være feil eller sikkerhetshull, men svakheter*".

Slike latente betingelser som eksempelvis dårlig design, for lite støtte, uoppdagede mangler fra produksjon, vedlikeholdsfeil, uhåndterlige prosedyrer, klosset automatisering, mindre tilfredsstillende verktøy og utstyr kan ifølge Reason (1997a, 1997b) være tilstede i årevis før de i kombinasjon med lokale omstendigheter og aktive feil bryter gjennom systemenes mange lag med beskyttelse.

De latente betingelsene dårlig design og uoppdagede mangler fra produksjon, sett i sammenheng med formell struktur i kapittel 6.1 om: kommando og kontroll prinsippet; at det ikke var planlagt med sikkerhet; sikkerhet var siste sjekkpunkt før lansering, gir grunnlag for å diskutere hvorvidt virksomhetene da fikk synliggjort kravene på en måte som industrien kunne

møte. Dette punktet kan også sees i sammenheng med utsagnet nedenfor om manglende godkjenning av komponenter. Den tekniske sikkerheten handler om å få frem et utvalg gode produkter som møter virksomhetenes sikkerhetsbehov, og for at det skal skje er industrien avhengig av å kjenne kravene før produktene designes. I det internasjonale arrangementet CCRA[25] forsøker medlemslandene for tiden å bidra til utforming av relevante sikkerhetskrav til produktutviklingen gjennom det man kaller *collaborative Protection Profiles* (cPP)[26] for gitte teknologiområder[27,28,29 og 30]. Hensikten er dels å stimulere til flere mer sikre kommersielle produkter på markedet, dels å understøtte myndighetenes behov for bedre kommersielle sikkerhetsprodukter. Bakgrunnen for behovet er: skreddersøm er i mange tilfeller dyrt; kutt i offentlige budsjetter; å kunne håndtere raske teknologiske skift på en bedre måte enn tidligere. Intensjonene med cPPer er å foreta hyppige oppdateringer av profilene for å kunne holde tritt med teknologiutviklingen og å møte endrede krav fra interessentene. Det handler altså om standardisering av IKT-sikkerhet.

Drøftingen over viser utfordringer knyttet til produkter som virksomhetene i denne casestudien ikke nødvendigvis kan løse alene. Det bringer oss over til en av konsekvensene med svakheter og mangler i produkter som virksomhetene var inne på, nemlig jevnlige sikkerhetsoppdateringer. Virksomhetene hadde etablert gode rutiner for sikkerhetsoppdateringer, noe som i de fleste tilfellene ble utført raskt. I enkelte sammenhenger kunne det imidlertid ta noe tid før sikkerhetsoppdateringer ble installert. Årsakene var at

[25] CCRA. (2014). *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, 2 July 2014, hentet 23.10.2016 fra http://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf

[26] Collaborative Protection Profiles (cPP) and Supporting Documents (SD). (udatert). Hentet 23.10.2016 fra http://www.commoncriteriaportal.org/pps/static.htm

[27] Network international Technical Community. (2015). *collaborative Protection Profile for Stateful Traffic Filter Firewall,* Hentet23.10.2016 fra https://www.commoncriteriaportal.org/files/ppfiles/CPP_FW_V1.0.pdf

[28] Full Drive Encryption international Technical Community. (2016). *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition.* Hentet 23.10.2016 fra https://www.commoncriteriaportal.org/files/ppfiles/CPP_FDE_AA_V2.0.pdf

[29] Full Drive Encryption international Technical Community. (2016). *collaborative Protection Profile for Full Drive Encryption – Encryption Engine.* Hentet 23.10.2016 fra https://www.commoncriteriaportal.org/files/ppfiles/CPP_FDE_EE_V2.0.pdf

[30] Network international Technical Community. (2015). *Collaborative Protection Profile for Network Devices.* Hentet 23.10.2016 fra https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf

sikkerhetsoppdateringer kunne: introdusere ustabiliteter i nettet; utfordre tilgjengelighet; stoppe samfunnskritiske tjenester; resultere i lavere robusthet i nettet.

Det ble ikke meldt om begrensninger i tekniske systemer i forhold til implementering av nødvendige roller og privilegier, men utfordringene var knyttet til policybeslutninger om best mulig og mest mulig effektiv måte å organisere arbeidet på som diskutert i kapitel 6.1 Formell struktur.

Reason (1997b) mener vi ikke kan unngå at det blir sådd latente betingelser i våre systemer siden de er et uunngåelig resultat av strategiske beslutninger. Det vi ifølge Reason (1997b) kan gjøre er å finne de latente betingelsene, og gjøre noe med de det haster mest med innen en gitt tidsramme. Utfordringen knyttet til det gjelder omgivelsenes tillit til metoden for å finne og rette mangler, samt eksternt press om tjenesteleveranser. Og det er klart når man retter opp disse, så vi andre ting feile (Reason, 1997b). Dette er jo sikkerhetsoppdateringene i et nøtteskall, noe som samsvarer godt med de opplevde utfordringene hos virksomhetene. Like fullt er det litt merkelig at informantene ikke diskuterte spørsmål om leverandørens ansvar for feil og kundenes toleranse for feil. Lysneutvalget er i NOU 2015: 13 (2015) inne på temaet ansvarliggjøring i sin beskrivelse om kompleksitet og sårbarhetslivssyklus i programvareutviklingen. Utvalget foreslår til slutt det må bygges bedre feiltolerante systemer for å redusere konsekvensene av sårbar kode. Det er minst to forhold som ikke ble diskutert av utvalget: virksomhetenes kost-/nytte ved bruk av uferdig programvare inneholdende for mange feil eller som mangler gode prinsipper for sikkert design; virksomhetenes kost-/nytte ved bruk av programvare designet etter gode sikkerhetsprinsipper. Et tredje forhold er knyttet til hvorvidt KI fritt skal kunne velge blant gode eller mindre gode sikkerhetsløsninger, gitt at det er forskjell på de to alternativene nevnt foran i favør av programvare designet etter gode sikkerhetsprinsipper. Dette betinger igjen at likelydende krav gjøres gjeldende for hele KI-sektoren, uavhengig av graderingsnivåer.

Gjennomgående utfordringer hos alle virksomhetene var at nye investeringer tilførte økt kompleksitet i IKT-infrastruktur og –systemer, samt kompatibilitetsproblemer. Spesielt gjaldt det ved sammenkoblinger mellom gammel og ny teknologi eller mellom systemer mot andre virksomheter. Alle disse forholdene utfordret dermed drift- og vedlikehold både med hensyn på kompetanse og kapasitet.

Samfunnskritiske tjenester kunne stoppe på grunn av kompatibilitetsproblematikk, fordi man ikke skjønte sammenhengene i systemet og dermed kunne forutse konsekvensene. Det var eksempler på at tetting av sikkerhetshull hadde stoppet hele tjenesten. Med stor kompleksitet i systemene kunne endringer påvirke mange andre komponenter og i enkelte tilfeller så mange som fem – ti andre. Det var med blandede følelser man foretok sikkerhetsoppdateringer, og mulig risiko for følgefeil var en av grunnene at man i visse tilfeller avventet å legge inn oppdateringene til det var gjort best mulig konsekvensvurdering. I 2006 og 2009 var det ifølge Almklov et al. (2010) to alvorlige bortfall av IKT-infrastrukturen ved St. Olavs Hospital som skyldtes henholdsvis programvarefeil i nettverkskomponenter fra en internasjonal produsent og feil utløst av oppdatering av printerdriver. I begge tilfellene var det små oppdateringer som fikk store konsekvenser.

Grunnlaget for systemulykker har ifølge Perrow (2011) oppstått gjennom høy interaktiv kompleksitet og tette koblinger, og at det er utformet så kompliserte design at vi ikke kan regne med å komme uunngåelige feil i forkjøpet. En ikke helt uvanlig strategi i kritiske systemer er å bygge inn redundans for å redusere sannsynligheten for uforutsette fellessvikt som også Lyseneutvalget var inne på i NOU 2015:13 (2015), men ifølge Perrow (2011) innebærer det økt interaktiv kompleksitet og større sannsynlighet for uforutsette fellessvikt; gjør systemene mer uoversiktlige for personell som normalt opererer og kontrollerer systemet; som en konsekvens av skjult og sofistikert redundans kan operatører og ledelse glemme å være redd. Flere informanter mente det ikke var mulig for én person å ha oversikten over systemene, og som nevnt tidligere hadde alle virksomhetene erfart feil og følgeskader i samband med implementering av utstyr- og programmer eller ved oppdateringer. Gitt budsjettrammene var det ikke mulig å bytte alt utstyr samtidig, så IKT-systemene besto derfor av både gammelt- og nytt utstyr. En blanding av både gammelt- og nytt utstyr resulterte ikke bare i økt teknisk kompleksitet, men utfordret også driftsorganisasjonen med hensyn på personell, kompetanse, interaksjon og sosiale relasjoner – kort sagt det utfordret organisasjonen ytterligere. Ifølge Reason (1997b) øker kompleksiteten i systemene når man legger til komponenter, spesielt i forbindelse med vedlikehold. Reason (1997a) beskriver den menneskelig faktor som det største problemet med vedlikeholds relaterte aktiviteter.

Det bringer oss over til utfordringene med filtrering av informasjon og risiko for konfigurasjonsfeil, både ved sammenkoblinger, drift- og vedlikehold.

En utfordring med vedlikehold i sikkerhetsarbeidet var å holde oppsett og konfigurasjon i tekniske barrierer[31] intakte ettersom systemene var komplekse. Konfigurasjonsfeil kunne være årsak til svikt i sikkerhetsarbeidet. Det var vanskelig for én person å ha den nødvendige oversikten til å kunne: utforme mest mulig optimal konfigurasjon i forbindelse med drift; sammenkoblinger og justering av trafikkmatriser; sørge for nødvendig funksjonalitet igjennom barrieren; se sammenhengene mellom systemene; ha oversikt over hva som ble sluppet igjennom barrieren og hva som ble stengt ute. Den forutgående risikovurderingen knyttet til endring av barrierer var også utfordrende på grunn av kompleksitet. Det var etablerte prosedyrer for endringskontroll som i praksis ble utført av spesialisert personell på de enkelte barrierene. I følge resultatene fra undersøkelsen var det ikke vanlig med dublert bemanning når virksomhetene utførte kritiske endringer. Som vi så i avsnittet over er den menneskelige faktor den største feilkilden i forbindelse med vedlikeholdsarbeid som eksempelvis tekniske barrierer, og som vist i kapittel 6.5 var menneskelige feil én årsak til utfordringer i denne casestudien. I teorien om *High Reliability Organisations* (HRO) brukes ifølge LaPorte og Consolini (1991) mannskapets overlappende oppgaver og kompetanse som et kompenserende middel for å sikre høyere pålitelighet i oppgaveutførelsen.

Ved anskaffelser av ny teknologi var det noen opplevde utfordringer som manglende godkjenning av komponenter og mangel på hensiktsmessige verktøy. Nye systemer ble ikke alltid overlevert til driftsorganisasjonen med nødvendige verktøy som kunne understøtte drift- og vedlikeholdsarbeidet på best mulig måte. Det omhandlet både type verktøy, hvilken versjon og om verktøyet var formelt godkjent for bruk. Mangel på verktøy skapte utfordringer for drift- og vedlikeholdsarbeidet, noe som ble løst gjennom bruk av flere manuelle operasjoner. Fravær av driftsstøtteverktøy som eksempelvis SIEM kan derfor hemme organisasjonens sensitivitet og evne til å oppdage og forstå farer eller uregelmessigheter som vist i Figur 4, noe som dermed innebærer lavere grad av robusthet, pålitelighet og sikkerhet.

Sett i lys av diskusjonen i avsnittene over er den menneskelige faktoren ifølge Reason (1997b) den største utfordringen i forbindelse med vedlikehold. Innføring av nye systemer medførte dermed også utfordringer i forhold til personellressurser, noe som behandles nærmere i kapittel 6.3. En årsak til manglende verktøy kunne være begrensninger i budsjettet. Vi ser dermed at målene kommer i konflikt med hverandre jfr. diskusjonen i kapittel 6.1. For å få bedre forståelse

[31] Eksempelvis slik som ruter, brannmur, svitsj

av utfordringene er det nødvendig å se diskusjonen i dette avsnittet i sammenheng med kapitlene 6.3 og 6.4.

Manglende tempestgodkjenning[32] av komponenter eller mangel på CC-sertifiserte produkter skapte utfordringer i forbindelse med sikkerhetsgodkjenning av løsninger, og førte til at virksomhetene måtte velge andre løsninger enn først planlagt. Valgene kunne omfatte enten: kompenserende tiltak; bruk av ikke-sertifiserte produkter med ønsket funksjonalitet og som integrerte godt med løsningen. Formelle godkjenningskrav til gitte produkter og komponenter snevret inn valgmulighetene, og flere var av den oppfatning at de ulike godkjenningsordningene ikke holdt følge med teknologiutviklingen. Det ble vist til et konkret eksempel hvor informantenes vurderinger var at det ikke-sertifiserte produktet både integrerte bedre med løsningen og var sikrere enn det sertifiserte produktet, men det benyttet ikke plattformens innebygde sikkerhetsfunksjoner. Bruk av det aktuelle produktet resulterte blant annet også i flere manuelle driftstiltak fra virksomhetens side. I følge avsnittene over så vi at den menneskelige faktoren er den største utfordringen i vedlikeholdsarbeidet som nevnt av Reason (1997b). Som vi så i kapittel 6.1 er kommando og kontroll-prinsippet utfordrende når det gjelder å følge opp revisjoner av rammebetingelsene i lys av den hurtige teknologiutviklingen.

6.2.1 Sammendrag teknologi

Det var utfordrende å realisere ønsket nivå av forebyggende vedlikehold på IKT-utstyret ettersom investerings-, lisens-, drift-, og sikkerhetskostnadene oversteg den økonomiske rammen, og man fikk dermed ikke tilstrekkelig fokus på proaktiv innsats hos to virksomheter hvor arbeidsformen da ble ad-hoc preget.

Latente feil i ny teknologi utfordret virksomhetenes drifts- og vedlikeholdspraksis som følge av eksterne strategiske beslutninger hos leverandørene, og som en konsekvens av det hadde alle virksomhetene etablerte rutiner for jevnlige sikkerhetsoppdateringer som igjen kunne medføre: ustabiliteter; tilgjengelighetsproblemer; stanse samfunnskritiske tjenester; mindre robusthet.

Nye investeringer i IKT-infrastruktur og –systemer resulterte i økt interaktiv kompleksitet og tette koblinger, og samfunnskritiske tjenester hadde stanset som følge av

[32] Med Tempest menes elektromagnetisk stråling fra elektronisk utstyr som utilsiktet kan forårsake at uvedkommende kan få tilgang til sikkerhetsgradert informasjon, samt undersøkelser og analyser knyttet til slike fenomener. NSM fastsetter nødvendige tiltak som må iverksettes for å beskytte et informasjonssystem mot Tempest. Kilde: FoI.

kompatibilitetsproblemer. Den menneskelige faktor er det største problemet ved vedlikehold, samtidig som vedlikehold gjennom patching er uunngåelig. Kombinasjonen av gammelt og nytt utstyr utfordret driftsorganisasjonen: teknisk; personellmessig; kompetanse; interaksjon; sosiale relasjoner.

Konfigurasjon og filtrering av informasjon gjennom tekniske barrierer utgjorde en risiko ved sammenkoblinger, drift- og vedlikehold på grunn av høy interaktiv kompleksitet og tette koblinger.

Manglende godkjenning av komponenter hadde ifølge virksomhetene bakgrunn i at godkjenningsordningene ikke holdt følge med teknologiutviklingen, noe som resulterte i at virksomhetene måtte gjøre nye produktvalg, inkludert tester, enn planlagt. Mangel på hensiktsmessige verktøy resulterte i mer manuelt drifts- og vedlikeholdsarbeid, noe som dermed også utfordret virksomhetene med hensyn på personellressurser.

6.3 Sosiale relasjoner og nettverk

I dette kapitlet analyseres og drøftes følgende resultater fra kapittel 5: Ressurskonflikter; Prosjekter og IKT-arbeid var fragmentert; Sammenkoblinger resulterte i økt risikoeksponering og interessekonflikter, og var avhengig av gjensidig tillit og avklaring av ansvarsforhold mellom mange aktører, samt manuelle integrasjons- og kontrolltiltak.

Ressurskonflikter var en av utfordringene virksomhetene møtte i forbindelse med sammenkoblinger.

De regulatoriske kravene som omtalt i kapittel 2.1 definerer hvordan virksomhetene skal organisere sikkerhetsarbeidet i form av både roller, funksjoner, metoder og strukturer, se også diskusjonen i kapittel 6.1. Bestemmelsene regulerer altså minimumskravene til ressursinnsats i form av bemanning, noe som dermed krever tilstrekkelige økonomiske rammer.

Opplevde utfordringer var at sikkerhetskravene kom i konflikt med: tjenesteleveranser og funksjonalitetskrav fra kunder; krav til raske leveranser; politisk bestemt leveransetidspunkt.

Det er ikke sikkert det ble oppfattet på samme måte fra *"blunt end*" som på det operative nivået, se figur 7. En mulighet er at beslutningstakere ifølge Albrechtsen (2008); Hagen et al. (2008) tar for gitt at eksisterende sikkerhetspolitikk, prosedyrer og kontroll, verktøy og metoder bidrar til tilstrekkelig sikkerhetsnivå.

Beslutningstakere har ikke nødvendigvis god nok innsikt i hva som kreves ettersom sikkerhetsorganisasjonen allerede er på plass i virksomheten. Det ville ifølge flere informanter alltid være fokus på å få lansert flere tjenester i markedet. Videre ble det sagt at kvaliteten, herunder sikkerhet, var underordnet politisk bestemt leveransetidspunkt. "Sikkerheten gikk dermed ut med badevannet". Ambisjonene om å ta igjen forsømmelsene på sikkerhetsområdet ble aldri realisert, fordi det var alltid krav om nye tjenester. Situasjonen som oppsto ble beskrevet som teknisk gjeld, spesielt i forhold til sikkerhet.

Lederne ble målt på leveranser og ikke på sikkerhet var ett av funnene. Det betød ikke nødvendigvis at lederne var likegyldige til sikkerhet, men at sikkerhetshensyn kom i konflikt med resultatkravene og lederne ble dermed tvunget til å prioritere. Som nevnt i kapittel 4.6 er ideer adoptert fra privat sektor til offentlig sektor som et ledd i effektiviseringen, samt modularisering av organisasjoner og kommodifisering av arbeidsoppgaver. Rasmussen (1997) har vist at effektiviseringskravene kommer i konflikt med sikkerhetskravene og at det kan gå utover sikkerhetsmarginene, jf Figur 6. Tilsvarende funn fra de Bruijne og van Eeten (2007); Schulman og Roe (2007) har vist at NPM går på bekostning av redundans og sikkerhet.

Organiseringen av prosjekter og IKT-arbeid var spesielt hos den ene virksomheten fragmentert, og de viktigste årsakene var at aktivitetene: var spredt over flere avdelinger; manglet overbygning; ikke var samlet under én felles IKT-sjef.

Arbeidet med drift, utvikling, sikkerhet, beredskap og operativ sikkerhet var enten lagt til det som ble betegnet som egne organisasjoner (dette gjaldt drift og utvikling), egne avdelinger eller seksjoner. Felles for alle virksomhetene var at utviklingsarbeid ble organisert som prosjekter med ulike roller litt avhengig av prosjektets størrelse. Sikkerhetsprosjekter må i henhold til FoI følge standardiserte arbeidsprosesser, noe som da kan betegnes kommodifisering av arbeidsoppgaver. Det systemtekniske arbeidet kan videre beskrives som modularisering, noe som også understøttes av NSMs ulike veiledninger på området.

Driftsorganisasjonen deltok i varierende grad i prosjektene, noe som dermed hadde konsekvenser for drift når prosjektene var ferdigstilt. Hos den ene virksomheten erkjente man

at organisasjonen kanskje ikke var flinke nok til å fremsette funksjonelle sikkerhetskrav, samtidig som systemer levert fra prosjektorganisasjonen ikke tilfredsstilte sikkerhetskravene. Årsakene til utfordringene med prosjektene var sammensatte og omfattet: underfinansiering; tidkrevende; spredt mellom flere avdelinger; manglet felles overbygning; mange bestillere; for dårlig kommunikasjon mellom *"søylene*". Almklov et al. (2010) omtaler fragmentering som følge av oppdeling og nye forretningsmessige grensesnitt mellom organisasjoner som opererer tett koblede systemer, noe som kan gi utfordringer med kommunikasjon og koordinering.

Samtidig var gamle systemer i ferd å nå utløpsdato, noe som skapte flere utfordringer. Flere mente drift- og utvikling burde samles under én felles IKT-sjef.

Hos den andre virksomheten var det også organisatoriske skiller mellom drift- og utvikling, og prosjektene ble ledet av systemeier. Etter ny praksis ble nå drifts- og sikkerhetspersonell oftest involvert tidligere i prosjektene, men deltakelsen varierte avhengig av prosjektleder. Driftspersonell hadde kun kapasitet til å delta i prosjektene for kortere tidsrom av gangen, da det ellers kunne få konsekvenser for driften. Det var eksempler på at prosjekter hadde blitt stoppet, blant annet fordi det ikke var tatt hensyn til sikkerhetskrav fra driftsmiljøet. Det var ellers varierende grad av sikkerhetsmessig kvalitetssikring, og leveranser av dokumentasjon kunne også by på utfordringer. Brukerne burde kobles inn i prosjektene.

Fra el-kraft sektoren fant Almklov og Antonsen (2010) at kommodifiseringen av arbeid ledet til fragmentering av arbeidsdagen for operativt personell, noe som hadde negative konsekvenser for kompetanseutvikling, oppmerksomhet mot og ansvarsfølelse for el-nettets tilstand.

Som nevnt i kapittel 5.2.8 resulterte sammenkoblinger i økt risikoeksponering og interessekonflikter, var avhengig av gjensidig tillit og avklaring av ansvarsforhold mellom mange aktører, og utløste behov for manuelle integrasjons- og kontrolltiltak.

Det krevet blant annet at man hadde et veldig godt sikkerhetssamarbeid: en god avtale som fungerte; at avtalen ble fulgt opp. Utfordringer omfattet avtale, systemer, kompetanse, og hvilken type informasjon som skulle deles mellom virksomheter og på tvers av landegrenser. Sammenkoblinger mellom virksomheter og over landegrenser var avhengig av tillit mellom partene, i motsetning til sammenkoblinger mellom systemer der tilliten hvilte på mekanismene som knyttet systemene sammen. Schiefloe (2011b) slår fast at tillit er en viktig bestanddel i interaksjon og noe som gjør det mulig å inngå i samhandling og betro seg til eller stole på andre.

Ifølge Schiefloe (2011b) handler tillit generelt om å ha positive forventninger til andres atferd i situasjoner som det er vanskelig å kontrollere, og der det er en mulighet for negativt utfall.

Sammenkoblinger handler om kommunikasjons- og informasjonsutveksling mellom flere parter. En utfordring ved slike sammenkoblinger var blant annet hvor sluttet ansvaret til den ene part og hvor begynte ansvaret til motparten. Det er aktuelle problemstillinger både i forbindelse med konfigurasjonsendringer eller ved hendelser med eksempelvis kaskaderende effekter. Avtaler om sammenkoblinger resulterte i ikke-tekniske utfordringer som handlet om ansvarsforhold, interessekonflikter og ressurskonflikter, spesielt når noe ikke virket.

Ifølge Almklov et al. (2011) er ansvarsproblematikken aktuell både for den enkelte infrastruktursektor og for de som jobber med helhetlig samfunnssikkerhetsproblematikk, for det er få målstyringsparametre som går på tvers av sektorene. I en beredskapssituasjon er det viktig at disse forholdene er avklart på forhånd, ettersom koordinering da i stor grad skjer gjennom etablert avtale.

Sammenkoblinger mellom ulike graderingsnivåer var teknisk og ressursmessig krevende å vedlikeholde. Andre utfordringer handlet om utvidelser av tjenestespekteret og konfigurasjon av trafikkmatriser; hvilke tilganger som skulle etableres; sporbarhet; hva brukere gjorde med informasjonen. En informant mente faren for kompromittering var høy.

Beslutninger på politisk nivå om sammenkoblinger på tvers av landegrenser skapte utfordringer for sikkerhetsorganisasjonen og det operative miljøet som skulle omsette vedtaket i praksis. Det var mange parter å forholde seg til i den aktuelle saken, og man manglet den tekniske løsningen for å ta imot informasjonen. Politisk nivå var altså bestiller, mens driftsorganisasjonen var utførende ledd.

Bruk av *"air-gap*" løsninger er en temporær sammenkobling som blant annet skal bidra til reduksjon av risiko sammenliknet med permanente sammenkoblinger. Slike løsninger ble brukt blant annet til sikkerhetsoppdateringer, men også her måtte man vite hva man skulle gjøre for å minimere risikoen, noe som ble tatt alvorlig ettersom det tross alt var risiko for hendelser. Det ble sagt at man kunne åpne for sårbarheter i stedet for å redusere (lukke) sårbarheter.

Sammenkoblinger mellom graderingsnivåer økte: plattformens kompleksitet; risikoeksponeringen for høyest gradert plattform, noe som krevde investeringer i fornyet sikkerhetsarkitektur. Av og til måtte man avvike fra det ved å innføre noe som ikke var standardisert. Sammenkoblingene kunne by på utfordringer i forhold til å håndtere

sikkerhetstilganger som andre lands tilgangskontroll, vedlikehold av adresser. Mange praktiske ting som krevde manuelle integrasjonstiltak, kontroller, kontrolltiltak uten at man fikk varsling fra systemet på grunn av manglende standardisering. Det økte kostnadene og utfordret kapasiteten.

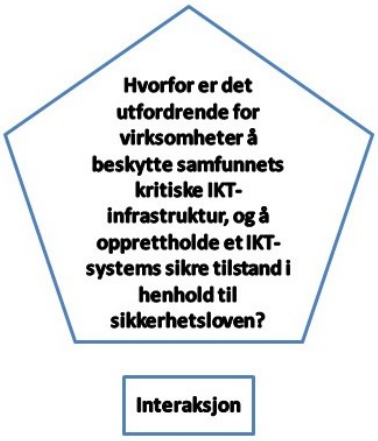
6.3.1 Sammendrag sosiale relasjoner og nettverk

Minimumskravene til sikkerhet og ressursinnsats kom i konflikt med beslutningstakernes fokus på tjenesteleveranser, enten fordi: sikkerhet ble tatt for gitt; lederne ble målt på leveranser; NPM reduserte sikkerhetsmarginene.

Sikkerhetsprosjekter skal følge standardiserte arbeidsprosesser hvor systemene utvikles gjennom moduler. Organiseringen av prosjekter og IKT-arbeid var: fragmentert; spredt på flere avdelinger/organisasjoner; hadde mange bestillere, og kommunikasjonen mellom avdelingene/organisasjonene kunne vært bedre. Driftspersonell ble koblet inn i varierende grad, og manglende deltakelse hadde resultert i at prosjekter hadde blitt stoppet.

Sammenkoblinger var teknisk og ressursmessig krevende og førte til økt kompleksitet, økt risikoeksponering og interessekonflikter. Det forutsatte et godt sikkerhetssamarbeid med avklarte ansvarsforhold og gjensidig tillit, ettersom koordinering ved beredskap hovedsakelig skjer gjennom etablert avtale fordi det er vanskelig å kontrollere andres adferd.

6.4 Interaksjon



I dette kapitlet analyseres og drøftes følgende resultater fra kapittel 5: Manglende kommunikasjons- og informasjonsflyt, samt koordineringssvikt og manglende samhandling mellom enheter; Utilstrekkelig styringsinformasjon; Knapphet på tid til å formidle sikkerhetsmessige kommentarer; Manglende lederforankring eller mindre ting ble håndtert tilfeldig avhengig av leders kapasitet; Manglende vilje til koordinering på tvers av enheter; Ikke planlagt m/sikkerhet el sikkerhet var siste sjekkpunkt før lansering av løsning; Mangelfull risikovurdering og planlegging; Undervurderte kapasitetsbehovet for både prosjekter og nye driftsoppgaver, og

manglet enten personellressurser (herunder dublerte roller) eller personellet var opptatt med andre oppgaver, noe som også hemmet fremdriften.

Det var for dårlig eller manglende kommunikasjons- og informasjonsflyt internt og mellom organisasjoner, samt koordineringssvikt og manglende samhandling mellom enheter. Forholdene hadde betydning for virksomhetenes sikkerhetstilstand; var årsaker til svikt i sikkerhetsarbeidet; alle så nær som én var kjent med hendelser siste år. Kommunikasjon, ofte i form av dokumenter, av kompleks informasjon om IKT og IKT-sikkerhet til ikke-teknologer var erkjent som et utbedringspunkt. Shannon-Weaver-modellen betinger ifølge Schiefloe (2011b) relativt like referanserammer ved innkoding, dekoding og fortolkning. En informant mente generasjonskløften mellom ledere og IKT-personell i noen tilfeller representerte en referansemessig barriere og dermed var en medvirkende årsak til for dårlig kommunikasjon.

Et annet forhold relatert til hendelseshåndtering var manglende vilje til koordinering på tvers av enheter, noe som gjorde samhandlingen skadelidende. Hos én virksomhet snakket ikke ulike enheter så godt sammen. Sikkerhetsarbeidet hos én annen virksomhet var imidlertid organisert under felles ledelse av de ulike enhetene, og erfaringen var at det bidro til bedre interaksjon mellom partene. I fortsettelsen skal vi se litt mer på utfordringene.

Som empirien viste var kommunikasjonen og samhandlingen svak, samt manglende vilje til koordinering mellom partene. Da kan man ifølge Hansen (2009) undersøke om samarbeid er formålstjenlig, samt utvikle vilje og evne til samarbeid mellom partene.

Mulige årsaker ifølge Hansen (2009) kan være motstand mot å gi hjelp og informasjon noe som kan skyldes: konkurranse mellom folk og enheter; belønning for å nå egne mål; ingen tid til å hjelpe andre; redusert makt ved å dele kunnskap. Fra empirien vet vi at tidspress var en faktor som spilte inn hvor sikkerhetsmessige kommentarer ikke ble avgitt, noe som dermed fremstod som motstand mot å gi hjelp og informasjon. Som nevnt i kapittel 4.6 definerte Mintzberg (1983) en av de fem koordineringsmekanismene som standardisering av arbeidsprosesser. Gitt sensitiviteten i informasjonen som behandles under SLs formelle rammer, så innebærer det kanskje at kommunikasjon, samhandling og koordinering utenfor de formelle rammene ikke er så lett å gjennomføre.

Det var mangelfullt fokus, forankring eller forståelse fra ledelsen, og ledelsens styringsinformasjon ble ikke vurdert som god nok.

Som nevnt i kapitlene 5.1.1, 5.2.3 ble høyere ledernivå og politisk nivå oppmerksomme på mangler i sikkerhetsarbeidet enten gjennom tilsynsrapporter eller som følge av ufordelaktig oppmerksomhet. Tidsvinduet kunne da holde seg oppe fra 2-3 måneder og opptil ett år før vinduet smekket igjen. Fenomenet illustrerer at det var krevende å nå frem til de høyeste beslutningsnivåene hvor blant annet også virksomhetenes økonomiske rammevilkår ble fastsatt. Empirien viste at styringsinformasjonen ikke ble ansett som god nok. Turner (1978) argumenterer for at viktig informasjon kan bli skjult som støy dersom det er mye overskuddsinformasjon i budskapet. Formidling av teknisk komplisert informasjon til ikke-teknologer var utfordrende for avsender og krevende å forholde seg til for mottaker som i mange tilfeller var ledelse på ulike nivåer. Det var eksempler på informanter som da aktivt oppsøkte eksperthjelp i virksomheten for å få verifisert innholdet og forvisset seg om at budskapet ble forstått korrekt. Det hadde stedvis blitt jobbet med utbedringer for å gjøre rapporteringen mer relevant for ledelsen, men flere respondenter mente det kunne gjøres mer. Bakgrunnen for det var blant annet kort oppmerksomhetsvindu hos ledelsen, og informasjon som ikke ble oppfattet som relevant for ledelsen ville da ikke få nødvendig fokus ifølge informanter. En mulig forklaring på mangelfull forståelse for sikkerhetsbehov og kompleksitet kan derfor handle om kvaliteten på informasjonen. I endringsprosesser er det ifølge Amundsen og Kongsvik (2008) sentralt med nøyaktig, hyppig og etterrettelig informasjon via formålstjenlige kanaler. Sikkerhetsarbeid kan sies å handle om å skape forbedringer fra uønsket til ønsket tilstand, noe som forutsetter felles forståelse mellom partene for de problemstillinger man søker å løse. Lederen som oppsøkte eksperten for nødvendige avklaringer benyttet seg dermed av kretsløpsmodellen for kommunikasjon hvor partene ifølge Amundsen og Kongsvik (2008); Jacobsen og Thorsvik (2007) veksler på rollene sendere og mottakere som koder og dekoder budskap hvor formålet i stor grad er forståelse. Eksemplet underbygger også at det var forbedringspotensiale i utformingen av ledelsesinformasjonen.

En annen utfordring kan være at forebyggende sikkerhetsarbeid handler om å sørge for at hendelser ikke skjer[33], og dersom man gjør den jobben på en god måte risikerer sikkerhetsorganisasjonen å bli *"usynlig"* eller i hvert fall ikke så veldig godt synlig. Det er i

[33] Hvis det ikke skjer hendelser, så er det lett å glemme ordspråket som blant annet er brukt i forbindelse med sikkerhetsdagene i Midt-Norge, og som på en god måte viser dynamikken i sikkerhetsarbeidet: *"sikkerhet må skapes og gjenskapes hver dag."* Hentet fra https://www.ntnu.no/sikkerhetsdagene

den forbindelse verdt å ta med formuleringene til Weick (1987) som i grunnen tegnet opp et situasjonsbilde som kan bidra til å forklare stedvis lunken forståelse for sikkerhetsarbeidet.

> Reliability is a dynamic Non-Event. Reliability is also invisible in the sense that reliable outcomes are constant, which means there is nothing to pay attention to. Operators see nothing and seeing nothing, presume that nothing is happening. If nothing is happening and if they continue to act the way they have been, nothing will continue to happen. This diagnosis is deceptive and misleading because dynamic inputs create stable outcomes. (Weick, 1987:118)

I tillegg rapporterte informanter at sikkerhet ikke nødvendigvis ble ansett som det viktigste ledelsen skulle ta seg av. Når det gjelder å fange ledelsens oppmerksomhet er en observasjon at feltet hendelseshåndtering har fått stigende oppmerksomhet i takt med de siste årenes økning i antall dataangrep.

Turner (1978), Pidgeon og O'Leary (2000) modell om menneskeskapte ulykker peker på manglende informasjonsflyt og feilaktige fortolkninger mellom individer og grupper som rotårsak til en lang rekke hendelser som til slutt resulterer i katastrofe. Sett i retrospekt kunne man ifølge Turner (1978) forhindret de fleste ulykker og katastrofer dersom man kjente årsaken til at informasjon ikke ble fanget opp eller ble mistolket.

Informanter rapporterte om stort tidspress blant annet som følge av stort arbeidspress og få personellressurser, og da ble ikke alltid dokumentasjon ferdigstilt. Sikkerhetsorganisasjonen ble koblet inn for sent i eksempelvis anskaffelsesprosessen til å kunne få avgitt sikkerhetsmessige kommentarer. Tidspresset og mange arbeidsoppgaver var derfor en grunn til at samhandlingen ikke var optimal, og begge forholdene resulterte dermed i sikkerhetsmessige forhold av betydning som ikke ble synliggjort overfor ledelsen. Effektivitetspresset mot de ansatte er også et resultat av NPM ifølge Schiefloe og Værnes (2010). Under stort arbeidspress vil spørsmål om å yte hjelp ifølge Hansen (2009) bli betraktet som en byrde ettersom hjelperen kommer på etterskudd med sitt eget arbeid. Avveiningene står da ifølge Hansen (2009) mellom å gjøre eget arbeid og ikke hjelpe andre, eller å hjelpe andre men få gjort mindre arbeid. Det første forholdet vil da kunne oppfattes som manglende samhandling, mens den egentlige årsaken er den enkeltes avveininger i forhold til leveransekravene.

Virusangrep i komplekse systemer og påfølgende utfordringer med å detektere og forstå symptomer på eventuelle følgeskader var problemstillinger som informanter brakte frem. Dette

berører flere av Turner (1978) og Pidgeon og O'Leary (2000) fire former for informasjonssvikt. I følge informanter kunne det være relatert til et virusangrep man ikke hadde sett før; at man ikke fikk satt sammen nødvendig informasjon som følge av manglende rapportering fra operativt nivå eller manglende deling av informasjon mellom andre involverte aktører; at informasjonen ble feiltolket som uskadelig; at signalene kanskje fantes der, men ikke ble fanget opp på grunn av tidspress.

Det var ikke planlagt med sikkerhet eller sikkerhet var siste sjekkpunkt før lansering av løsning, og en forklaring på det var manglende ledelsesforankring og forståelse for utøvelse av sikkerhetsarbeid. Konsekvensene var at det dermed skapte utfordringer for ferdigstilling av nye tjenester. Det var eksterne krav til nye tjenester og leveransetidspunkt, og da enten fra politisk nivå eller fra kunder ettersom IKT-avdelingene ble betraktet som et serviceapparat. Sikkerhet i løsningen ble da enten en hastverksløsning eller noe som skulle legges til senere. Målkonflikter er én av kildene til risikoatferd hos velmenende organisasjoner (Reiman og Oedewald, 2009:40).

Ett av flere eksempler på målkonflikter der leveranse av tjenester kommer i konflikt med krav til sikkerhet, er felles innloggingsportal til offentlige tjenester som i sin tid ble foreslått av moderniseringsminister Morten Meyer[34]. Portalen skulle etter planen gi tilgang til flere tjenester inneholdende sensitiv informasjon, noe som dermed medførte høyere sikkerhetskrav enn for tjenester med ikke-sensitiv informasjon. Lanseringstidspunktet ble endret flere ganger, og i 2006 presenterte fornyings- og administrasjonsminister Heidi Grande Røys løsningen[35]. En av årsakene til utsettelsene og at løsningen omfattet kun de laveste sikkerhetsnivåene i starten, var at ønsket løsning for høyeste sikkerhetsnivå ikke lot seg realisere i tråd med politiske vedtak innen den fastsatte tidshorisonten, samt behovet for å sikre tillit til løsningen. En arbeidsgruppe foreslo i 2007 innføring av frivillig nasjonalt ID-kort[36] hvor brukeren kunne velge eller fravelge

[34] NTB. (2006). *MinSide utsatt på ubestemt tid*. Hentet 06.01.2017 fra http://www.bt.no/nyheter/okonomi/MinSide-utsatt-pa-ubestemt-tid-127820b.html; Ryvarden. (2006). *Departementet bekrefter MinSide-lansering*. Hentet 06.01.2017 fra http://www.digi.no/artikler/departementet-bekrefter-minside-lansering/281363; Morten Meyer går til IBM Norge (2005). Hentet 06.01.2017 fra http://www.digi.no/artikler/morten-meyer-gar-til-ibm-norge/318137.

[35] Fornyings- og administrasjonsdepartementet. (2006). *Lansering av innbyggjarportalen Miside*. Hentet 06.01.2017 fra https://www.regjeringen.no/no/aktuelt/lansering-av-innbyggjarportalen-miside/id440091/.

[36] Justis- og politidepartementet. (2007). *Nasjonalt ID-kort, Sluttrapport 10. februar 2007*. Hentet 06.01.2017 fra https://www.regjeringen.no/globalassets/upload/jd/vedlegg/id-kort-sluttrapport.pdf.

aktiv eID. Ifølge sluttrapporten skulle eID baseres på sertifikatklasse Person Høyt i henhold til Kravspesifikasjon for PKI i offentlig sektor[37]. ID-kortet var planlagt lansert i 2017, men er nå utsatt til 2018 blant annet av sikkerhetsmessige grunner[38].

Et annet eksempel av betydning og som kan ha konsekvenser for samfunnssikkerhet er innføringen av Avanserte måle- og styringssystemer (AMS)[39] i Norge. De opprinnelige planene fra politisk nivå var at AMS skulle være på plass hos alle husstander i løpet av 2015[40], men planene ble senere justert til full utrulling i løpet av 2017[41] og nå er målsettingen 2019[42]. En medvirkende årsak til utsettelsene var usikkerhetsfaktorer knyttet til sikkerhetskravene.

Reason (1997b) nevner at den mest sannsynlige og uunngåelige årsaken til flere småflyulykker i Australia i tidsrommet 1993-1994 var målkonflikten til *Australian Civil Aviation Authority* (ACAA) som altså var mer opptatt med å synliggjøre og markedsføre småflyselskapet Minarch Air enn å ivareta sikkerhetsbehovene for passasjerene. En medvirkende årsak til at ACAA handlet som de gjorde var ifølge Reason (1997b) at dereguleringer i flyindustrien hadde resultert i at ACAA var delfinansiert av flyselskapene de skulle overse, og at de dermed var opptatt av å holde liv i flyselskapene.

Som Rasmussen (1997) poengterer søker samfunnet å kontrollere sikkerhet gjennom lovverket hvor sikkerhet har høy prioritet, men det samme har andre samfunnsområder som eksempelvis arbeid og handelsbalanse. Figur 5 illustrerer stegene fra politiske vedtak, fortolkninger,

---

[37]Fornyings-, administrasjons- og kirkedepartementet. (2010). *Kravspesifikasjon for PKI i offentlig sektor*. Hentet 06.01.2017 fra https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/; https://www.regjeringen.no/no/aktuelt/ny-kravspesifikasjon-for-pki-i-offentlig/id621773/

[38] Ruud. (2016). *Nasjonalt ID-kort utsatt igjen*. Hentet 07.01.2017 fra http://www.aftenposten.no/norge/Nasjonalt-ID-kort-utsatt-igjen-606640b.html (Sist lest); Aftenposten, trykt utgave, 06.01.2017.

[39] Funksjon og drift av AMS er regulert av Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. (1999) Forskrift 11. mars 1999 nr 301 om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. Hentet 07.01.2017 fra https://lovdata.no/dokument/SF/forskrift/1999-03-11-301

[40] NVE, (2015) *Smarte målere (AMS), Status og planer for installasjon og oppstart pr 1. kvartal 2015*, Oslo, 77/2015, ISBN 978-82-410-1124-5, Hentet 07.01.2017 fra http://publikasjoner.nve.no/rapport/2015/rapport2015_77.pdf

[41] Sviland, Øverjordet, Hårstad, Rydland og Johnsen. (2013). *PROSJEKTRAPPORT TET4850 EiT SMART GRIDS VÅR 2013, FORBRUKER OG NETTSELSKAPS FORDELER VED INNFØRING AV AVANSERTE MÅLE- OG STYRINGSSYSTEM*. Hentet 07.01.2017 fra http://smartgrids.no/wp-content/uploads/sites/4/2013/06/Forbruk-og-nettselskapers-fordeler-ved-innføring-av-AMS.pdf

[42] NVE, (2015) *Smarte Strømmålere (AMS)*. Hentet 07.01.2017 fra https://www.nve.no/elmarkedstilsynet-marked-og-monopol/sluttbrukermarkedet/smarte-strommalere-ams/

implementering, operasjonalisering til operatørnivået som i IKT-sikkerhetssammenheng er ingeniører og annet teknisk personell. Det blir dermed ganske stor avstand fra politiske beslutninger om hvilke IKT-sikkerhetstiltak som skal realiseres innen en gitt tidsramme til det operative nivået hvor vedtaket skal implementeres i praksis.

Resultatet er ifølge Rosness et al. (2010) at det oppstår inkonsekvenser og in-optimale beslutninger. Rosness et al. (2010) og Reason (1997b) argumenterer for at sikkerhetsmarginene forvitrer, noe som også er fremstilt i Figur 6. Figuren viser at grensene for akseptabelt sikkerhetsnivå gradvis flyttes mot en mer uakseptabel grense som følge av ledelsens effektivitetskrav og økonomiske rammer, samt grensen for uakseptabel arbeidsmengde i forhold til minst mulig innsats. Tre risikoreduserende strategier ved målkonflikter er ifølge Rosness et al. (2010): å synliggjøre grensene for uakseptabel risiko for relevante aktører; redusere arbeidsbelastningen; yte press som favoriserer sikre handlinger.

Flere informanter pekte på manglende forståelse for IKT og IKT-sikkerhet på høyere beslutningsnivåer, og da ikke bare avgrenset til politisk ledelse. Spesielt følgende tre forhold kunne påkalle tilstrekkelig oppmerksomhet fra høyere beslutningsnivå som politisk nivå: negative hendelser; alvorlige avvik presentert i tilsynsrapporter; alvorlige avvik presentert i risikoanalyser.

Tilbakekoblingssløyfen fra mer operativt nivå til høyere beslutningsnivå ser derfor ut til å være av mer reaktiv karakter som vist i figur 4. Som en informant beskrev det: *"du er nødt til å ha operativ erfaring for å forstå hvor ufattelig komplekst dette er."* Dersom man manglet den dimensjonen ble ikke nødvendigvis et politisk vedtak enkelt å gjennomføre i praksis, noe som er belyst i denne casestudien. For å unngå målkonflikter i situasjoner hvor det foregår mye aktivitet foreslår Rosness et al. (2010) å gi tilgang til mer informasjon, og denne strategien kan trolig også brukes for å skape bedre forståelse mellom operative utfordringer og politiske samt regulative nivåer.

Mangelfull risikovurdering og planlegging skapte utfordringer både for drift- og forvaltningsoppgavene. FoI angir krav til planlegging av IKT-sikkerhet i systemer som skal behandle gradert informasjon. FoO fokuserer mest på fysiske sikringstiltak og er ikke like tydelige på IKT–sikkerhetskravene som FoI, med to unntak: § 3.1 i omhandler generelle krav til beskyttelsen som blant annet omfatter grunnsikring, barrierer, deteksjonstiltak, verifikasjonstiltak, reaksjonstiltak; mens § 3-3 omhandler tilrettelegging for beskyttelse av

IKT-infrastruktur og at NSM kan bestemme nærmere hvordan eventuell internettilknytning skal settes opp og forvaltes. Grunnsikringskravene i FoO viser til FoA når det gjelder utforming av instrukser og prosedyrer tilpasset virksomhetens størrelse og kompleksitet ved økt risiko. De generelle kravene i FoO kan derfor basert på definisjonene i reguleringsbestemmelsene i kapittel 4.4 og diskusjonen i kapittel 6.1 sies å ligge nærmere funksjonelle krav i motsetning til kravene i FoI som har en preskriptiv innretning. Informasjonssystemer som er en del av samfunnskritisk infrastruktur kunne være underlagt FoO samtidig som informasjonen ifølge informanter paradoksalt kunne være ugradert. Det var dermed ikke like klart hvorvidt informasjonen skulle sikres i henhold til FoI eller ikke. Dersom informasjonseier i et slikt tilfelle ikke trenger å forholde seg til kravene i FoI, men kun forholder seg til kravene i FoO blir derfor tolkningsrommet med hensyn på IKT-sikkerhetskravene større. Det ser derfor ut til at følgende to tilfeller utgjør en gråsone i reguleringen av KI: den delen av KI som befinner seg utenfor SLs reguleringsområde; ugraderte systemer som både er en del av KI og er innenfor SLs reguleringsområde. Det er dermed ikke gitt at eiere av informasjonssystemer, som er en del av samfunnskritisk infrastruktur, beskytter systemene med utgangspunkt i FoI. Derfor kan det være grunn til å stille spørsmål ved hvilke sikkerhetsprinsipper anvendes for beskyttelse av systemer som befinner seg i gråsonen etter og om prinsippene er gode nok i omgivelser med hurtig skiftende trusselbilde. Flere informanter betraktet FoI med veiledninger som gode prinsipper og retningslinjer som med enkelte tilpasninger også kunne anvendes for sikring av ugraderte systemer.

Mangelfull risikovurdering og planlegging kan også ha sammenheng med at kurs- og utdanningstilbudene som drøftet i kapittel 6.5 ikke var dekkende. På den annen side var det ifølge informanter ikke eksplisitte kompetansekrav i regelverket om IKT-risikovurderinger for sikkerhetsledere og datasikkerhetsledere som drøftet i kapittel 6.1, noe som var en mulig forklaring på fraværet av kurs- og utdanningstilbud innen feltet.

Både i forbindelse med IKT-investeringer og prosjekter var et gjennomgående trekk at virksomhetene undervurderte kapasitetsbehovet for både prosjekter og nye driftsoppgaver. Det hadde blant annet sammenheng med at man enten manglet personellressurser (herunder dublerte roller), eller personellet var opptatt med andre oppgaver, noe som også hemmet fremdriften. Hos to virksomheter var det dessuten ikke utstrakt samhandling mellom avdelingene.

Det å konvertere til ny teknologi og/eller endre arbeidsrutiner og –prosesser kan også bety tap av produktivitet i en overgangsperiode fordi organisasjonen trenger tid til å omstille seg (Meyer og Stensaker, 2011:21).

I forbindelse med implementering av store IKT-prosjekter påpeker Meyer og Stensaker (2011) at det er ganske vanlig med bruk av vikarer for å ivareta den daglige driften, samtidig som ansatte får brukt nok tid på opplæring. I motsatt fall er konsekvensene ifølge Meyer og Stensaker (2011) dårlig utnyttelse av systemene og lang gjennomføringstid som et resultat av at virksomhetene undervurderer kapasitetsbehovet. Selv om det er relasjonen virksomhet og brukere som er beskrevet her, kan det argumenteres for at virksomheten kan undervurdere kapasitetsbehovet også i driftsorganisasjonen når det gjelder den type omstillings- og endringsprosesser som innføring av IKT-systemer faktisk innebærer.

6.4.1 Sammendrag interaksjon

Det oppsto svikt i sikkerhetsarbeidet og hendelseshåndteringen som følge av dårlig eller fraværende kommunikasjons- og –informasjonsflyt. Samhandlingen og hendelseshåndteringen mellom enheter ble skadelidende som følge av koordineringssvikt og uvilje mot koordinering. Årsakene til svak koordinering, kommunikasjon, og samhandling kan skyldes motstand mot å be om eller å ta imot hjelp og informasjon, noe som igjen kan bunne i: lokal kultur; status; selvtillit; frykt; konkurranse; smale incentiver; tidspress.

Mens mangelfullt fokus, forankring eller forståelse fra ledelsen dels kunne forklares som følge av ikke-hendelser, bidro kritiske tilsynsrapporter og hendelser til oppmerksomhet fra høyeste beslutningsnivåer som da kunne vedvare i opptil ett år. Ledelsens styringsinformasjon ble ikke vurdert som god nok, og modellen om menneskeskapte ulykker trekker frem mangelfull informasjon eller feiltolking som rotårsak til mange hendelser.

Når det gjelder årsakene til samhandlingsproblemer mellom partene og ikke ferdigstilt dokumentasjon, viser drøftingen foran med støtte i teorien at tids-, og arbeidspresset samt leveransekravene er mulige forklaringer på utfordringene.

Sikkerhetsorganisasjonen ble koblet inn for sent i eksempelvis anskaffelsesprosessen til å kunne få avgitt sikkerhetsmessige kommentarer.

Det var ikke planlagt med sikkerhet, eller sikkerhet var siste sjekkpunkt før lansering av løsning, noe som resulterte i målkonflikt mellom sikkerhet og tjenesteleveranser. Risikoatferden hadde

sammenheng med manglende ledelsesforankring og forståelse for sikkerhetsarbeid, og slike in-optimale beslutninger eroderte dermed sikkerhetsmarginene. Følgende tre forhold resulterte i oppmerksomhet fra høyere beslutningsnivå: negative hendelser; alvorlige avvik i tilsynsrapporter; alvorlige avvik i risikoanalyser.

Mangelfull risikovurdering og planlegging skapte utfordringer både for drift- og forvaltningsoppgavene. Ugraderte informasjonssystemer under FoO som samtidig var en del av KI havnet i en gråsone med hensyn på krav til sikringstiltak, og et tilsvarende forhold gjaldt ugraderte informasjonssystemer under SL. Et annet forhold som kunne forklare utfordringen med IKT-risikovurderinger var at regelverket manglet spesifikke kompetansekrav til IKT-risikovurderinger for sikkerhetsledere og datasikkerhetsledere.

Innføring av ny teknologi; nye rutiner; nye arbeidsprosesser resulterte i midlertidig produktivitetstap, som resultat av at virksomhetene undervurderte kapasitetsbehovet for både prosjekter og drift. Det hadde blant annet sammenheng med enten manglende personellressurser (herunder dublerte roller) eller personellet var opptatt med andre oppgaver, noe som også hemmet fremdriften.

6.5 Kompetanse, verdier og holdninger

I dette kapitlet analyseres og drøftes følgende resultater fra kapittel 5: Manglende eller for lav kompetanse, herunder ikke-dublert kompetanse; Manglende forståelse hos ledelsen for kompetansebehovet; Kurs- og utdanningstilbud var enten ikke tilgjengelige eller dekket behovet; Endret bruksmønster på IKT-systemet; Begrensede kompetansebudsjetter i forbindelse med nyanskaffelser av teknologi eller opprettholdelse av kompetanse; Menneskelige feil, feiltolkning eller manglende forståelse for at det hadde oppstått en feil eller sikkerhetsrelatert hendelse, og ble dermed ikke innrapportert; Fulgte ikke sikkerhetsbestemmelsene og avvek fra etablerte rutiner; Brukeratferd; høyt arbeidspress; Turnover.

Alle informantene i A og halvparten av informantene i B og C mente kompetansebehovet ikke var tilfredsstilt godt nok. Aksept hos ledelsen; systematisk satsning på kompetansebygging og

tid, penger og budsjetter var imidlertid årsaker til at halvparten av informantene i B og C også mente det var mye bra. Årsakene til gjenstående utfordringer var sammensatte og kan oppsummeres slik: manglende forståelse hos ledelsen; kurs- og utdanningstilbud var enten ikke tilgjengelige eller dekket behovet; endret bruksmønster på IKT-systemet; begrensede budsjetter; ikke eksplisitte krav til risikovurderinger; turnover; mer kompleks sikkerhetsdokumentasjon.

Flere av informantene mente det var et kontinuerlig behov for å styrke kompetansen. Det var imidlertid ingen av informantene som koblet kompetansebehovet direkte med hyppige teknologiske skift og endringer i trusselbildet, noe som etter undertegnedes vurdering understøtter behovet for kontinuerlig kompetansebygging.

Resultatene viste at det kunne inntreffe svikt i sikkerhetsarbeidet og hendelseshåndtering. Årsakene ble antydet som manglende eller for lav kompetanse, herunder ikke-dublert kompetanse. Det innebar dermed at virksomheten ikke hadde nok personell på alle områdene til å inneha det LaPorte og Consolini (1991) kaller organisatorisk redundans. Det vil eksempelvis si at en person utfører konfigurasjonsendringer i brannmur, mens en annen person samtidig kontrollerer utførelsen. En slik tilnærming kan være bra når man gjennomfører kritiske endringer i komplekse systemer med lav feiltoleranse. Enkelte informanter sa man var godt på vei med å nå målsettingen om å styrke organisasjonen med hensyn på bemanning og kompetanse for å redusere organisatorisk sårbarhet, og dermed også styrke sikkerhetsnivået. Reason (1997b) beskriver Mintzbergs tre Cer: *commitment*; *competence*; *cognisance* som nødvendige drivere i sikkerhetsarbeidet. Sikkerheten i virksomhetens IKT-system og mulighetene for å nå fastsatte sikkerhetsmål avhenger ifølge Reason (1997b) av at det er tilsatt nødvendig teknisk kompetanse, som igjen er betinget av ledelsens engasjement, motivasjon, nødvendig antall ressurser med rett kvalitet, samt status i virksomheten.

Manglende forståelse hos ledelsen for kompetansebehovet resulterte da i at man ikke fikk tilsatt nødvendig personell med ønsket kompetanse. Partene hadde altså ikke felles forståelse for behovene. Det å skape felles forståelse er som drøftet i kapittel 6.4 tett knyttet til kommunikasjon, og ulike referanserammer kan ifølge Schiefloe (2011b) medføre misforståelser, at vi snakker forbi hverandre eller ikke forstår hverandre. Å synliggjøre konsekvensene var et viktig virkemiddel for å skape forståelse ifølge Meyer og Stensaker (2011). I denne casestudien var ifølge informanter en konsekvens at det ble benyttet innleid arbeidskraft. På den annen side mente enkelte informanter det også var vel så mye spørsmål om

å utnytte kompetansen rett, at personell ble brukt til de rette oppgavene. Kjernen i problemstillingen var altså ledelsens manglende forståelse for behovet ifølge informantene. Grunnlaget for treffe beslutninger om kompetansemidler er blant annet knyttet meningsdanning som ifølge Weick (1995) er en prosess hvor individer registrerer og tolker det de: hører; observerer; blir fortalt, inn i et rammeverk som gjør det mulig å fatte, forstå, forklare, kategorisere, ekstrapolere og forutsi. Meninger revideres kontinuerlig i kjølvannet av påfølgende hendelser og andres tolkninger som Weick (1995) uttrykker det. Som vi så i kapittel 6.4 var det blant annet manglende kommunikasjons- og informasjonsflyt, samt behov for utforming av bedre styringsinformasjon. Det er derfor ikke tydelig om det var skapt enhetlig forståelse for problemstillingen i alle relevante organisasjonsledd. Som illustrert i Figur 7 innebærer organisatorisk og hierarkisk avstand mellom operativt ledd og ledelsen at det kan by på utfordringer å skape forståelse hos ledelsen for hvilke problemstillinger operativt personell møter daglig i den skarpe delen av virksomheten. Et annet forhold som kan forsterke den utfordringen er ledelse som kommer og går, samt omorganiseringer, noe alle virksomhetene på ulike tidspunkter hadde vært igjennom. Ett forhold til, som også er drøftet i kapitlene 5.2.4, 5.2.5, 5.2.6 og 6.2, var budsjettene som begrensende faktor.

Kurs- og utdanningstilbud var enten ikke tilgjengelige eller dekket behovet. Kurs i risikovurderinger var mangelvare, og spesialkurs fra eksterne leverandører var ikke tilgjengelige når behovet var tilstede. FFI-rapport 2007/01204 (2007) påpeker mangelfull forståelse av både IKT-systemer og fagområdet risikoanalyse. Det første forholdet kunne henge sammen med det som ble diskutert i kapittel 6.1 om fravær av kompetansekrav til risikovurderinger for sikkerhetsledere og datasikkerhetsledere. Det siste forholdet resulterte i at det tok lang tid før man fikk oppdatert kompetansen, og virksomheten fikk dermed avvik på kompetanse. Viktigere enn påviste avvik i samband med revisjoner er at det dermed oppstår en organisatorisk sårbarhet som ikke blir tettet tilfredsstillende før virksomheten har opparbeidet nevnte kompetanse. Forvaltning av kompetanse handler også ifølge Reiman og Oedewald (2009) om opplæring og sosialisering av nyansatte gjennom kunnskapsoverføring fra erfarne til mindre erfarne medarbeidere. Så internopplæring er en mulighet til å bygge opp nyansatte, i alle fall til passende kurs blir tilgjengelig. Dette ble også praktisert hos enkelte så langt tiden strakk til, men som vi så tidligere var tid mangelvare.

I samband med innføring av ny teknologi var det begrensede muligheter til å bygge opp kompetansen på ny teknologi eller til å kunne opprettholde kompetansenivået. Halvparten av

informantene mente det var krevende å få på plass nødvendig kompetanse ved innføring av ny teknologi. Årsakene til utfordringene var: avklaringer av kompetansebehov på hvilke nivåer; stort arbeidspress; nye krav; begrensede kompetansemidler; tidsfrist for ferdigstilling; økt kompleksitet ved integrasjon med gammel teknologi.

Mye av kompetansebehovet var av spesialisert karakter, og det var ikke alltid satt av midler til kompetanseheving i forbindelse med innføring av ny teknologi. Flere pekte på at det var vanskelig å få spesialkurs til eksempelvis kroner 15.000,- for én person. Det var eksempler på at kompetanseheving hos gruppe 1 ble prioritert fremfor hos gruppe 2, med den konsekvensen at det da ikke var rom for kompetansebygging hos gruppe 2.

Ved innføring av ny teknologi, nye sikkerhets- og effektiviseringskrav, endret jobbinnhold og arbeidspraksiser for eksempelvis vedlikeholds personell, kan ifølge Reiman og Oedewald (2009) bety at noen gamle vaner og begreper må avlæres. For eksempel kunne det være relevant i forbindelse med endret bruksmønster på IKT-systemet gjennom etablering av en ny brukergruppe og mer operativ bruk av IKT-systemet, noe som resulterte i behov for mer kompetanseoppbygging hos driftspersonell. Mer operativ bruk av systemet økte også tilgjengelighetskravene til IKT-systemet.

I kjølvannet av NPN ble grensene for sikker operasjon utfordret av ledelsens krav til effektivitet, slik som illustrert i Rasmussens Figur 6 og drøftet i kapittel 6.4. En medvirkende årsak til at virksomhetene ikke fikk gjennomført kompetanseoppbygging ved innføring av ny teknologi var blant annet høyt arbeidspress. Ettersom virksomhetene ikke byttet ut alle løsninger samtidig, måtte driftsorganisasjonen følgelig opprettholde kompetanse på *"gamle*" systemer og samtidig bygge opp ny kompetanse. Innføring av nye løsninger forsterket dermed allerede høyt arbeidspress. I tillegg var det som nevnt før stramme økonomiske rammer, og i noen tilfeller politisk bestemte leveransefrister.

En mulig forklaring på mangelfull kompetansebygging før introduksjon av ny teknologi kan også sees i sammenheng med variabel deltakelse av driftspersonell i utviklingsprosjektene som diskutert i kapittel 6.1. Hyppige teknologiske skift forsterker behovet for vedlikehold av kompetanse, og kompetansebygging blir dermed en kontinuerlig og viktig del av sikkerhetsarbeidet.

Sikkerhetsarbeidet og håndtering av hendelser kunne svikte på grunn av menneskelige feil; feiltolkning; manglende forståelse for at det hadde oppstått en feil eller sikkerhetsrelatert

hendelse. Det siste forholdet kunne dermed lede til at saken ikke ble innrapportert. Menneskelige feil er ifølge Reason (1997b) en konsekvens og ikke en årsak, men blir ofte nevnt som årsak på grunn av menneskets natur som psykologene kaller grunnleggende attribusjonsteori. Ifølge Reason (1997b) er det lettere å skylde på folk fremfor situasjonen, og den del av forklaringen er illusjonen om menneskets frie vilje. Feilsituasjoner har imidlertid gjerne multiple årsaker som eksempelvis: personlige, oppgaverelaterte, situasjonsbetingede og organisatoriske ifølge Reason (1997b).

Svikt kan ifølge Turner (1978) skje ved akkumulering av feil gjennom motstridende hendelser i inkubasjonsperioden ved enten: ingen kjenner hendelsen; hendelsen er kjent, men ikke fullt ut forstått av alle parter og dermed heller ikke implikasjonene av hendelsen. Årsakene omfatter ifølge Turner (1978) følgende fire forhold: 1) hendelser ble ikke oppdaget eller misforstått pga feil antakelser; 2) motstridende hendelser ble ikke oppdaget eller misforstått pga vanskeligheter med å håndtere informasjon i komplekse situasjoner; 3) varsler om faresignaler ble ikke lagt merke til eller misforstått som følge av vanlig og veldokumentert menneskelig motstand mot å frykte det verste; 4) brudd på formelle regler og reguleringer ble akseptert som normalt, der hvor det ikke fantes oppdaterte prosedyrer. I teorikapitlet 4.3 så vi at SIEM-verktøy eksempelvis kan være bra for å understøtte sikkerhetsarbeidet og håndtere hendelser, men det krever at man vet hva man skal se etter og investerer mye tid til konfigurasjonsarbeid for å få god oversikt i komplekse IKT-systemer. Fra empirien vet vi drift ikke alltid fikk ønskede verktøy, noe som innebar mer manuelt arbeid som nevnt i kapitlene 5.2.1, 5.2.4 og muligheter for feil i utførelsen. Tilfellet som utløser hendelser er ifølge Turner (1978) uforutsigbart; innebærer vanligvis nye fortolkninger; avdekker motstridende hendelser fra inkubasjonsperioden; kan resultere i mange følgeskader. Det kan derfor bli krevende å håndtere kaskaderende hendelser enten virksomheten har hensiktsmessig verktøy eller ikke, ettersom det både må gjøres løpende fortolkninger og det kan være ukjente trusler som verktøyet eller manuelle prosesser ikke klarer å fange opp. Og dersom man ikke fanger opp noe eller mistolker, blir det heller ikke noe å rapportere. Diskusjonen foran illustrerer kompleksiteten i: sikkerhetsarbeidet; fortolkninger; håndtering av hendelser; noe som dermed hadde betydning for sikkerhetstilstanden i virksomhetene.

Ifølge informanter var det ikke nødvendigvis alle som så på tilgjengelighet som sikkerhetsrelatert.

Feiltolkninger eller manglende forståelse for feil eller situasjoner som oppstod kunne ha sammenheng med arbeidspraksis, holdninger eller kompetanse. Tilsvarende funn var ifølge Schiefloe et al. (2005); Schiefloe og Vikland (2007) resultatet av granskningen etter ulykken på Snorre A, men med en forskjell at lokal kompetanse var vesentlig for å håndtere den alvorlige situasjonen som oppsto.

Et annet forhold som trekker i samme retning er manglende eller mangelfull dokumentasjon i kombinasjon med komplekse systemer, som isolert sett kan være krevende nok selv ved drift- og vedlikehold av enkle systemer. I kombinasjon med komplekse systemer, som også er koblet mot andre virksomheter, blir utfordringen enda større. Dokumentasjonen representerer på mange måter det vi kan kalle virksomhetens formelle hukommelse. Ettersom det kan være feil i dokumentasjonen, får dermed virksomhetens uformelle hukommelse stor betydning. Kapittel 6.1 omtalte en et IKT-system som var for dårlig dokumentet, hvor eksperter på ulike felt ble kalt sammen i forbindelse med en hendelse for å tegne opp hvordan systemet var designet og samvirket. Ekspertene jobbet da sammen for å finne årsakene til hendelsen. Et annet eksempel var at rutinebeskrivelsene ikke dekket en aktuell hendelse, og personell måtte da improvisere. Det fordret at personellet har både gode formelle kunnskaper, lokal kunnskap og *"tacit knowledge*" eller taus kunnskap som ifølge Clegg et al. (2011) bruker når du gjør noe, men som ikke nødvendigvis kan uttrykkes. Et eksempel i IKT-sammenheng kan være rutiner og praksiser i forbindelse med installasjon av komponenter hvor teknisk personell ikke følger den beskrevne rutinen, fordi vedkommende sitter med ikke-uttalte kunnskaper om en bedre prosedyre som reduserer feilraten eller fordi vedkommende er den eneste som forstår hvordan komponenten kan påvirke gamle installasjoner. I de nevnte eksemplene så kan taus kunnskap overføres til eksplisitt kunnskap. Erfaring og lokal kunnskap var i denne casestudien altså viktig for å kunne forstå de komplekse IKT-systemene, og det var viktig for å kunne utforme god sikkerhetsdokumentasjon. For å kunne ha godt begrep om IKT-systemets sikre tilstand er det vesentlig at dokumentasjonen gjenspeiler den faktiske tilstanden.

Resultatene viste at sikkerhetsbestemmelser ikke ble fulgt og at det forekom avvik fra etablerte rutiner, noe som utfordret sikkerhetstilstanden og kunne lede til svikt i sikkerhetsarbeidet eller hendelseshåndtering. Tidspress, latskap, menneskelige feil eller at man ikke anså saken som viktig nok i øyeblikket var medvirkende årsaker til at man avvek fra rutiner. Andre faktorer var mangelfulle rutiner eller at det oppsto hendelser som ikke var dekket av rutinebeskrivelsene. Manuelle rutiner var tatt i bruk spesielt der hvor man ikke hadde tilstrekkelige verktøy til å

understøtte eksempelvis automatisering. En underliggende årsak til enkelte manuelle rutiner i virksomheten var altså fravær av teknologiske hjelpemidler, noe som dermed også resulterte i et økt arbeidspress på de som skulle drifte systemene.

Reason (1997b) skiller mellom: rutinemessige brudd; brudd for å optimere; og nødvendige brudd. Det første forholdet handler ifølge Reason (1997b) om at en velger minste motstands vei; spesielt hvis omgivelsene ikke belønner etterlevelse av rutiner; straffer brudd på rutinene; eller prosedyrene er tungvinte. Det andre forholdet kan ifølge Reason (1997b) skyldes mange ting som ikke nødvendigvis er relatert til funksjonelle sider ved oppgaven, men begge de to første forholdene er relatert til personlige mål. Det siste forholdet handler ifølge Reason (1997b) om at det er nødvendig å avvike fra prosedyren for å få jobben gjort, så dette punktet er relatert til en gitt arbeidssituasjon. Resultatene fra kapittel 5.2 viste et stort arbeidspress i IKT-virksomheten, noe som dermed kunne resultere i det Rasmussen (1997); Snook (2000) kalte *"practical drift*" som vil si at man gradvis sklir vekk fra etablerte prosedyrer. Noen ganger kan det være riktig å avvike fra rutiner og improvisere slik plattformsjefen besluttet i forbindelse med Snorre A jf (Schiefloe og Vikland, 2007), spesielt i situasjoner der prosedyrer er mangelfulle eller det ikke er tatt høyde for en gitt hendelse. I tilfellet med Snorre A var lokal kunnskap og erfaring viktig for å forstå hva man kunne gjøre og hvor grensene gikk for sikker operasjon.

Avvik fra etablerte rutiner og gjeldende praksis kan også introdusere feilsituasjoner. Informantene snakket om stort tidspress og menneskelige feil i forbindelse med sikkerhetsarbeidet. Ettersom installasjon og vedlikehold ifølge Reason (1997b) i flere empiriske studier er funnet som den viktigste årsaken til organisatoriske ulykker, er det neppe gode grunner for å tro at sikkerhetsarbeid på kritiske IKT-systemer under stort tidspress skulle være mer skjermet mot tilsvarende fenomener. I sikkerhetskritiske organisasjoner er regler og prosedyrer ifølge Reiman og Oedewald (2009) ofte ansett for å gjøre menneskelige aktiviteter og virksomheter mer pålitelige. I stille perioder som ferie kunne det forekomme at personell avvek fra etablerte rutiner på operasjonssenteret, uten at det medførte feilsituasjoner eller hendelser.

Flere informanter påpekte at det var vanskelig å regulere atferd og vaner hos brukeren. Hos en virksomhet var det praksis å kjøre kampanjer et par ganger året rettet mot alle ansatte, og hensikten var dels å skape bevissthet og dels påvirke brukeratferd. Albrechtsen (2008) fant at brukerinvolvering i grupper var det mest effektive virkemiddelet for å påvirke atferd. Som nevnt

i kapittel 6.1 er IKT-sikkerhetsarbeidet regulert gjennom formell dokumentasjon, herunder brukerinstrukser. Hverken brukere eller sikkerhetsledere trodde ifølge Albrechtsen (2008) at policyer, prosedyrer og instrukser med krav til brukeratferd hadde særlig innflytelse på brukerens utøvelse, dels på grunn av: tilgjengelighetsutfordringer; vanskeligheter med å forstå innholdet; mangel på tid; incentiver til å studere dokumentasjonen. Det var imidlertid en sammenheng mellom atferd og uformelle normer, og brukernes kompetanse og erfaring. I forbindelse utvikling av HMS-systemer var det ifølge Hovden (1998) toppledelsens involvering og deltakelse fra ansatte som førte til bedre formelle systemer, enn systemer etablert uten deltakelse fra virksomhetens ansatte. Informanter i denne casestudien oppnådde som nevnt i kapittel 5.2.7 god læreeffekt av å gjennomføre risikoanalyser i grupper, og sammenholdt med Albrechtsen (2008) og Hovden (1998) funn indikerer det at aktiv medvirkning fra brukere og lederinvolvering kan være nyttig ved innføring av ny teknologi og utforming av brukerprosedyrer.

Brukernes adferd pekte i retning av preferanser for ny og moderne teknologi, mens sikkerhetsløsningene i mange tilfeller ble sett på som foreldet som følge av langvarig utviklings- og godkjenningsprosess. Det var særlig to forhold som ble trukket frem som utfordringer i casestudien: Brukeren var i privat sammenheng vant til å anvende moderne systemer og dele informasjon, mens i jobbsammenheng måtte brukeren forholde seg til tungvinte og *"gammeldagse"* sikkerhetssystemer; I samband med prosjekt- eller teamarbeid med eksempelvis mange eksterne parter, kunne teamene finne på å ta i bruk skytjenester for å få løst sine arbeidsoppgaver. Det innebar dermed at teamene gikk utenfor de etablerte barrierene, og virksomheten hadde da ikke like god kontroll på håndtering og forvaltning av informasjonen. Resultatene indikerte dermed at brukere hadde preferanser til systemer som: var enkle å bruke; gjenkjennbare; hjalp brukeren med å løse oppgavene. Utfordringer er derfor knyttet til utforming av funksjonelle systemer med hensiktsmessige brukergrensesnitt.

Virksomhetene brukte mye ressurser til å bygge opp kompetanse på sine medarbeidere, men ble tidvis tappet for kompetanse gjennom turnover. Sikkerhetsmarkedet var ifølge informantene preget av konkurranse om arbeidskraften, i tillegg til at det ikke alltid var enkelt å finne personell med de ønskede kvalifikasjonene. Periodevis var derfor enkelte virksomheter tynnere bemannet enn ønskelig. Det kan være utfordrende å håndtere de endringene som følger av personellutskiftinger, og da gjelder det ikke bare hvorvidt det er mulig å få tak i ønsket arbeidskraft eller ikke. Ifølge Reiman og Oedewald (2009) handler det om forhold som at nye

ledere eller tekniske spesialister ikke kjenner: virksomhetens historie; etablerte praksiser; hvilke utfordringer virksomheten har møtt; hvordan utfordringer er løst; hvilke sårbarheter som fortsatt eksisterer. Videre må nytt personell slik som Reiman og Oedewald (2009) beskriver det: forholde seg til komprimert og forutinntatt informasjon fra kolleger og offisielle dokumenter; det er fare for at de ikke forstår rasjonale for tidligere beslutninger og praksiser, og dermed forsøkte å endre disse; på den annen side kan nykommere bringe med seg nye ideer og utfordre etablerte sannheter. Turnover kan altså ha flere effekter. Ved turnover kan altså virksomheten miste nøkkelpersonell, og som nevnt i kapittel 6.1 var erfaring og kjennskap til lokale forhold blant annet en viktig faktor ved utforming av sikkerhetsdokumentasjon for komplekse systemer. Kompetanseoppbygging av nytt personell var ifølge informanter både tids- og ressurskrevende prosesser, noe som dermed skapte organisatoriske sårbarheter i en overgangsfase. Og som vi så tidligere i dette kapitlet var utfordringer med spesialisert kompetanseoppbygging også betinget av tilgjengelighet til kurs- og utdanningsprogrammer.

6.5.1 Sammendrag kompetanse, verdier og holdninger

Enkelte virksomheter var godt i gang med å styrke bemanningen og kompetansenivået, men fortsatt manglet eller hadde virksomheter for lav kompetanse på enkelte områder, herunder ikke-dublert kompetanse. Virksomhetene hadde således ikke god organisatorisk redundans, noe som ville kunne styrke sikkerhetsnivået. Det siste er betinget av: nødvendig teknisk kompetanse; ledelsens engasjement; motivasjon; tilstrekkelig antall ressurser med rett kvalitet; status i virksomheten.

Manglende forståelse hos ledelsen for kompetansebehovet resulterte da i at man ikke fikk tilsatt nødvendig personell med ønsket kompetanse. Mulige forklaringer på manglende forståelse kan ha sammenheng med svakheter og mangler i kommunikasjons- og informasjonsflyten samt behov for å bedre styringsinformasjon som diskutert i kapittel 6.4. Andre mulige årsaker er: ulike referanserammer; meningsdanning; hendelser; tolkning; avstanden mellom butt og skarp ende av organisasjonen; nye ledere; omorganiseringer; budsjett.

Kurs- og utdanningstilbud var enten ikke tilgjengelige eller dekket behovet, noe som dermed resulterte i organisatorisk sårbarhet. Virksomhetene forsøkte å bøte på dette gjennom kunnskapsoverføring fra erfarne til mindre erfarne medarbeidere så langt tiden strakk til, men tid var også mangelvare.

Faktorer som virket begrensende på mulighetene for kompetanseheving innen ny teknologi eller til å kunne opprettholde det spesialiserte kompetansenivået var: behovsavklaringer; høyt arbeidspress; nye krav; budsjett; tidsfrister; økt kompleksitet ved integrasjon med gammel teknologi; fravær av driftspersonell i prosjekter. Høyt arbeidspress utfordret grensene for sikker operasjon, og ved innføring av ny teknologi måtte virksomhetene samtidig opprettholde kompetanse på gammel teknologi

Ved innføring av ny teknologi, nye sikkerhets- og effektiviseringskrav, endret jobbinnhold og arbeidspraksiser for eksempelvis vedlikeholds personell, kan ifølge Reiman og Oedewald (2009) bety at noen gamle vaner og begreper må avlæres. For eksempel kunne det være relevant i forbindelse med endret bruksmønster på IKT-systemet

Sikkerhetsarbeidet og hendelseshåndtering kunne svikte på grunn av menneskelige feil; feiltolkning; manglende forståelse for at det hadde oppstått en feil eller sikkerhetsrelatert hendelse, noe som også understøttes godt av Turner (1978), og kunne skyldes: 1) feil antakelser; 2) vanskeligheter med å håndtere informasjon i komplekse situasjoner; 3) motstand mot å frykte det verste; 4) normalisering av brudd på formelle regler og reguleringer. Utløsing av hendelser er ifølge Turner (1978) uforutsigbart; innebærer vanligvis nye fortolkninger; avdekker motstridende hendelser fra inkubasjonsperioden; kan resultere i mange følgeskader. Motstridende hendelser kunne dermed lede til at saken ikke ble innrapportert.

Årsakene til brudd på sikkerhetsbestemmelser og avvik fra etablerte rutiner i utøvelsen av sikkerhetsarbeidet og hendelseshåndteringen kunne være enten personlige mål eller funksjonelle sider ved oppgaven som informantene karakteriserte som: tidspress; latskap; menneskelige feil; saken ikke viktig nok; mangelfulle rutiner; hendelser var ikke omfattet av rutinebeskrivelsene. Stort arbeidspress var en mulig forklaring på gradvis frikobling fra rutinene som ellers var ment å bidra til styrket pålitelighet, men arbeidspresset kunne ikke forklare at personell fravek rutinene i stille perioder.

Brukeratferd representerte spesielt to utfordringer ved innføring av ny teknologi. For det første praktiserte en virksomhet atferd- og bevissthetskampanjer mot ansatte, noe som er mindre effektivt enn brukerinvolvering i grupper som bør brukes ved innføring av ny teknologi og utforming av brukerprosedyrer. For det andre representerte bruk av privat moderne utstyr utfordringer for å regulere atferd og bruk av mindre moderne sikkerhetsutstyr i arbeidssituasjonen.

Virksomhetene brukte mye ressurser til å bygge opp kompetanse på sine medarbeidere, men ble tidvis tappet for kompetanse gjennom turnover og dermed oppsto organisatoriske sårbarheter i en overgangsfase. Utfordringene i overgangsfasen handler ifølge Reiman og Oedewald (2009) om å stifte nytt bekjentskap med: virksomhetens historie; etablerte praksiser; erfarte utfordringer og hvordan de er løst; og eksisterende sårbarheter, noe som er tidkrevende.

7 Konklusjon

Denne studien undersøkte IKT-sikkerhetsutfordringene hos tre virksomheter på bakgrunn av forskningsspørsmålet:

Hvorfor er det utfordrende for virksomheter å beskytte samfunnets kritiske IKT-infrastruktur, og å opprettholde et IKT-systems sikre tilstand i henhold til sikkerhetsloven?

Studien ble gjennomført ved hjelp av kvalitative semi-strukturelle intervjuer med i alt 13 informanter.

Pentagonanalysen og drøftingen i kapittel 6 viste for det første at utfordringene omhandlet mer enn bare formelle kvaliteter som formell struktur og teknologi ettersom mange funn omfattet de uformelle kvalitetene kompetanse, verdier og holdninger; interaksjon; sosiale relasjoner og nettverk. For det andre viste analysen at det er avhengigheter mellom formelle og uformelle kvaliteter. Funnene kan derfor ikke betraktes som isolerte fenomener, men må forstås i sammenheng med hverandre. Et tredje moment er at virksomhetene også møtte utfordringer knyttet til eksterne faktorer som politisk nivå, NPM og leverandører.

Ut i fra diskusjonen i kapittel 6 fremgår at mesteparten av kritisk IKT-infrastruktur ble regulert gjennom enten preskriptive regler som FoI eller funksjonelle regler som FoO, mens resten av infrastrukturen ikke var omfattet av SL. Uklarheter ved fortolkningen av FoO medførte at ikke alle relevante IKT-systemer ble beskyttet i henhold til bestemmelsene. Det var risiko for at virksomheter fravek krav som ble oppfattet som ikke-legitime. Uklare eller ikke-legitime regler kan derfor resultere i utfordringer med å sikre IKT-infrastrukturen i et organisatorisk- og samfunnsmessig perspektiv. FoI både fremmet og hemmet virksomhetenes sikkerhetsarbeid ettersom kravene bidro til prioritering av sikkerhetstiltak, mens praksis viste at tilfredsstillelse av kravene i mange tilfeller bød på utfordringer. Som et svar på det siste lempet myndigheten ganske ofte på kravene ved å utstede midlertidige brukstillatelser. Hovedårsaken til utfordringene med å fylle kravene var målkonflikter som hadde bakgrunn i stramme budsjetter, tjenesteleveranser og undervurderte anskaffelseskostnader. Virksomhetene fikk dermed ikke løst alle behov.

Mangel på tekniske veiledninger gjorde virksomhetene usikre på hvordan ny teknologi skulle integreres i bestående systemer, noe som i mange tilfeller førte til at virksomhetene tok i bruk proprietære løsninger for å ivareta tjenesteleveransene. Det siste forholdet gjorde allerede

komplekse systemer bestående av både gamle og nye løsninger, enda mer komplekse og påførte virksomheten mer manuelt arbeid. Mangel på hensiktsmessige verktøy påførte IKT-personellet flere manuelle operasjoner og ytterligere arbeidspress. Kompleksiteten, tette koblinger, latente feil og gjensidig avhengighet i systemene og utfordringer med å forutsi risiko gjorde virksomhetene bekymret ved eksempelvis sikkerhetsoppdateringer. Samfunnskritiske funksjoner og tjenester hadde stanset som følge av enkeltstående feil, oppgraderinger. Hovedårsaken til utfordringene skyldtes målkonflikter, manglende kompetanse og mangelfull kommunikasjon som dermed eroderte sikkerhetsmarginene og medførte risikoatferd.

En gjennomgående utfordring for virksomhetene var avveininger om ressursinnsats mellom IKT-sikkerhet og tjenesteleveranser. I mange tilfeller var det heller ikke et spørsmål om IKT-sikkerhetsorganisasjonens avveininger ettersom leveranseplanen enten var politisk bestemt; eller sikkerhet var siste sjekkpunkt, noe som ofte førte til at IKT-sikkerhet da måtte løses på et senere tidspunkt. Medvirkende årsaker til målkonflikten kunne være at sikkerhet ble tatt for gitt; lederne ble målt på tjenesteleveranser; NPM-krav ledet til ad-hoc pregete arbeidsprosesser. Manglende lederforankring eller manglende forståelse for sikkerhetsarbeid var andre faktorer som spilte inn.

De fleste informantene så behov for å tette kompetansegapet, men slik som behovsavklaringer; høyt arbeidspress; nye krav til tjenesteleveranser; budsjettbegrensninger; tidsfrister; økt kompleksitet ved integrasjon med gammel teknologi; fravær av driftspersonell hemmet og kompliserte realiseringen. Kompetansegapet resulterte dermed i svekket organisatorisk redundans.

Målkonfliktene kan forklares som et resultat av at virksomhetene var preget av kommunikasjonsproblemer; koordineringssvikt; manglende samhandling; manglende lederforståelse, herunder også på politisk nivå; utilstrekkelige kunnskaper om komplekse forhold. Sosiale relasjoner og nettverk var preget av ressurskonflikter og fragmentering. Sikkerhetsarbeidet ble i stor grad drevet nedenfra via formell kommunikasjon. De underliggende faktorene som er nevnt i dette avsnittet bidrar sammen med politikk, budsjettbegrensninger, tjenesteleveranser og NPM til å forklare at målkonflikter oppstod.

Det var imidlertid tre forhold som bidro til et reaktivt lederfokus på sikkerhet: negative hendelser; alvorlige tilsynsrapporter; alvorlige risikoanalyser. I et organisatorisk- og

samfunnsmessig perspektiv viser funnene og drøftingen fra denne studien behov for å videreutvikle det proaktive sikkerhetsarbeidet som da bør forankres helt på toppnivå.

7.1 Anbefalinger

Risikoatferden som følge av at virksomhetene fravek eller ikke tilfredsstilte kravene og myndighetens normalisering av avvik som omtalt av Rosness et al. (2010); Vaughan (1996) bør endres slik at det bidrar til mer robuste systemer hos virksomhetene, og KI-sektoren bør vurderes under ett. En mulig tilnærming kan være å lempe på ikke-legitime krav eller å gå over til mer funksjonelle krav. Forhold som taler imot er kompleks teknologi og et raskt skiftende trusselbilde. Strengere håndheving av bestemmelsene er en annen mulig tilnærming som også informanter var inne på. Utforming av teknologiveiledninger bør imidlertid styrkes for å møte etterspørselen og dermed bidra til mer robuste tekniske barrierer. Ikke alle utfordringer identifisert i denne casestudien kan løses på en gang, og derfor bør det fokuseres på det viktigste først som omhandler målkonfliktene.

Fire lærdommer kan trekkes frem for å løse målkonfliktene i favør av styrket sikkerhet: Etablere en mer proaktiv tilbakekoblingssløyfe til høyere beslutningsnivåer; å synliggjøre grensene bedre for uakseptabel risiko; å redusere arbeidsbelastningen for IKT-personell; å yte press som kan favorisere sikre handlinger.

Det første kan styrkes gjennom en kombinasjon av bedre kommunikasjon også i lys av at koordinering gjennom standardisering synes ikke å fremstå som et tilstrekkelig verktøy alene; kompetanseheving gjennom involvering og uformell kommunikasjon; kartlegging av kapasitetsbehovet; mer realistisk budsjettering; politiske beslutninger om komplekse tjenester/sammenkoblinger bør planlegges gjennom involvering av miljøer med førstehåndkjennskap til utfordringene.

Det andre punktet henger i stor grad sammen med foregående punkt og gjelder egentlig hvordan førstehåndskjennskap til trusler i den spisse enden av virksomheten skal omsettes og formidles til den myke enden av virksomheten inkludert politiske nivåer. Tre forhold som kan vurderes ut fra casestudien funn i lys av komplekse systemer, sårbarheter i systemer og flere manuelle operasjoner er redusert kompleksitet i systemene, fjerne de mest sårbare systemene som trolig ikke er en god løsning i NPM-sammenheng samt å innføre bruk av egnede driftsstøtteverktøy. Bruk av objektive måleparametere på sikkerhet kan være et mulig virkemiddel for å synliggjøre virksomhetens fokus på sikkerhet.

Det tredje punktet om arbeidsbelastningen vil få bedre grunnlag for normalisering som følge av de to første punktene. I tillegg bør det fokuseres på å holde systemdokumentasjonen intakt, både fordi det er vesentlig for å kunne opprettholde systemenes sikre tilstand og også som grunnlag for å kunne håndtere kritiske situasjoner.

Det fjerde punktet handler om å yte press som favoriserer sikre handlinger dreier seg om å stimulere til sikker atferd. De tre første punktene er viktige bidrag. Virkemidlene spenner fra frivillige tiltak, standarder, selvdeklarasjon, akkreditering, juridiske (fra preskriptive til funksjonelle), økonomiske incentiver, omdømme, legitimitet, politiske. Ut i fra drøftingene i casestudiet var preskriptive krav et godt hjelpemiddel for sikkerhetsorganisasjonene, og Skotnes (2015) fant også at detaljerte retningslinjer var foretrukket fra operativt nivå ved innføring av nye teknologier i komplekse og tett koblede systemer. Problemstillingen er imidlertid kompleks og effekten av de regulatoriske virkemidlene kan være vanskelig å forutsi ifølge Sinclair (1997), men kombinasjoner av virkemidler i spennet mellom kommando og kontroll og selvregulering er oftest anbefalt. Videre er endring av atferd komplisert og tidkrevende. Et forhold som bør nevnes er leverandørenes ansvar for utvikling av robuste produkter og systemer. Et annet forhold er politiske beslutninger. Et tredje moment er kravutforming og bestillerkompetanse. Problemstillingen er omfattende, det er ingen enkle svar og virksomhetene kan trolig ikke løse utfordringene alene. Virksomhetene kan imidlertid starte gjennom å opptre som krevende kunder og styrke den organisatoriske robustheten gjennom å minimere kjent risikoatferd.

7.2 Videre arbeid

Det er fire områder som peker seg ut for videre forskning innen IKT-sikkerhet og kritiske infrastrukturer basert på funnene i denne casestudien.

Det første området handler om at resultatene fra denne casestudien kunne kombineres med en kvantitativ undersøkelse i de samme tre virksomhetene A, B og C, noe som ifølge Silverman (2014); Yin (2014) betegnes som data triangulering. Datagrunnlaget som da fremskaffes ved hjelp av ulike metoder kan brukes til gjensidig validering av datasettene.

Det andre området gjelder studiet av gråsonen i KI. For beskyttelse av IKT-systemer som er en del av KI kommer enten SL og FoI og/eller FoO til anvendelse, men samtidig er det deler av KI som ikke er omfattet av reguleringene. Det er i hovedsak to tilfeller som befinner seg i en gråsone: ugraderte systemer under SL som del av KI og er klassifisert som objekter under FoO;

ugraderte systemer under KI som ikke er underlagt SL. Det er to grunner til at det er uklart hvordan IKT-systemene beskyttes: FoO fokuserer hovedsakelig på fysiske forhold og det er opp til objekteier å finne frem til passende sikringstiltak av IKT; IKT-systemer utenfor SL er uregulert, og det er dermed uklart hvilke prinsipper som er lagt til grunn for sikring av systemene. Det bør derfor forskes på om det er sårbarheter knyttet til gråsonen og i tilfelle hvilke sårbarheter som eksisterer.

Det tredje området kan beskrives slik: En refleksjon er at det synes å ha vært lite fokus på organisatoriske- og samfunnsmessige kostnader som følge av latente betingelser i IKT. Spørsmålet er om det er bedre for virksomhetene og samfunnet å forlange at industrien må tilfredsstille sikkerhets- og kvalitetskrav til IKT-produkter- og komponenter som brukes innen KI (kanskje også andre sektorer), eller om det er bedre at industrien fastsetter kravene og at kunden tar det som blir levert. Problemstillingen henger sammen med dagens praksis innenfor IKT-industrien hvor feilretting og patching er ganske utbredt etter gjennomførte leveranser. Sagt på en annen måte handler det om forholdet mellom tiltak for å designe bedre og sikrere produkter (barrierer) og komponenter, eller bruk av produkter og komponenter som innehar svakheter og som dermed er en dårligere barriere. Vi har gjennom en årrekke vært vitne til at virksomhetene bygger ut det organisatoriske apparatet som et motsvar til svake barrierer i IKT-systemene. Det kan forstås som at virksomhetene bærer kostnadene for produkter med feil og mangler. Eller sagt på en annen måte at skattebetalerne bærer byrdene med sikkerhet i KI-sektoren fremskaffet fra private firmaer, selv om firmaene som Egan (2007) påpeker har gjort valg som reduserer systemisk pålitelighet. Det synes å være en trend at denne utviklingen har funnet sted uten at det er gjort forskning på hvilke organisatoriske- og samfunnsmessige kostnader (konsekvenser) en slik praksis har. Med utgangspunkt i figur 4 om organisatoriske egenskaper for sikker drift, er kost-/nyttevurdering av proaktive- reaktive tiltak og robusthet i systemene et område som bør undersøkes nærmere. Det vil også kunne gi bedre forståelse av hvorvidt sterkere reguleringer av sikkerhet er et virkemiddel som bør vektlegges mer eller ikke for å oppnå ønsket robusthet i KI-sektoren.

Det siste punktet som kan være av interesse er en studie som ser på styrker og svakheter (evt kost-/nytte) ved mulige løsninger på de utfordringer og funn som er gjort i denne casestudien.

8 Vedlegg A Intervjuguide

"Hvorfor er det utfordrende for virksomheter å beskytte samfunnets kritiske IKT-infrastruktur og å opprettholde et IKT-systems sikre tilstand i henhold til sikkerhetsloven?"

1. a) Hvordan oppfatter du IKT-sikkerhetskravene dere som organisasjon må etterleve?
1. b) Hvordan har de formelle bestemmelsene etter din vurdering virket med hensyn til å sette virksomheten i stand til å drive et godt sikkerhetsarbeid?
2. Hvorfor kan eventuelt arbeidet med vedlikehold av tekniske barrierer være utfordrende?
3. Hvorfor kan introduksjon av ny teknologi by på utfordringer?
4. Beskriv kort din oppfatning av ledelsens forståelse og forankring for å drive IKT-sikkerhetsarbeid i virksomheten, og hvorfor tror du situasjonen er slik som beskrevet?
5. Hvordan virker kravene og tiltakene i forhold til NSMs intensjoner om å beskytte samfunnets kritiske IKT-infrastruktur?
6. Hvorfor er det eventuelle utfordringer mellom IKT-investeringer og tilgjengelige ressurser?
7. Beskriv kort status for NSMs fire anbefalte tiltak[43], og hvorfor er nåsituasjonen slik som beskrevet?
8. Beskriv kort status for det kompetansebehovet som ansees nødvendig for å kunne utføre sikkerhetsarbeidet i virksomheten, og hvorfor er nåsituasjonen slik som beskrevet?
9. a) Kan du si noe om bruken av risikoanalyse i virksomheten, dokumentasjon av resultatene og hvorfor det gjennomføres risikoanalyse?
9. b) Hvilken effekt har risikoanalysen på de virksomhetsansvarliges risikoforståelse?
9. c) Hvordan vil du beskrive de ansvarliges kunnskap om/forståelse av kompleksiteten i IKT-systemene?
10. Hvorfor kan sammenkobling av informasjonssystemer med forskjellige graderingsnivåer eller mellom ulike organisasjoner by på utfordringer?
11. Hvorfor kan regulering av IKT-sikkerhet gjennom sikkerhetsloven med tilhørende forskrifter og veiledninger resultere i utilsiktede virkninger i organisasjonen?

[43] Oppgrader maskin- og programvare; Installasjon av sikkerhetsoppdateringer; Ikke tildel sluttbrukere administrator rettigheter; Blokker kjøring av ikke-autoriserte programmer.

12. Beskriv kort hvordan utviklingsprosjektene som skal lede frem til sikkerhetsgodkjente informasjonssystemer er organisert i dag, og hvorfor er dagens praksis **e**gnet / ikke egnet?
13. Beskriv kort hvordan informasjonsflyten og koordineringen av IKT-sikkerhetsrelaterte oppgaver utøves i dag, og hvorfor kan dagens praksis ha betydning for sikkerhetstilstanden i virksomheten?
14. Hvorfor kan det inntreffe svikt i IKT-sikkerhetsarbeidet og håndtering av IKT-sikkerhetshendelser?
15. Hvordan vil du karakterisere det arbeidet NSM gjør gjennom tilsynsvirksomheten?
16. Er det til slutt noe du ønsker å legge til som jeg ikke har spurt om?

9 Referanser

Albrechtsen, E. (2008). *Friend or foe? : information security management of employees*. (2008:101), Norwegian University of Science and Technology, Faculty of Social Sciences and Technology Management, Department of Industrial Economy and Technology Management, Trondheim.

Albrechtsen, E. (2015). Major accident prevention and management of information systems security in technology-based work processes. *Journal of Loss Prevention in the Process Industries, 36*, 84-91. doi:http://dx.doi.org/10.1016/j.jlp.2015.05.004

Albrechtsen, E., & Hovden, J. (2007). Industrial safety management and information security management: risk characteristics and management approaches. In T. Aven & J. E. Vinnem (Eds.), *Risk, Reliability and Social Safety: Proceedings of the European Safety and Reliability Conference 2007 (Esrel 2007)* (pp. 2333-2340). London, UK: Taylor & Francis.

Almklov, P. G., & Antonsen, S. (2010). The Commoditization of Societal Safety. *Journal of Contingencies and Crisis Management, 18*(3), 132-144. doi:10.1111/j.1468-5973.2010.00610.x

Almklov, P. G., Antonsen, S., & Fenstad, J. (2010). *IKT, nye grensesnitt og nye sårbarheter? : hvordan nye teknologier og organisasjonsformer påvirker robusthet og beredskapsevne for IKT-hendelser ved sykehus*. Trondheim: Studio Apertura, NTNU Samfunnsforskning AS.

Almklov, P. G., Antonsen, S., & Fenstad, J. (2011). *NPM, kritiske infrastrukturer og samfunnssikkerhet : sluttrapport i SAMRISK-prosjektet 'Critical infrastructures, public sector reorganization and societal safety'* (2. utg. ed.). Trondheim: Studio Apertura, NTNU Samfunnsforskning AS

Amundsen, O., & Kongsvik, T. Ø. (2008). *Endringskynisme*. Oslo: Gyldendal akademisk.

Argyris, C., & Schön, D. A. (1996). *Organizational learning II : theory, method, and practice*. Reading, Mass: Addison-Wesley.

Brattbakk, M., Østvold, L.-Ø., van der Zwaag, C., & Hallvard, H. (2004). *Granskning av gassutblåsning på Snorre A, brønn 34/7-P31 A 28.11.2004*: Petroleumstilsynet.

Clegg, S., Kornberger, M., & Pitsis, T. (2011). *Managing & organizations : an introduction to theory & practice* (3rd ed. ed.). Los Angeles, Calif: SAGE.

Cleland, D. I. (1986). Project Stakeholder Management. *Project Management Journal (September), 17*, 36-44.

Cleland, D. I. (2008). Project Stakeholder Management. In D. I. Cleland & W. R. King (Eds.), *Project Management Handbook* (Second Edition ed., pp. 275-301): John Wiley & Sons, Inc.

Corbin, J. M., & Strauss, A. L. (2008). *Basics of qualitative research : techniques and procedures for developing grounded theory* (3rd ed. ed.). Thousand Oaks, Calif: Sage.

Corbin, J. M., & Strauss, A. L. (2015). *Basics of qualitative research : techniques and procedures for developing grounded theory* (4th ed. ed.). Thousand Oaks, Calif: Sage.

de Bruijne, M., & van Eeten, M. (2007). Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies & Crisis Management, 15*(1), 18-29. doi:10.1111/j.1468-5973.2007.00501.x

DSB. (2012). *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner - modell for overordnet styring*. (ISBN 978-82-7768-256-3). Direktoratet for samfunnsikkerhet og beredskap Hentet fra https://www.dsb.no/rapporter-og-evalueringer/sikkerhet-i-kritisk-infrastruktur---delrapport-1/.

Egan, M. J. (2007). Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems. *Journal of Contingencies and Crisis Management, 15*(1), 4-17. doi:10.1111/j.1468-5973.2007.00500.x

FFI-rapport 2007/01204. (2007). *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer – sluttrapport*. (ISBN 978-82-464-1222-1). Forsvarets forskningsinstitutt Hentet fra http://www.ffi.no/no/Rapporter/07-01204.pdf.

Forskrift om informasjonssikkerhet. (2001). *Forskrift om informasjonssikkerhet. Forskrift 1. juli 2001 nr. 744 om Forskrift om informasjonssikkerhet.* Hentet fra https://lovdata.no/dokument/SF/forskrift/2001-07-01-744.

Forskrift om objektsikkerhet. (2011). *Forskrift om objektsikkerhet. Forskrift 1. januar 2011 nr. 1362 om Forskrift om objektsikkerhet.* Hentet fra https://lovdata.no/dokument/SF/forskrift/2010-10-22-1362.

Forskrift om personellsikkerhet. (2001). *Forskrift om personellsikkerhet. Forskrift 1. juli 2001 nr. 722 om Forskrift om personellsikkerhet.* Hentet fra https://lovdata.no/dokument/SF/forskrift/2001-06-29-722.

Forskrift om sikkerhetsadministrasjon. (2001). *Forskrift om sikkerhetsadministrasjon. Forskrift 1. juli 2001 nr. 723 om Forskrift om sikkerhetsadministrasjon.* Hentet fra https://lovdata.no/dokument/SF/forskrift/2001-06-29-723.

Forskrift om sikkerhetsgraderte anskaffelser. (2001). *Forskrift om sikkerhetsgraderte anskaffelser. Forskrift 1. juli 2001 nr. 753 om Forskrift om sikkerhetsgraderte anskaffelser.* Hentet fra https://lovdata.no/dokument/SF/forskrift/2001-07-01-753.

Groth, L. (2005). *Lederen, organisasjonen og informasjonsteknologien : det du må vite for ikke å bli overkjørt av IT-folk*. Bergen: Fagbokforl.

Haddon Jr, W. (1970). On the escape of tigers: an ecologic note. *American Journal of Public Health and the Nations Health, 60*(12), 2229-2234.

Haddon, W. (1980). The basic strategies for reducing damage from hazards of all kinds. *Hazard prevention, 16*(1), 8-12.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397. doi:10.1108/09685220810908796

Hansen, M. T. (2009). *Collaboration : how leaders avoid the traps, create unity, and reap big results*. Boston, Mass: Harvard Business Press.

Herriott, R. E., & Firestone, W. A. (1983). Multisite Qualitative Policy Research: Optimizing Description and Generalizability. *Educational Researcher, 12*(2), 14-19. doi:10.2307/1175416

Hollnagel, E., Tveiten, C. K., & Albrechtsen, E. (2010). *Resilience Engineering and Integrated Operations in the Petroleum Industry* (ISBN 9788214049015). Hentet fra http://www.sintef.no/publikasjon/?pubid=SINTEF+A16331

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering : concepts and precepts*. Aldershot: Ashgate.

Hovden, J. (1998). The ambiguity of contents and results in the Norwegian internal control of safety, health and environment reform. *Reliability Engineering & System Safety, 60*(2), 133-141. doi:http://dx.doi.org/10.1016/S0951-8320(98)83006-8

Jacobsen, D. I., & Thorsvik, J. (2007). *Hvordan organisasjoner fungerer* (3. utg. ed.). Bergen: Fagbokforl.

Jergeas, G. F., Williamson, E., Skulmoski, G. J., & Thomas, G. L. (2000). Stakeholder Management on construction projects. *AACE International Transaction*, P12.11-P12.16.

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2010). *Introduksjon til samfunnsvitenskapelig metode* (4. utg. ed.). Oslo: Abstrakt.

Karlsen, J. T. (2002). Project Stakeholder Management. *Engineering Management Journal, 14*(4), 19-24. doi:10.1080/10429247.2002.11415180

Kruke, B. I. (2012, 13.03.2012). *Samfunnssikkerhet og krisehåndtering: Relevans for 22. juli 2011*. (Notat: 7/12).

Kvale, S. (2007). *Doing Interviews*. London, England: SAGE Publications, Ltd.

Kvale, S., Anderssen, T., & Rygge, J. (1997). *Det kvalitative forskningsintervju*. Oslo: Ad notam Gyldendal.

Kvale, S., Brinkmann, S., Anderssen, T. M., & Rygge, J. (2009). *Det kvalitative forskningsintervju* (2. utg. ed.). Oslo: Gyldendal akademisk.

Kvale, S., Brinkmann, S., Anderssen, T. M., & Rygge, J. (2015). *Det kvalitative forskningsintervju* (3. utg., 2. oppl. ed.). Oslo: Gyldendal akademisk.

LaPorte, T. R., & Consolini, P. M. (1991). Working in Practice but Not in Theory: Theoretical Challenges of "High-Reliability Organizations". *Journal of Public Administration Research and Theory: J-PART, 1*(1), 19-48.

Lindøe, P. H., & Engen, O. A. (2013). "Offshore Safety Regimes - A Contested Terrain". *Center for Oceans Law and Policy : The Regulation of Continental Shelf Development : Rethinking International Standards (1)*, 195-212.

Line, M. B., & Albrechtsen, E. (2016). Examining the suitability of industrial safety management approaches for information security incident management. *Information and Computer Security, 24*(1), 20-37. doi:doi:10.1108/ICS-01-2015-0003

Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. *ACM Comput. Surv., 26*(1), 87-119. doi:10.1145/174666.174668

Meyer, C. B., & Stensaker, I. G. (2011). *Endringskapasitet*. Bergen: Fagbokforl.

Mintzberg, H. (1983). *Structure in fives : designing effective organizations*. Englewood Cliffs, N.J: Prentice-Hall.

NOU 2000: 24. (2000). *Et Sårbart samfunn : utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet : innstilling fra utvalg oppnevnt ved kongelig resolusjo n 3. september 1999 : avgitt til Justis- og politidepartementet 4. juli 2000*. (ISBN 8258305379). Oslo: Justis- og politidepartementet Hentet fra https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf.

NOU 2006:6. (2006). *Når sikkerheten er viktigst : beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner : innstilling fra utvalg oppnevnt ved kongelig resolusjon 29. oktober 2004 : avgitt til Justis- og politidepartementet 5. april 2006*. (ISBN 8258308742). Oslo: Justis- og politidepartementet Hentet fra https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf.

NOU 2015: 13. (2015). *Digital sårbarhet - sikkert samfunn: Beskytte enkeltmennesker og samfunn i en digitalisert verden: innstilling fra utvalg oppnevnt ved kongelig resolusjo n 20. juni 2014 : avgitt til Justis- og beredskapsdepartementet 30. november 2015*. (ISBN 978-82-583-1249-6). Oslo: Justis- og beredskapsdepartementet Hentet fra https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf.

Olsen, O. E., & Lindøe, P. H. (2009). Risk on the ramble: The international transfer of risk and vulnerability. *Safety Science, 47*(6), 743-755. doi:http://dx.doi.org/10.1016/j.ssci.2008.01.012

Perrow, C. (1984). *Normal accidents : living with high-risk technologies*. New York: Basic Books.

Perrow, C. (2011). *Normal Accidents : Living with High Risk Technologies*. Princeton: Princeton University Press.

Pidgeon, N., & O'Leary, M. (2000). Man-made disasters: why technology and organizations (sometimes) fail. *Safety Science, 34*(1–3), 15-30. doi:http://dx.doi.org/10.1016/S0925-7535(00)00004-7

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science, 27*(2–3), 183-213. doi:http://dx.doi.org/10.1016/S0925-7535(97)00052-0

Reason, J. (1990). *Human error*. Cambridge: Cambridge University Press.

Reason, J. (1997a). *Managing the risks of organizational accidents*. Aldershot: Ashgate.

Reason, J. (1997b). *Managing the Risks of Organizational Accidents*: Routledge.

Reiman, T., & Oedewald, P. (2009). *Evaluating safety-critical organizations–emphasis on the nuclear industry. SSM: Swedish Radiation Safety Authority*. Hentet fra

Rosness, R. (2001). *"Om jeg hamrer eller hamres, like fullt så skal der jamres" : målkonflikter og sikkerhet* (Vol. STF38 A01408). Trondheim: SINTEF, Teknologiledelse, Sikkerhet og pålitelighet.

Rosness, R., Grøtan, T. O., Guttormsen, G., Herrera, I., Steiro, T., Størseth, F., . . . Wærø, I. (2010). *Organisational Accidents and Resilient Organisations: Six Perspectives. Revision 2* (ISSN 1504-9795 ISBN 9788214050561). Hentet fra http://www.sintef.no/publikasjon/Download/?pubid=SINTEF+A17034

Schiefloe, P., Vikland, K. M., Ytredal, E., Torsteinsbø, A., Moldskred, I., Heggen, S., . . . Syversen, J. (2005). Årsaksanalyse etter Snorre A hendelsen 28.11. 2004. *Stavanger: Statoil*.

Schiefloe, P. M. (2011a). En modell for samfunnssikkerhet: Institutt for sosiologi og statsvitenskap, NTNU Samfunnsforskning.

Schiefloe, P. M. (2011b). *Mennesker og samfunn : innføring i sosiologisk forståelse* (2. utg. ed.). Bergen: Fagbokforl.

Schiefloe, P. M. (2013). *Analyzing and developing organizations: The Pentagon approach*. NTNU Samfunnsforskning AS.

Schiefloe, P. M. (2014). Analyzing and developing organizations: The Pentagon approach: Norwegian University of Science and Technology.

Schiefloe, P. M., & Vikland, K. M. (2007). "Når barrierene svikter. Gassutblåsningen på Snorre A, 28.11.04". *Søkelys på arbeidslivet 2/07*, 207-219.

Schiefloe, P. M., & Værnes, R. (2010). Bestillere og utførere: koordinering og samarbeid. *Søkelys på arbeidslivet, 27 E*(04).

Schulman, P. R., & Roe, E. (2007). Designing Infrastructures: Dilemmas of Design and the Reliability of Critical Infrastructures. *Journal of Contingencies & Crisis Management, 15*(1), 42-49. doi:10.1111/j.1468-5973.2007.00503.x

Sikkerhetsloven. (1998). *Sikkerhetsloven. Lov av 20. mars 1998 nr. 10 om Lov om forebyggende sikkerhetstjeneste*. Hentet fra https://lovdata.no/dokument/NL/lov/1998-03-20-10?q=sikkerhetsloven.

Silverman, D. (2006). *Interpreting qualitative data : methods for analyzing talk, text and interaction* (3rd ed. ed.). Los Angeles: SAGE.

Silverman, D. (2014). *Interpreting qualitative data* (5th ed. ed.). Los Angeles: SAGE.

Sinclair, D. (1997). Self-Regulation Versus Command and Control? Beyond False Dichotomies. *Law & Policy, 19*(4), 529-559. doi:10.1111/1467-9930.00037

Siponen, M. T., & Oinas-Kukkonen, H. (2007). "A Review of Information Security Issues and Respective Research Contributions. " The DATA BASE for Advances in Information Systems 38(1):60.

Skotnes, R. Ø. (2015). Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector: University of Stavanger, Norway.

Skotnes, R. Ø., & Engen, O. A. (2015). Attitudes toward risk regulation – Prescriptive or functional regulation? *Safety Science, 77*, 10-18. doi:http://dx.doi.org/10.1016/j.ssci.2015.03.008

Snook, S. A. (2000). *Friendly Fire: The Accidental Shootdown og U.S. Black Hawks over Northern Iraq*. Princeton, N.J.: Princeton University Press

SOU 2015:23. (2015). *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten*. (ISBN 978-91-38-24256-8). Stockholm: Justitiedepartementet Hentet fra http://www.sou.gov.se/wp-content/uploads/2015/03/SOU-2015_23_webb.pdf.

St. meld. 10 (2016-2017). (2016). Risiko i et trygt samfunn - Samfunnssikkerhet.

Thagaard, T. (2009). *Systematikk og innlevelse : en innføring i kvalitativ metode* (3. utg. ed.). Bergen: Fagbokforl.

Thagaard, T. (2013). *Systematikk og innlevelse : en innføring i kvalitativ metode* (4. utg. ed.). Bergen: Fagbokforl.

Turner, B. A. (1978). *Man-made disasters* (Vol. 53). London: Wykeham.

Turner, B. A., & Pidgeon, N. F. (1997). *Man-made disasters* (2nd ed.). London: Butterworth-Heinemann.

Vaughan, D. (1996). *The Challenger launch decision : risky technology, culture, and deviance at NASA*. Chicago: University of Chicago Press.

Weick, K. E. (1987). Organizational Culture as a Source of High Reliability. *California Management Review, 29*(2), 112-127.

Weick, K. E. (1995). *Sensemaking in organizations*. Thousand Oaks, Calif: Sage.

Yin, R. K. (2014). *Case study research : design and methods* (5th ed. ed.). Los Angeles, Calif: SAGE.