Institutt for ingeniørvitenskap og sikkerhet

Sikring av virksomheter mot tilsiktede uønskede handlinger

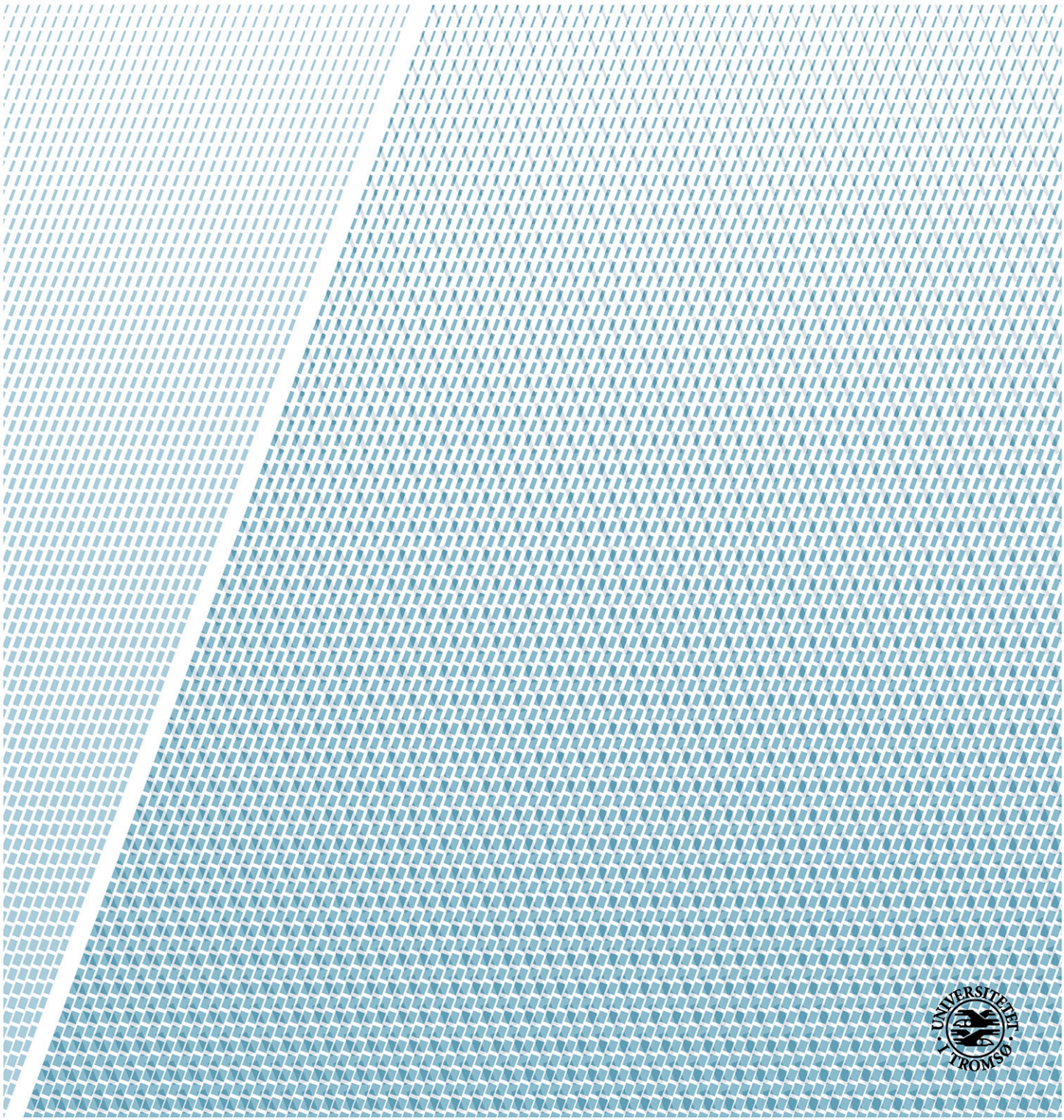
—

Aksel Hødnebø Duus

Masteroppgave i samfunnssikkerhet – Fordypning i sikkerhet og beredskap i nordområdene

Juni 2016

Antall ord*:* 22 669



Forord

Denne masteroppgaven markerer avslutningen på masterstudiet samfunnssikkerhet ved UiT – Norges Arktiske Universitet. Oppgaven er blitt skrevet ved Institutt for ingeniørvitenskap og sikkerhet. Jeg har fått studere et felt jeg er meget interessert i. Dette har ført til at det har vært lærerikt og spennende gjennom hele prosessen.

Jeg ønsker å takke de personene jeg har snakket med i sikkerhetsfagmiljøet. En stor takk til Morten Bremer Mærli for de innspill og råd jeg har fått under oppgaveprosessen, og til informantene som stilte til intervju. Dette har jeg satt virkelig pris på.

Jeg vil spesielt takke min veileder, Maria Hammer, for en veldig god oppfølging. Uten dine råd ville jeg stått fast i oppgaveprosessen langt flere ganger enn det jeg gjorde. Videre vil jeg trekke frem alle de fremragende medelevene jeg har blitt kjent med i løpet av dette studiet. En fantastisk gjeng.

Til sist vil jeg takke mine nærmeste venner og familie.

Dere betyr alt.

Sammendrag

Denne masteroppgaven ser nærmere på sikring av virksomheter mot tilsiktede uønskede handlinger, med mål om å kartlegge hva som kan være årsaker til at virksomheter ikke sikrer seg. Videre søker oppgaven å belyse ufordringer ved utføringen av sikringsrisikoanalyser. Som en følge av at det i de siste årene har blitt utført flere terrorangrep i Europa, har det blitt et større fokus på at virksomheter bør sikre seg mot terror og andre alvorlige kriminelle handlinger. Det å sikre virksomheter mot slike handlinger har utviklet seg til å bli et eget fagområde. Dette har ført til at det har blitt utarbeidet en en tilnærming for å vurdere og analysere risiko knyttet til tilsiktede uønskede handlinger (NS 5832). Det er en rekke utfordringer knyttet til sikring av virksomheter, og oppgavens problemstillingen er derfor som følger: *Hva er mulige årsaker til at virksomheter ikke sikrer seg mot tilsiktede uønskede handlinger?* Det er valgt tre forskningsspørsmål for å belyse problemstillingen. Oppgaven er kvalitativ, og datamaterialet stammer fra to telefonintervjuer, dokumentanalyse og deltakelse på kurs og konferanse. Dette vil sammen med det teoretiske rammeverket være med på å besvare oppgavens problemstilling.

Oppgaven konkluderer med funn og antakelser om mulige årsaker til at virksomheter ikke sikrer seg mot tilsiktede uønskede handlinger. Hovedfunnene i oppgaven er at sikkerhet ofte er dårlig forankret i virksomheters ledelse, og at ledere ikke involverer seg i stor nok grad risikoanalyseprosesser. Dette medfører en begrenset risikoforståelse. Dette er noe som påvirker kvaliteten på de beslutningene som gjelder sikring av virksomhet. Beslutningsprosessen i virksomheter bærer i mange tilfeller preg av at ledelsen mangler beslutningsevne og handlingskraft til å følge opp risikoanalysers sikkerhetsråd. Dette fører til at risikoanalysen ikke operasjonaliseres og at anbefalte sikringstiltak ikke implementeres. Sikkerhetstesting av forebyggende sikringstiltak utføres ikke, noe som fører til at sårbarheter i virksomheter ikke avdekkes. Virksomheter legger seg ofte på et minimums sikringsnivå, og dermed overholdes ikke ALARP-prinsippet. Økonomiske hensyn prioriteres mer eller mindre konsekvent foran sikkerhetsmessige hensyn. Virksomheter er ofte lite villige til å investere i sikkerhet, men sikkerhet er også en mulighet til å bygge omdømme og fremstå som profesjonell aktør i bransjen. Sikkerhet har også blitt en forretningsmulighet.

Innholdsfortegnelse

1. Innledning

Trusselbildet i Norge og Europa har i de senere årene endret seg, og man ser at norske sikkerhetsmyndigheter i langt større grad fokuserer på sikkerhet mot terrorhandlinger. Den 22. juli 2011 ble Norge rammet av bombeangrep mot regjeringskvartalet og massedrap på Utøya. Terrorangrepet resulterte i at 77 mennesker mistet livet. Frankrike har i de siste årene blitt utsatt for flere terrorangrep. Det franske satiremagasinet Charlie Hebdo ble angrepet av to terrorister den 7. januar i 2015. Terroristene tvang seg inn i Hebdos lokaler, og angrepet resulterte i at 12 mennesker ble drept og 11 andre såret. Dette var det mest alvorlige terrorangrepet Frankrike hadde sett på 50 år, men landet skulle kort tid senere bli utsatt for et langt større terrorangrep. Den 13. november i 2015 slo terrorister til på seks forskjellige lokasjoner i Paris. Det var blant annet skyting i konsertlokalet Bataclan under en konsert, samt en selvmordsbombe utenfor en fotballarena. Totalt ble 130 mennesker drept og 351 såret som følge av de seks angrepene (Store Norske Leksikon, 2016). Terrorisme kjennetegnes ved at målrettede aktører har en klar intensjon om å forårsake ødeleggelse og frykt (Arnesen et. al., 2006:16), og terrorisme er definert i Sikkerhetsloven som: ”*ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkningen eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål”* (Lov om forebyggende sikkerhetstjeneste, 1998, §3, pkt.5). I følge Jon Hoffman Fitje, fagdirektør i PST, oppfattes terror som et angrep på samfunnet, og begrepet ”politisk motivert vold” kan også brukes. I dag er det nulltoleranse for at terror kan skje, mens man i større grad kan akseptere ”konvensjonelle” voldshandlinger som ikke er motivert i å skape ødeleggelse og frykt i samfunnet. Til syvende og sist rammer terror den enkelte sivile borger som en hvilken som helst annen alvorlig voldshandling. Det er en illusjon at vi kan sikre oss helt mot terror og samtidig være borgere i et fritt samfunn (Fitje, 2015). Den 5. april 2004 ble Norges Bank i Stavanger utsatt for et nøye planlagt ran. Ransmennene var godt forberedt og hadde stor kapasitet til å gjennomføre ranet. Ranet endte med at 57 millioner kroner ble bortatt, men det mest alvorlig med hendelsen var en politimann ble skutt og drept. Det som kjennetegner alle disse handlingene er at gjerningspersoner med intensjon og kapasitet gjennomfører voldshandlinger mot sivilbefolkningen og skaper frykt i samfunnet.

Et fellestrekk ved alle disse hendelsene er at sikringstiltak ble utfordret. Noen av sikringstiltakene klarte å begrense skadeomfanget eller forsinke angriperne, mens andre sikringstiltak var

manglende eller sviktet. Det manglet kjøretøysperrer i Regjeringskvartalet, og adgangskontrollsystemet i Charlie Hebdos lokaler, hindret ikke terroristene i å komme inn. På fotballarenaen i Paris oppdaget sikkerhetsvakter selvmordsbomberen i en sikkerhetssjekk, noe som førte til at selvmordsbomberen sprengte seg utenfor arenaen. Dette sparte mest sannsynlig mange menneskeliv. Det skuddsikre vinduet i bakgården av NOKAS bygningen var så motstandsdyktig at ranerne brukte langt lengre tid på å komme seg inn i lokalet enn beregnet, noe som også førte til at politiet rakk frem til stedet før ranerne hadde kommet seg avgårde.

1.2 Bakgrunn og problemstilling

Terrorisme, spionasje, sabotasje og kriminalitet kalles ”tilsiktede uønskede handlinger”, heretter kalt TUH. Faguttrykket for å hindre eller motvirke tilsiktede uønskede handlinger er *security* og betyr ”sikkerhet mot uønskede handlinger som et resultat av overlegg og planlegging” (NOU:2006:6). Det har blitt et langt større fokus på security i norske virksomheter og sikkerhetsmyndigheter de siste årene. Som en følge har det blitt publisert en rekke veiledere, håndbøker og retningslinjer som verktøy for å oppnå godt forebyggende sikkerhetsarbeid i virksomheter. Et eksempel er *”Terrorsikring: En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger”* (2015) utarbeidet av Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste. Formålet med veilederen er å gi offentlige og private virksomheter veiledning i forebyggende sikringsarbeid mot TUH (PST,NSM og PDO 2015).

Virksomheter har forskjellige behov for å sikre seg. Man skiller mellom de virksomhetene som er ”skjermingsverdige objekter”, og de som ikke er det. Skjermingsverdige objekter er underlagt Lov om forebyggende sikkerhetstjeneste av 1998 (Sikkerhetsloven), og disse defineres som *«eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale* (Sikkerhetsloven, §3). Loven har spesifikke krav og retningslinjer til det forebyggende sikkerhetsarbeidet mot TUH. Slik forebygging kan for eksempel være at virksomheten skal ha tilfredsstillende fysiske sikringstiltak. Det finnes samtidig en rekke virksomheter som ikke er underlagt sikkerhetsloven, men som har et behov for eller et ønske om å sikres mot TUH. Offentlige og private virksomheter som ikke er underlagt Sikkerhetsloven, er selv ansvarlig for egen sikkerhet og sikkerhet er et lederansvar. Dette medfører utfordringer fordi

det ofte ikke foreligger håndfaste retningslinjer og krav til hvordan sikringsarbeidet skal foregå i motsetning til virksomhetene som er underlagt Sikkerhetloven. Et typisk eksempel på en virksomhet som ikke er underlagt sikkerhetsloven, er en kommersiell virksomhet som ikke har en kritisk betydning for verken samfunnet.

Den overordnede prosessen for forebyggende sikkerhetsarbeid i virksomheter kalles "risikostyring". Risikostyring er i korte trekk en kontinuerlig ledelsesprosess der målsettingen er å identifisere, analysere og vurdere risikoforhold i en virksomhet, samt å finne frem til og iverksette tiltak som kan redusere skadevirkningene (Rausand og Utne, 2009:77). Risikovurderinger og risikoanalyser inngår som sentrale elementer i risikostyringen, og skal legge grunnlaget for de beslutninger og prioriteringer lederne i en virksomhet gjør for å styre risiko (DSB, 2015). Det er likevel knyttet en rekke utfordringer til sikring av virksomheter. For virksomheter som ønsker å sikre seg mot TUH, vil det være ekstra viktig med fysiske sikringstiltak. En av utfordringene med fysiske sikringstiltak er at det er både er tids- og kostnadskrevende å få disse på plass. Konsekvensene av manglende sikkerhet i virksomheter kan i mange tilfeller overstige kostnadene ved enkle sikringstiltak, og riktig utført sikring er økonomisk fornuftig. Sikringstiltakene må også være balanserte, og ikke for inngripende eller overstige verdien de skal beskytte. Dersom en virksomhet er sårbar, øker muligheten for at en tilsiktet uønsket handling vil kunne inntreffe gjennomføres (NSM, 2015). For å få en forståelse for hvilke sårbarheter virksomheten innehar og formålet med sikring, må det gjennomføres gode og sikringsrisikoanalyser. Dette legger tilrette for balanserte og kostnadseffektive sikringstiltak. Sikkerhet koster, men viser sjeldent sin verdi før den blir utfordret eller testet. *«Det er krevende å betale for at noe ikke skal skje»* (Mærli, 2012). Sikkerhetstesting vil kunne vise sikringstiltakenes effekt og verdi. På bakgrunn av dette er følgenede problemstilling valgt for oppgaven:

Hva er mulige årsaker til at virksomheter ikke sikrer seg mot tilsiktede uønskede handlinger?

For å besvare problemstillingen er det valgt følgende forskningsspørsmål:

1. *Hva er sikkerhet og risiko i en sikringkontekst?*
2. *Hvordan foregår sikring i dag?*

3. Hvordan tas beslutninger i en sikringskontekst?

1.2.1 Struktur på oppgaven

I kap. 1 presenteres oppgavens tema og hvorfor problemstillingen i oppgaven er aktuell i dag. I kap. 2 presenteres de teoriene som er valgt til å drøftes opp mot empirien i oppgaven. Kap. 3 er metodekapittelet, der forskningsprosessen beskrives. Kap. 4 består av presentasjon av empiri, og drøfting av empirien opp mot teori. I kap 5 er konklusjonen som søker å besvare oppgavens problemstilling, og i kap. 6 er litteraturlisten. Til sist er kap. 7 vedlegg til oppgaven, og her finnes definisjoner av begreper, oversikt over sentrale aktører og personer i sikkerhetsfagmiljøet.

1.2.2 Begrepsforståelse

En av utfordringene i denne oppgaven er å ha en konsistent og klar forståelse av hva sentrale begreper i litteraturen betyr. Det er ingen konsensus i sikkerhetsfaget om begrepenes eksakte betydning og hvordan de skal defineres. Begrepsforståelsen varierer mellom lærebøker, dokumenter, standarder og fagmiljøer. Begreper er formulert likt, men har ulik betydning. Det er viktig å ha klarhet i begrepenes betydning. Videre vil det forklares hva NS 583X-serien omfatter.

2. Teori

Første del av teorikapitlet er en teoretisk fremstilling begrepene ”sikkerhet” og ”risiko” i en sikringskontekst. Giovanni Manunta har skrevet en doktoravhandling ”Towards a Security Science Through a Specific Theory and Methodology” (1997), og denne er sentral for å forklare sikkerhetsbegrepet. Videre består teorikapitlet av to samfunnsvitenskapelige kriminologiske teorier. Kriminalitetsteorier kan og bør bidra til kriminalitetsbekjempelse. Kriminalitetsteorier skal være virkelighetsnære, enkle å forklare, lære og bruke i praksis (Felson og Clarke, 1998). Disse teoriene bygger på et gammelt ordtak som sier at «mulighet gjør tyv». Dette er mer enn et gammelt ordtak, og har en viktig betydning for politisk og praktisk bekjempelse av kriminalitet. Til slutt består teorikapitlet av risikostyring, sikkerhetsråd til forebyggende sikkerhet og beslutningstaking under usikkerhet med beslutningsstrategier.

2.1 Sikkerhet, risiko og kriminalitet

2.1.1Sikkerhet

Å skulle definere «sikkerhet» er en vanskelig oppgave. Sikkerhet kan være så mangt: en enhet, -prosess, tilstand, et produkt eller makt (Stranden). Begrepet sikkerhet blir ofte brukt løst i forskjellige kontekster, som for eksempel nasjonal sikkerhet, internasjonal sikkerhet, industriell sikkerhet, privat sikkerhet og fysisk sikkerhet. Definisjonene er ikke klare og brukes ofte om hverandre (Post og Kingsbury, 1991:1, Manunta, 1997:28). Sikkeret er et flyktig begrep, og det er ikke enighet på operasjonelt nivå om definisjonen av sikkerhet. (Manunta, 1997:19). En generell definisjon av «sikkerhet» er *«reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare»* (NS 5830:2). Denne definisjonen stammer fra samfunnsvitenskapelig akademia og har sitt utspring i den originale latinske betydningen “frihet fra bekymring, frykt angst, og fare…”(FFI, 2015:120)

«Security appears to be as old as life» (Manunta, 1997:20). Det ligger i menneskets overlevelsesinstinkt å vokte seg mot farer og trusler for å beskytte liv, hese og verdier. I «fight or flight» begrepet ligger det at vi mennesker forsøker å eliminere farer og trusler ved å unnvike eller bekjempe disse (Manunta, 1997:21). Det blir vanskelig å beskytte sine verdier

nå man flykter, og det ble naturlig mer fokus på tiltak som kunne hindre farer og trusler fra å skade familie og verdier.

Manunta (1998) har utarbeidet en formell definisjon av sikkerhet :

$$S = f(A, P, T)$$

Dette kan grovt oversettes til norsk som: "Sikkerhet er en funksjon av interaksjonen mellom komponentene: verdi, beskytter og trussel" (Manunta, 1998:134). Det finnes *ingen* verdi før den som innehar verdien anser den verdt å beskytte. En *beskytter* er noen som: er i besittelse av- eller som har asnvaret for en verdi, er interessert i å beskytte verdien, har den nødvendige myndigheten og kapasiteten til å gjøre dette og tar beslutningen om å beskytte verdien. I en gitt sikkerhetskontekst eksisterer ikke en *trussel* før en beskytter oppfatter den som en trussel (Manunta, 1997:156-157).

Den formelle definisjonen av sikkerhet ovenfor tar ikke hensyn til hvordan sikkerhet påvirkes av eksterne faktorer. Den blir for enkel når man skal forklare beslutningstakingprosesser i en sikkerhetskontekst. Det er nødvendig å bevege seg fra teori til praksis, for å kunne forstå hvordan faktorer gjør hver sikkerhetskontekst unik. Derfor er begrepet *situasjon* (Si) blitt inkludert i den formelle definisjonen av sikkerhet:

$$S_{(A)} = f(P, T)\ Si$$

Sikkerheten til en gitt verdi S(A) er en funksjon av beskytteren (P), Trusselen (T), i henhold til deres spesifikke Situasjon Si. Identifisering, analysering og vurdering av forhold som har med sikkerhet å gjøre påvirkes av konteksten og omstendighetene rundt. "Si" er er med på å forklare hvordan omstendighetene og konteksten rundt sikkerhetsprosessen påvirker de tre faktorene: verdi, trussel og beskytter (Manunta, 1998:177).

Det er flere akademiske tilnærminger til sikkerhet og kontekster sikkerhet oppstår i. Hver og en av disse utgjør et særegen disiplin i sikkerhetsstudiet Noen av disse kontekstene er listet opp under (Manunta, 1997:34):

- Statlig: opprettholde den offentlige orden for offentlig gode.
- Politisk: opprettholdelse og beskyttelse av Statens makt.
- Juridisk: juridiske konsekvenser for ulovlig atferd.
- Kriminologisk: årsakene og dynamikkene til kriminell atferd.
- Sosiologisk: de sosiale årsakene og dynamikkene til avvikende atferd.
- Sosial: hvor interaksjonene med samfunnet er det viktige.
- Psykologisk: aspekter ved kognitive og atferd i en situasjon som medfører frykt.
- Matematisk: den sannsynlige effekt av en skadelig hendelse.
- Økonomisk: økonomiske aspekter og handlinger som årsaker til konsekvenser av en skadelig hendelse.

Det er mange tilnærminger, både teoretiske og operative, til konseptet sikkerhet. Hver og en har forskjellige karakteristikker, mål, antakelser, definisjoner og metodikker. De operasjonelle definisjonene påvirkes av kultur og forståelse av sikkerhet. Dette påvirker videre hvilken sikkerhetsmetodikk som anvendes, enten det er kriminalitet, økonomi, risikoanalyser når det gjelder sårbarhet eller mulighet (Manunta, 1997:36). Hovedproblemområdene forståelsen av sikkerhet er mangelen på teori, forvirring rundt definisjoner og det store mangfoldet av tilnærminger.

2.1.2 Risiko

Risiko dreier seg alltid om hva som kan skje i framtiden (Rausand og Utne, 2009). Det er flere måter å forstå risikobegrepet på. Det er også viktig å forstå at det er flere perspektiver på risiko når ulike fagområder og tradisjoner skal samarbeide om problemstillinger. Tradisjonelt kan risiko forstås som: *"usikkerhet om hva som blir konsekvensene eller utfallene av en gitt aktivitet»* (Aven, et. al. 2004:37). I Norge er det to tilnærminger til risikovurderinger. Dette er NS 5814 og NS 5832. De har forskjellige tilnærminger til risikobegrepet. NS 5814 er tuftet på en tradisjonell teknisk – naturvitenskapelig tilnærming, mens NS 5832 har en samfunnsvitenskapelig tilnærming til risiko. Risiko defineres i de to standardene som:

NS 5814: *«uttrykk for kombinasjonen av sannsynligheten for og konsekvensene av en uønsket hendelse»* (Rausand og Utne, 2009:22).

NS 5832: *«uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens*

sårbarhet overfor den spesifiserte trusselen» (NS 5830:5).

Tradisjonell teknisk – naturvitenskapelig tilnærming til risiko

Det er flere perspektiver på risiko i risikostyring. I det tekniske perspektivet fungerer fortiden som en guide for fremtiden (Renn, 2008). Den tekniske tilnærmingen til risiko begrenser seg til å estimere risiko ved bruk av matematiske/statistiske og fysiske modeller. Risikoen uttrykkes ofte kvantitativt og begrenser seg til å estimere fysisk skade. Dermed blir det mulig å tallfeste sannsynligheten (Aven et. al. 2004:38). I en teknisk sannsynlighetsvurdering fremstilles risiko ofte i en risikomatrise, med variablene *sannsynlighet* og *konsekvens*. Den teknisk tilnærmingen er avhengig av to betingelser: For det første må det foreligge nok statistisk data slik at det kan gjøres meningsfulle prediksjoner, og for det andre må de kausale årsaks-virkningsforholdene som fører til de negative effektene, opptre stabilt over en tidsperiode (Renn, 2008:13). Naturhendelser som flom opptrer ved jevne mellomrom over tid, og er et eksempel på en hendelse det går an å beregne en statistisk risiko for. Uten tilstrekkelig data vil estimatene kunne bli veldig usikre. Den tekniske tilnærmingen er blitt kritisert av samfunnsvitenskapen, da denne tilnærmingen ikke tar hensyn til det folk oppfatter som en uønsket effekt. Forskjellig oppfattelse av risiko bestemmes i stor grad av at vi mennesker har ulike verdier, preferanser og kultur som former vår opplevelse av den verden vi lever i (Renn, 2008:13). Derfor kan den sosiale og kulturelle risikopersepsjonen være forskjellig fra en vitenskapelig teknisk tilnærming til risiko. Begge tilnærmingene har behov for å analysere og beskrive risiko, men forskjellen ligger i hvordan risikoen blir tolket, brukt og kommunisert.

Samfunnsvitenskapelig tilnærming til risiko

«Risikopersepsjon handler om hvordan folk flest forstår, opplever og håndterer risiko og farer» (Aven, et. al., 2004:40). Her beskrives det at langt flere faktorer spiller inn i risikopersepsjon enn det man tar hensyn til i de tekniske-naturvitenskapelige og økonomiske tilnærmingene (Boyesen, 2003). I de to sistnevnte tilnærmingene vil man gå glipp av viktige momenter som er nødvendige for å forstå risiko, og hvordan risikoen skal håndteres og reduseres (Aven, et. al., 2004:41). Sammfunnsvitenskapelig tilnærming til risiko er ikke en statistisk prediksjon, men heller en subjektiv fortolkning av risiko. Den subjektive

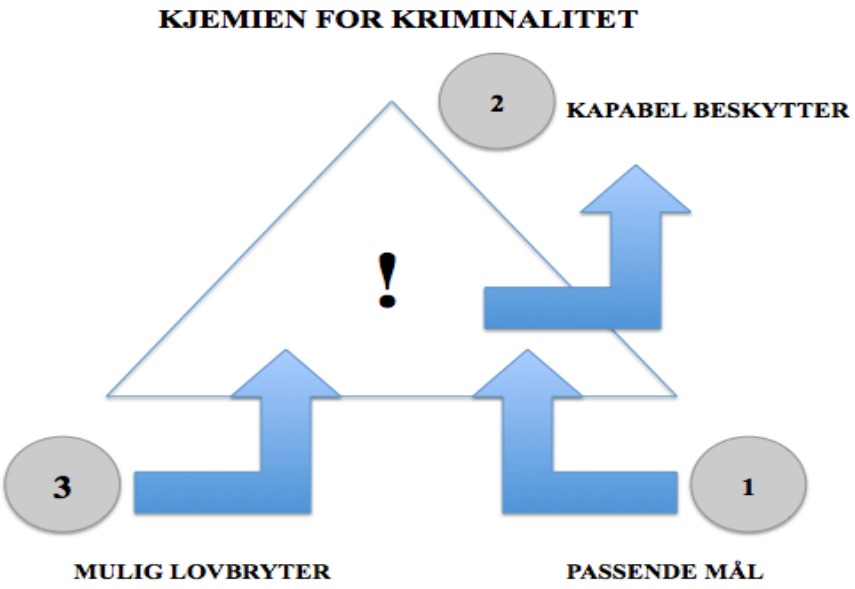
fortolkningen baserer seg blant annet på folks holdninger, verdier, verdensforståelse og kultur, og er gjetninger ut fra forestillinger fremfor vitenskapelig data (Boyesen, 2003:9).

Økonomisk tilnærming til risiko

Risikoen i det økonomiske perspektiv representerer subjektiv nytteverdi, fremfor fysisk skade/uønskede effekter. Nytteverdien kan beskrives som graden av tilfredsstillelse eller misnøye forbundet med en mulig handling eller endring. Skiftet fra «forventet skade» til «forventet nytte» fører til at alle konsekvenser, inkludert psykologiske og sosiale effekter, kan måles ved subjektiv (u)tilfredshet. Subjektiv tilfredshet gjør det mulig å sammenlikne risikoutfordringer- og fordeler ved ulike beslutningsalternativer (Boysesen, 2003). Den klassiske måten å måle nytte på er å se hvor mye penger noen er villige til å bruke for å oppnå en høyere grad av tilfredshet enn å bli værende på status quo (Renn, 2008).

2.1.3 Rutineaktivitetsteorien

Lawrence E. Cohen og Marcus Felson presenterte i 1979 *Routine Activity Theory* for å kunne analysere og forklare kriminalitet. Teorien fokuserer ikke på å karakterisere kriminelle, men heller omstendighetene rundt kriminelle handlinger. Individuell oppførsel er et produkt av interaksjon mellom person og omstendighet. Det må foreligge tre faktorer for at en kriminell handling skal skje: *likely offenders, suitable targets* and the *absence of capable guardians*. Det må altså en motivert gjerningsperson, et passende mål og fravær av kapable beskyttere til for at en kriminell handling kan finne sted i et gitt tidsrom (Cohen og Felson, 1979, s. 588). Hvis minst et av disse elementene fjernes, så fjernes også forutsetningene for at en kriminell handling kan skje. Dette er hovedessensen i securityfaget.



Figur 1: Kriminalitetstriangelet (Felson & Clarke, 1998, s. 4)

Figur 1 illustrerer hvilke rammevilkår som må være tilstede for at kriminalitet skal kunne skje. Man må altså ha en mulig lovbryter og et passende mål i sammenfallende tid og sted, der målet har fravær av kapable beskyttere. Teorien tar for gitt at det er en motivert gjerningsperson og fokuserer heller på de to andre elementene. Teorien bruker «mål» i stedet for «offer», fordi målet for en kriminell handling kan være både en person og et objekt. Målets verdi og tilgjengelighet har effekt på gjerningspersonens motivasjon for å gjennomføre den kriminelle handlinge (Felson og Clarke, 1998, s. 5).

2.1.4 Teorien om situasjonell kriminalitetsforebygging (SCP)

Situasjonell kriminalitetsforebygging (*Situational Crime Prevention - SCP*) handler om å redusere muligheten for spesifikke typer kriminalitet ved å øke risiko, samt vanskeliggjøre og redusere gevinsten av ugjerningen (Clarke, 1997:4). Poenget er å gjøre det mindre attraktivt å begå kriminelle handlinger ved å forbedre samfunnet og institusjoner. Her snakkes det ikke om rettssystemet, men heller om at flere aktører og institusjoner, private og offentlige, søker å gjøre seg mindre attraktive mot kriminelle handlinger. Situasjonelle kriminalitetsforebyggende tiltak må i stor grad skreddersys til modus og de spesifikke kriminalitetskategoriene, fordi omstendighetene rundt hver ugjerningen er så forskjellig (Clarke, 1997:4). De mulighetsreduserende tiltakene kan være alt fra fysiske sikringstiltak til

opplæring i sikkerhetsrutiner. I SCP er det utarbeidet et sett «mulighets-reduserende» teknikker for avskrekke forbrytere fra å gjøre en ugjerning, samt å redusere attraktiviteten mot spesifikke kriminelle mål.

2.2 Risikostyring, sikkerhetsråd og beslutningstaking

2.2.1 Risikostyring

I følge Covello og Mumpower (1985), har statsmaktene helt siden oldtidens dager grepet direkte inn for å redusere, dempe og kontrollere risiko. De tidligste statlige forsøk på å redusere risiko kan spores til Kina i det femte århundre før Kristus, da religiøs tro førte til at mennesker ble ofret for å redusere sjansen for flom eller andre uønskede naturfenomener med negative konsekvenser. Et annet eksempel er under Svartedøden år 1348 til 1349, ca 25 prosent av Europas befolkning døde. Tiltak som isolasjon og karantene ble innført av statsmaktene (Covello og Mumpower, 1984:111).

Det er flere definisjoner på hva risikostyring. Rausand og Utne (2009) definerer risikostyring som *«en kontinuerlig ledelsesprosess som har som målsetting å identifisere, analysere og vurdere mulige risikoforhold i et system eller i en virksomhet, samt finne fram til og iverksette tiltak som kan redusere skadevirkninger»* (Rausand og Utne, 2009, s. 77). Renn (2008) beskriver risikostyring (risk governance) som et komplekst nett av aktører, regler, konvensjoner, prosesser og mekanismer som omhandler hvordan relevant informasjon om risiko blir samlet, analysert og kommunisert, og hvordan ledelsesbeslutninger blir gjort. Risikostyring er videre et struktureringsverktøy og rammeverk som kombinerer risikovurderinger, risikoledelse og risikokommunikasjon for å styre risiko (Renn, 2008, s. 8-9). Aven definerer videre risikostyring som «*alle tiltak og aktiviteter som gjøres for å styre risiko. Formålet med risikostyring er å sikre den riktige balansen mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap»*. (Aven, 2007, s. 13).

Det er viktig å utvide kriteriene for vurdering, karakterisering, evaluering og ledelse av risikoer til å omfatte mer enn de teknologiske og vitenskapelige faktorene som tidligere har dominert modeller for risikostyring. Allmenhetens verdier, bekymringer og persepsjon av

risiko er like viktige å identifisere og forstå, og må derfor bli inkludert i risikostyringsmodeller (Renn, 2008:3). Risikostyring kan brukes både deskriptivt og normativt. Deskriptivt i form av at risikostyring beskriver hvordan flere aktører, individer, institusjoner, offentlige og private, arbeider sammen om usikre, komplekse og/eller tvetydige risikoer. Normativt i den forstand at risikostyring består av regler, rammeverk, konvensjoner, prosesser og mekanismer som handler om hvordan relevant informasjon om risiko blir innsamlet, analysert og kommunisert, og videre hvordan regulerende beslutninger blir tatt (van Asselt og Renn, 2011:435). I følge van Asselt og Renn (2011) kan risikostyring defineres på to måter: (1) «som et kritisk studie av komplekse interaksjoner mellom nettverk der valg og beslutninger om risiko gjøres». (2) «som et sett av normative prinsipper som kan informere alle relevante aktører i samfunnet om hvordan man skal håndtere risiko på en forsvarlig måte» (van Asselt og Renn, 2011, s. 443). Risikovurderinger og risikoanalyser inngår som et sentralt element i risikostyringen, og skal legge grunnlaget for de beslutninger og prioriteringer lederne i en virksomhet gjør for å styre risiko (FFI, 2015:27).

2.2.2 Veileder i terrorsikring (2015) - sikkerhetsråd

Det å ha god forebyggende sikkerhet og beredskap er et kollektivt samfunnsansvar, og noe enhver virksomhet bør kunne ivareta. Det viktigste er å forberede seg på det uventede, da den største sårbarheten er *likegyldighet* overfor sikkerhet (Veileder i terrorsikring, 2015:03). Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Politidirektoratet (POD) har utarbeidet ”Veileder i terrorsikring” (2015), heretter omtalt som VT (2015). I VT er det utarbeidet 9 sikkerhetsråd som skal være et hjelpemiddel for virksomheter i å systematisere og tilpasse sikringstiltak i forhold til verdiene virksomheten ønsker å beskytte, realistiske trusler og sårbarheter som uttnyttes (PST, NSM, POD, 2015:3). De følgende sikkerhetsrådene er listet opp i tabell nr. 1.

Tabell 1: Sikkerhetsråd (Veileder i terrorsikring, 2015:)

Sikkerhetsråd		
1	**Sikkerhet er et lederansvar.**	Planlegg sikkerhet fra starten ved alle type endringer, prosjekter og programmer, slik som omorganisering, relokalisering eller lignende.
2	**Gjennomfør en sikringsrisikoanalyse av virksomheten.**	For å kartlegge hvilke verdier som skal beskyttes, hvilke trusler virksomheten kan være utsatt for og hvilke sårbarheter som kan utnyttes. Forstå virksomheten opp mot de sikringsbehov som foreligger og beskytt verdiene med tilpassede tiltak.
3	**Virksomheten bør ha en hensiktsmessig organisering av sikkerhets- og beredskapsarbeidet med en utpekt sikkerhetsleder og et styringssystem.**	De ansatte skal være kjent med sikkerhetsinstrukser, sikkerhetsrutiner, evakueringsplaner, samt være årvåkne overfor aktuelle trusler.
4	**Sørg for grunnsikring i normalsituasjonen.**	Dette er virksomhetens eget ansvar. Man kan ikke forvente forvarsel om terrorhandlinger. Fysisk sikring beskytter både informasjon, objekt og personell.
5	**Hold orden i bygg og publikumsområder, sørg for at de er god opplyst.**	Vurder å begrense adkomstpunkter og sørg for at ansatte, besøkende og kjøretøy har adgangstegn. Hvis det er mulig, unngå at kjøretøy parkeres i eller i nærheten av bygningen.
6	**Lag et beredskapssystem for virksomheten med forberedte tiltak, som kan iverksettes ved endringer i trusselbildet eller dersom det skjer en hendelse.**	Forbered påbygningstiltak ved skjerpet trussel, slik som adgangskontroll for ansatte, besøkende, kjøretøy, samt epost- og varemottak.
7	**Ingen plan er bedre enn selve gjennomføringen.**	Sørg for å gjennomføre øvelser for å teste ut beredskapsplaner og sikringstiltak. Dette gjelder eksempelvis mottak av terrortrusler, søkerutinger og evakuering ved sikkerhetshendelser.
8	**Vurder hvordan virksomheten best kan beskytte sensitiv informasjon om hvilke informasjonssikkerhetstiltak som er nødvendige.**	Husk at det er nær sammenheng mellom fysisk sikkerhet og IKT-sikkerhet. Sørg for at virksomhetens viktigste funksjoner kan gjenopprettes dersom IKT eller eiendom blir utilgjengelig.
9	**Søk råd og opplysninger hos politiet og andre myndigheter.**	Etabler gode rutiner for kontakt mellom virksomheten og politi/nødetater.

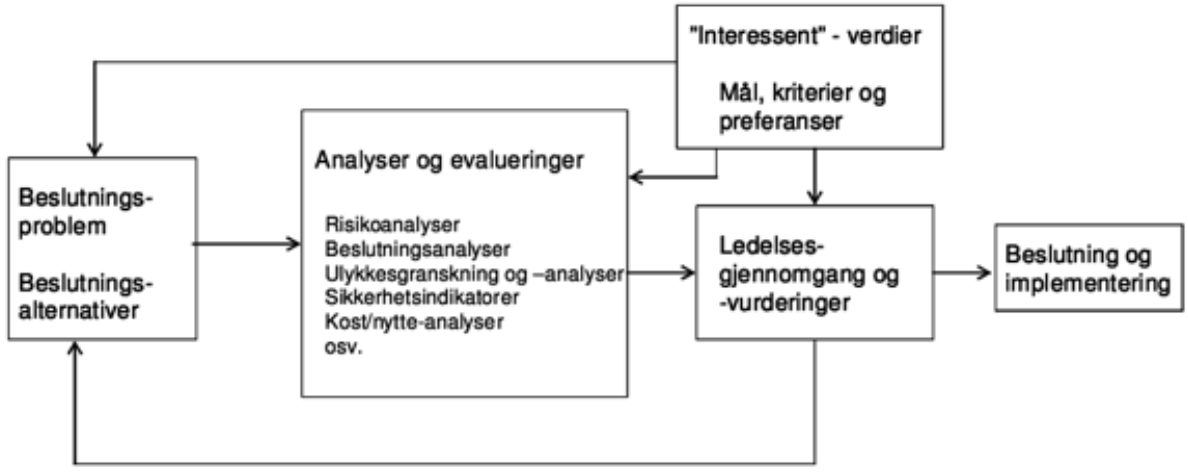
2.2.3 Security

Som tidligere nevnt er faguttrykket for sikkerhet mot tilsiktede uønskede handlinger er *"security"*. Et annet begrep i sikkerhetsfaget er *"safety"*. *Safety* er hendelser som skjer som en rekke av tilfeldigheter, der ingen har bevisst intensjon om å utgjøre skade. Hendelser som faller under *safety* er for eksempel ulykker og natrukatastrofer. Det foreslås at man bruker de norske begrepene *"sikring"* for security og *"trygghet"* for safety (NOU:2006:6). Disse begrepene skiller med andre ord mellom to typer sikkerhet:

Security: *"Sikkerhet mot uønskede hendelser som et resultat av overlegg og planlegging"*.
Safety: *"Sikkerhet mot uønskede hendelser som opptrer som en følge av en eller flere tilfeldigheter"* (NOU:2006:6).

2.3 Beslutningstaking og usikkerhet

«Risikostyring innebærer beslutningstaking i situasjoner med høy risiko og store usikkerheter, og slik beslutningstaking er utfordrende, da det er vanskelig å forutsi (predikere) konsekvensene (utfallene) av beslutningene» (Aven, 2008:21). Hvis man skal vurdere kvaliteten på en beslutning kan man med fordel fokusere på selv beslutningsprosessen. Det er i denne prosessen det gjøres vurderinger og handlinger som er nødvendig for å ta den beste beslutningen.



Figur 2: Modell for beslutningstaking under usikkerhet (Aven, 2008:22)

Utgangspunktet er et beslutningsproblem, der oppgaven er å velge mellom alternativer som på en best mulig måte oppfyller og møter de mål og kriterier som er satt av ledelsen og interessenter. Resultatet av ulike risikoanalyser og risikovurderinger legger et beslutningsgrunnlag som beslutningstaker må gjennomgå før en beslutning blir tatt. Beslutningsgrunnlaget vil sjelden være komplett og avdekke alle forhold knyttet til beslutningsproblemet. Det er leders oppgave å ta beslutninger når det oppstår usikkerhet. Analytikere skal kun produserer beslutningsgrunnlaget (Aven, 2008:22). Mangel på kunnskap skaper usikkerhet, og det finnes ulike metoder som kan bidra til å vurdere styrken på kunnskap. En metode fremholder at hvis en eller flere av betingelsene er tilstede, er kunnskapen svak:

1. Antakelser er veldig forenklet.
2. Data er ikke tilgjengelig eller upålitelig.
3. Det er mangel på enighet/konsensus mellom eksperter.
4. Fenomenet som er involvert er ikke godt forstått; modeller er ikke-eksisterende, eller er er kjennetegnet av å gi dårlige predikasjoner. (Aven, 2013:138).

Beslutningsstrategier er den filosofien og de prinsippene som følges i forhold til hvordan beslutningsprosessen skal være, og hvordan beslutningen tas. Hvem skal være med i beslutningsprosessen, hvordan skal prosessen gjennomføres og hvilke analysemetoder skal brukes? *«En beslutningsstrategi tar hensyn til effekt på risiko (slik som den fremkommer i risikoanalysene) og tar usikkerhetsdimensjoner som ikke fanges gjennom analysene».* Dette resulterer i at beslutninger baseres på beregnet risiko, kost-nytteanalyser, og anvendelse av føre-var-prinsippet og forsiktighetsprinsippet. Ulike beslutningssituasjoner krever ulike strategier (Aven, 2008, s. 24).

Forsiktighetsprinsippet handler om at *«forsiktighet skal være et rådende prinsipp når det er usikkerhet knyttet til konsekvensene (utfallene)* (Aven, 2007:99). Ved anvendelse av forsiktighetsprinsippet spiller ikke sannsynligheten for om en uønskede hendelse skal inntreffe en rolle, så lenge risikoen vurderes som signifikant. Forsiktighetsprinsippet er forankret i industrien i form av reguleringer og krav. Forsiktighetsprinsippet praktiseres blant

annet ved at virksomheter implementerer robuste løsninger og sikkerhetsbarrierer for å unngå og/eller redusere mulige negative konsekvenser av en uønsket hendelse. Graden av robuste løsninger og sikkerhetsbarrierer må vurderes og balanseres mot andre hensyn som økonomi og kostnader (Aven, 2007:100). I komplekse organisasjoner foreligger det som regel alltid motstridende mål, der for eksempel produksjonsmål kommer i konflikt med sikkerhetsmål (Boyesen, 2003:10).

Et annet prinsipp er ALARP-prinsippet (As Low As Reasonable Practicable). ALARP-prinsippet er et hjelpemiddel i vurderingen av om en risiko er tolerabel, og innebærer at identifiserte tiltak skal implementeres, såfremt man det ikke kan dokumenteres at det foreligger et urimelig misforhold mellom kostnader/ulemper og nytten ved tiltaket. Risikoen bør med andre ord reduseres så langt som praktisk mulig (Aven, 2007:118). Hvis kostnaden ved å redusere en risiko overstiger nytten, anses risikoen som akseptabel. Selv om ALARP-prinsippet fremstår som en enkel metode for å vurdere risiko, krever den likevel en betydelig tolkning. Den kan også være vanskelig og kostbar å anvende. For å fastsette om en risiko er ALARP, er det nødvendig å demonstrere at alle risikoreduserende tiltak og metoder er upraktiske. For å kunne gjøre dette må alle mulige risikoreduserende tiltak identifiseres, noe som er en stor og kostbar oppgave (Hughes, 2016). Ved sikkerhet bruker man risiko, beredskap og ytelse for barrierene for å vurdere kvaliteten på løsninger og tiltak. *«Et risikoakseptkriterium (angitt som øvre grense for risiko) angir et område som er slik at dersom den beregnede risikoen faller innenfor dette området, vurderes risikoen som uakseptabel og tiltak er påkrevd"* (Aven, 2007:116). For en som ikke har mye kunnskap om risiko, vil et risikoakseptkriterium fremstå som oversiktlig. Et problem er imidlertid at dette fører til en mekanisert prosess der beslutninger under stor usikkerhet er nødvendig. Det bør også tas hensyn til andre aspekter knyttet til hva tiltakene vil koste, og hva som er praktisk mulig å få til, samt hvordan risikoen oppleves. Vanskelige beslutninger skal tas under stor usikkerhet, og da kan risikoakseptkriterier mekanisere prosessen (Aven, 2007:116).

3. Metode

Dette kapittelet vil redegjøre for de metodiske valg som er gjort i denne oppgaven, og inkluderer valg av forskningsdesign, fremgangsmåte for datainnsamling, og til sist en evaluering av oppgavens pålitelighet og gyldighet.

3.1 Forskningsdesign

Utgangspunktet for oppgaven var et ønske om å kartlegge sikkerhetsfagfeltet med fokus på sikring av virksomheter mot terror og andre kriminelle handlinger. Det var derfor behov for en åpen og fleksibel tilnærming til forskningsdesign. En slik tilnærming er fleksibel i den forstand at den tillater at forskningen kan endre retning etter hvert som ny informasjon blir tilgjengelig, og utformingen passer bra til forskning hvor problemstillingens karakter er dårlig forstått. Forskningsdesignet er basert på flere ulike datakilder inkludert et massivt litteraturstudium, kvalitative intervjuer og deltakelse på møter og konferanser.

3.2 Datakilder

I denne oppgaven er det hentet data fra flere ulike kilder; jeg har studert nøkkeldokumenter, deltatt på kurs, møter og konferanser. Jeg har gjennomført to telefonintervjuer, og brukt et lydopptak av en paneldebatt. I denne oppgaven er det med andre ord brukt både *primær-*, *sekundær-* og tertiærdata. *Sekundærdata* er data som allerede er innsamlet av andre og kan ha et generelt formål som offentlige statistikker og publikasjoner eller med formål for et spesifikt forskningsprosjekt (Blaikie, 2010:160). Primærdata får man ved å benytte metoder som intervju, observasjon eller spørreskjema (Jacobsen, 2005:137). Ved sekundærdata har ikke forsker innhentet informasjonen direkte fra kilden. I stedet baserer forskeren seg på opplysninger som er samlet av andre. Denne informasjonen kan være samlet til et annet formål enn det forskeren ønsker å belyse, kan kan samles under fellesbetegnelsen *tekster* (Jacobsen, 2005:137).

Tabell 2: Oversikt over datakilder

Dokumentanalyse:	Det har vært et kontinuerlig litteraturstudie gjennom hele oppgaveprosessen. Dette har i hovedsak vært sekundær- og tertiærdokumenter.

Telefonintervju:	Det ble gjennomført to semistrukturerte telefonintervjuer i april 2016. Dette er primærdataen i oppgaven.
Kurs:	Deltagelse på kurset "Innføring i sikringsrisikoanalyse" 29-30. april, 2016.
Konferanse:	Deltagelse på konferansen "Security by Crime" 19. september, 2015
Samtaler og møter:	Møter og samtaler med fagpersoner gjennom forskningsprosessen.

I denne oppgaven er de to intervjuene utvetydig primærdata. På møtet ble det holdt en PowerPoint presentasjon som jeg fikk tilgang på etterpå. Powerpoint presentasjonen i kurset og Roy Strandens gjennomgang av denne fungerte som et bakteppe for oppgaven. Når det refereres til Powerpointen og Strandens forklaring refereres det slik: (Stranden). Som nevnt er store deler av empirien innhentet ved et omfangsrikt dokumentstudium. Her er alt fra offentlige myndigheters veiledere og rapporter, til artikler i nettaviser og foredrag som er lagt ut på internett brukt. Et sentralt dokument i denne oppgaven er FFI-rapporten "Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger" (2015). I rapporten er det for eksempel vedlagt transkriberte intervjuer av sentrale personer i sikkerhetsfagmiljøet. Dette er en form for rådata, da det ikke er analysert, men transkrivert. Rådataen i FFI-rapporten er innsamlet til det formål som ligger nært opp mot det denne oppgaven ønsker å kartlegge. Derfor har mange av disse intervjuene blitt veldig sentrale og brukt flittig gjennom hele oppgaven. Andre svært sentrale kilder er Norsk Standard 5832 "Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse" og Norsk Standard 5814 "Krav til risikovurderinger". I følge Blaikie (2010) er tertiærdata dekundærdata som har blitt analysert av noen andre, og i slike tilfeller er ikke rådataen tilgjengelig, men bare resultatene av analysen (Blakie, 2010). Hvis man ser bort i fra intervjuene i vedlegget som er en form for rådata, så kan selve FFI-rapporten betegnes som tertiærdata. FFI har analysert rådataen og kommet med resultater og konklusjoner som følge av dette.

I kvalitativ forskning bruker forskeren seg selv som et instrument og bearbeider og fortolker data ut i fra subjektivitet, kunnskap og kompetanse. Det blir derfor vanskelig for en annen forsker å kopiere en annens kvalitative forskning. For å styrke påliteligheten kan forskeren gi en inngåeende beskrivelse av kontekst og en åpen og detaljert fremstilling av framgangsmåten for forskningsprosessen (Johannessen, et. al., 2010:229).

3.3 Datainnsamling

Det er som nevnt flere former for datainnsamling, og under følger en grundigere beskrivelse av datagrunnlaget.

3.3.1 Dokumentanalyse

Èn av metodene i oppgaven er en kvalitativ dokumentanalyse, der veiledninger, publikasjoner, rapporter og standarder er det empiriske fundamentet. Videre er tidsskrifter og artikler fra ulike aviser og nettsider en del av empirien. Disse dokumentene kan betegnes som sekundær- og tærtierdata (Blaikie, 2010). De offentlige rapportene, veiledningene og standardene kan man si er utarbeidet det det formål å gi generell informasjon om dokumentets innhold. Tidsskrifter, artikler og debattinnlegg er sekundær- og tertiærdata, da de er fortolket og bearbeidet av andre.

Oppgaveprosessen startet med et litteratursøk, med fokus på å finne oversiktsartikler om oppgavens tema. I litteratursøket ble det brukt nøkkelbegreper som: sikkkerhet, sikringstiltak, virksomheter, objektsikring, fysisk sikring, risikoanalyse, risikostyring, beslutningstaking med mer. Som følge av dette ble det tydelig at de mest sentrale fagmiljøene innenfor oppgavens tema var norske sikkerhetsmyndigheter og andre organer som blant annet Nasjonal sikkerhetsmyndighet, Politiets sikkerhetstjeneste, Forsvarets forskningsinstitutt, Næringslivets sikkerhetsråd. Det var to oversiktsartikler som skilte seg særlig ut i denne fasen av oppgaven. Dette var *"Terrorsikring: En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger"* (2015) utarbeidet av Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste og FFI rapporten "*Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger"* (2015). Formålet med "veilederen i terrorsikring" er å gi offentlige og private virksomheter et hjelpemiddel i hvordan man skal sikre seg mot terror og kriminalitet, og fungerte for oppgavens del som en innføring i sikringsarbeid mot TUH. FFI-rapporten er en vurdering av to forskjellige risikovurderingsprosesser (NS 5814 og NS 5832) i forhold til TUH, og videre gi anbefalinger om hvilken risikovurderingsprosess og momenter som bør brukes mot TUH. I FFI-rapporten er det gjort flere semistrukturerte telefonintervjuer av personer i sikkerhetsfagmiljøer som uttaler seg om risikovurderinger mot TUH. Disse

kvalitative intervjuene samlet i et vedlegg og kan derfor anses som sekundær-rådata, da de er transkribert, men ikke analysert. De kvalitative telefonintervjuene er brukt aktivt i oppgaven.

3.3.2 Semistrukturert telefonintervju

I denne oppgaven er det gjennomført kvalitative semistrukturerte telefonintervjuer av to informanter. Informant 1 jobber som sikkerhetsrådgiver for et konsulentselskap og informant 2 jobber med fysisk sikring av virksomheter. Et telefonintervju kan betegnes ved at det er middels nærhet i form av fysisk avstandt til informasjonskilden og lav til middels grad standardisering. Standardisering vil si hvor fleksibel intervjuet er. En spørreundersøkelse med identiske spørsmål er høy grad av standardisering, mens samtaleintervjuer er mer fleksibelt og av lavere standardisering (Ringdal, 2013:118).

Intervjuguiden var i liten grad av standardisert karakter, og bestod av overordnede temaer med åpne spørsmål. Dette førte til at det ble mulig å improvisere og stille oppfølgingsspørsmål underveis i intervjuet. Intervjuene ble tatt opp på lyd og begge intervjuene hadde en varighet på omtrent 30 minutter. Begge samtykket til at intervjuet ble tatt opp på lyd og lydopptakene er ble slettet etter at dataen var transkribert. Transkripsjonen skjedde kort tid etter at intervjuene ble gjennomført, og transkripsjonen bærer preg av at det er valgt ut passasjer fra intervjuet som ble oppfattet som mest relevant for oppgaven (Brinkmann & Tanggaard, 2010).

De to informantene som er intervjuet er anonymisert og det fremkommer ingen personopplysninger i oppgaven. Informantene ble informert om at deltakelse på intervjuet var frivillig og at de ikke måtte føle seg forpliktet til å svare på spørsmål de ikke ønsket å svare på. Videre ble de fortalt at de kunne trekke seg fra intervjuet på et hvilket som helst tidspunkt. Det er derfor ikke vedlagt et informasjonsskriv i denne oppgaven. Prosjektet er derfor ikke meldingspliktig til Norsk senter for forskningsdata.

Tabell 3: Informanter i oppgaven.

Informasjon	**Telefonintervju 1**	**Telefonintervju 1**
Informant:	Informant 1	Informant 2
Stilling:	Sikkerhetsrådgiver	Sikkerhetsrådgiver
Arbeidsoppgaver:	Jobber blant annet med utrabeidelse av risikoanalyser for virksomhet.	Jobber spesifikt mot å gi råd til virksomheter om fysiske sikringstiltak.

3.3.3 Deltakelse på konferanse, kurs og møter

Den 10.09.2015 deltok jeg på konferansen "Designing out crime" i regi av Næringslivets sikkerhetsråd (NSR) og COWI. Konferansen handlet om hvordan arkitektur kan redusere risiko for kriminalitet. Ved å integrere sikkerhet i prosjekteringsfasen og byggeprosessen ligger forholdene til rette for gode og kostnadseffektive sikringstiltak, og på samme tid ivaretas estetikk og åpenhet.

I mars 2016 deltok undertegnede på kurset "Innføring i sikringsrisikoanalyse" i regi av NSR. Kursleder var Roy Stranden. Dette var et innføringskurs i sikringsrisikoanalyseprosessen NS 5832, som innebar en teoretisk og praktisk gjennomgang av NS 5832. Deltakerne ble i stor grad involvert i kurset og det var stor takhøyde for å stille spørsmål. En sentral del av kurset var gruppebasert oppgaveløsing. Når det i oppgaven refereres til Stranden (Stranden) uten årstall og sidetall, er det fordi informasjonen er hentet fra powerpoint og Strandens fremstilling av denne i kurset.

I desember 2015 deltok undertegnede på et diskusjonsmøte om FFI-rapporten "*Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger"*(2015), arrangert av COWI. FFI presenterte rapporten for representanter fra blant annet NSR, NSM, COWI og Stortinget, påfulgt av diskusjon representantene i mellom etter presentasjonen. I april 2016 møtte undertegnede Audun Vestli og Julie Elisabeth Indrelid fra Senter for risikoreduserende design i COWI. Vestli er spesialrådgiver og Indrelid er sikkerhetsrådgiver i COWI. Møtet skapte en økt forståelse av hvordan sikkerhetsbransjen fungerer. Dette var ikke et intervju.

I mars 2016 holdt Morten Østerhaug, styreleder for Sikkerhetsledelse AS, en presentasjon og gjennomgang av sikringsrisikoanalysen NS 5832 for undertegnede i deres lokaler. Dette var en detaljert gjennomgang som gav en praktisk forståelse av utførelsen av NS 5832, samt annen relevant informasjon om sikkerhetsfagfeltet. Dette var ikke et intervju.

Ved å ha deltatt på konferanser, kurs og aktivt tatt kontakt med velvillige sentrale fafgpersoner i sikkerhetsfagmiljøet har jeg fått mange gode innspill. Noen av de personene jeg har snakket med blir ikke navngitt i metodekapittelet eller i oppgaven, da det ikke er avklart om disse vil navngis. De personene som navngis er hentet fra litteraturen oppgaven baserer seg på. Personenes navn og stilling er listet opp i vedlegget.

3.4 Datareduksjon og analyse

Utfordringen med kvalitativ forskning er å få noe fornuftig ut av en stor mengde, ofte ustrukturert data (Johannessen, Tufte, Christoffersen, 2010:165). Det første man må gjøre er å redusere noe av kompleksiteten, forenkle og strukturere for å få en oversikt. Analyse av kvalitativ data dreier seg om tre faser. Den første hovedoppgaven er å *beskrive* datamaterialet som er innhentet for å systematisere dataen. For det andre må *systematisere og kategorisere* uoversiktlig informasjon for å kunne formidle funn i datamengden. Til sist må man når dataen er systematisert *sammenbinde* og *fortolke* data og lete etter meninger, årsaker eller forsøke å generalisere (Jacobsen, 2005:186). Utgangspunktet for oppgaven var å kartlegge og få kunnskap om sikkerhetsfagfeltet. Dette medførte en omfattende orienteringsprosess som innebar gjennomgang av relevant litteretur og samtaler med fagpersoner. I takt med oppgavens utvikling og problemformulering ble det tydeligere hvordan datamaterialet skulle reduseres. I følge Johannesen (et.al, 2010) har en dataanalysen to hensikter: 1) organisere data etter tema, og 2) analysere og tolke (Johannesen, et.al., 2010:165). Datamaterialet ble organisert etter forskningsspørsmålene for å legge et et systematisk grunnlag for analysen. I denne oppgaven er det valgt å presentere empiri og drøfte denne fortløpende i samme kapittel. Årsaken til dette er at det vil bli mindre gjentakelser, og man får en tettere drøfting mot empirien fordi poenger og funn nevnes underveis. I konklusjonen vil det være lagt ved en tabell som oppsummerer antakelser og funn gjort i oppgaven.

3.5 Pålitelighet og gyldighet

Hoveddatamaterialet i oppgaven er publikasjoner utgitt av offentlige sikkerhetsmyndigheter og andre sikkerhetsorganisasjoner. Disse publikasjonene er blant annet veiledere, forskrifter, standarder og rapporter, og er i følge Brinkmann og Tangaard (2012) sekundære dokumenter, da det er dokumenter som er tilgjengelig for alle. De som har utarbeidet dokumentene er også i umiddelbar nærhet til det dokumentet handler om, for eksempel ved at en sikkerhetsorganisasjon praktiserer den veiledningen de har utarbeidet (Brinkmann & Tangaard, 2012:155). Videre er andre dokumenter i datamaterialet tidsskrifter, artikler, internettsider med mer. Disse kan betegnes som tertiære dokumenter, da de er tilgjengelige for alle og at de er bearbeidet på en eller annen måte med en hensikt, for eksempel en vitenskapelig debatt. Sekundærdokumentene som er utarbeidet av sikkerhetsmyndigheter og organiasjoner går til dels hånd i hånd med mange av de tertiære dokumentene. Årsaken til dette er at ofte så er tertiærdokumentene artikler og intervjuer med fagfolk fra sikkerhetsmyndighetene. På den måten kan man si at tertiærdokumentene kan fungere som en ”forlengelse” av sekundærdokumentene, noe som fører til at dokumentene oppleves konsistente med hverandre. Det er likevel viktig å vite at selv om mange av dokumentene er utarbeidet av offentlige aktører, så er det en utfordring med slike dokumenter at det ofte ikke fremkommer svakheter og uoverstemmelser i disse. I FFI-rapporten er det utført flere intervjuer med fagpersoner. Disse blir brukt og analysert i FFI-rapporten, men et sammendrag av hvert intervju er lagt i et vedlegg i rapporten. Disse anser jeg som en form for ”annenhånds rådata”, tatt i betrakning at FFI har den påvirkningen slike intervjuer preges av og at de har transkribert intervjuene. I og med at det fremkommer mye relevant i disse intervjuene brukes disse i denne oppgaven, selv om disse har blitt gjennomført med et til dels annet formål enn denne oppgaven har.

De to semistrukturerte telefonintervjuene er gjennomført forholdsvis sent i oppgaveskrivingprosessen, da det var et ønske om å få ytterligere belyst visse momenter som er av betydning i oppgaven. Hovedgrunnen til at dette ble gjort sent i prosessen var at det ikke ble funnet tilstrekkelig med spesifikk informasjon om dette i dokumentanalysen. Spørsmålene i intervjuene er forsøkt å være så åpne som mulige innenfor det området som var ønsket belyst. Det at spørsmålene var åpne førte til at det under intervjuene ble fremkom andre

momenter som var av stor relevans for oppgaven, uten jeg var klar over disse på forhånd. Dette gjorde intervjuene fyldigere enn først tenkt. Ideelt sett burde flere personer blitt intervjuet. Det var sannsynligvis mulighet for å gjøre intervjuer i mange av de møtene jeg deltok på, men på grunn av manglende kunnskap om feltet, så ble det en barriere å gjøre dette før kunnskapen var så god at jeg kunne stille relevante spørsmål. Det må tas høyde for at kontakten med fagpersoner med sterke meninger om problemstillinger i sikkerhetsfagfeltet har påvirket den objektiviteten man burde ha i en oppgave. På den andre siden har dette vært nødvendig for å forstå hvor utfordringene som ligger og det har bidratt til en dypere forståelse enn det ellers ville vært. De kriminologiske teoriene i oppgaven er valgt fordi dette er noe av den teoretiske forankringen i NS 5832.

Datainnsamlingen i stor grad baserer seg på dokumenter utarbeidet av myndigheter, offentlige rapporter og samtaler med fagpersoner i sikkerhetsfagfeltet. Det at det er brukt sekundærdokumenter og at det refereres i oppgaven til sidetall oppgaven, fører til at litteraturen i oppgaven er lett tilgjengelig. Grunnen til at det enkelte steder ikke refereres med sidetall er at dataen er hentet fra artikler på internett som ikke har sidetall. Det fagfeltet oppgaven søker å kartlegge er i stadig utvikling. Oppgaven kan på ingen måte generaliseres, men det lett tilgjengelig å finne litteraturen i oppgaven, da det konsekvent er referert med sidetall.

4. Empiri og drøfting

I dette kapittelet presenteres empirien og funnene som er gjort i relevant litteratur og intervjuer. Det er valgt å bruke forskningsspørsmålene som overskrifter, slik at man kan knytte teorikapitlene opp mot empirikapitlene. Denne oppgaven tar utgangspunkt i NS 5832 når fremgangsmåten for sikring av virksomhet gjennomgås. De ni sikkerhetsrådene i veiledning for terrorsikring vil fungere som et bakteppe i presentasjonen av empirien og drøftingen av denne.

4.1 Hva er sikkerhet og risiko i en sikringskontekst?

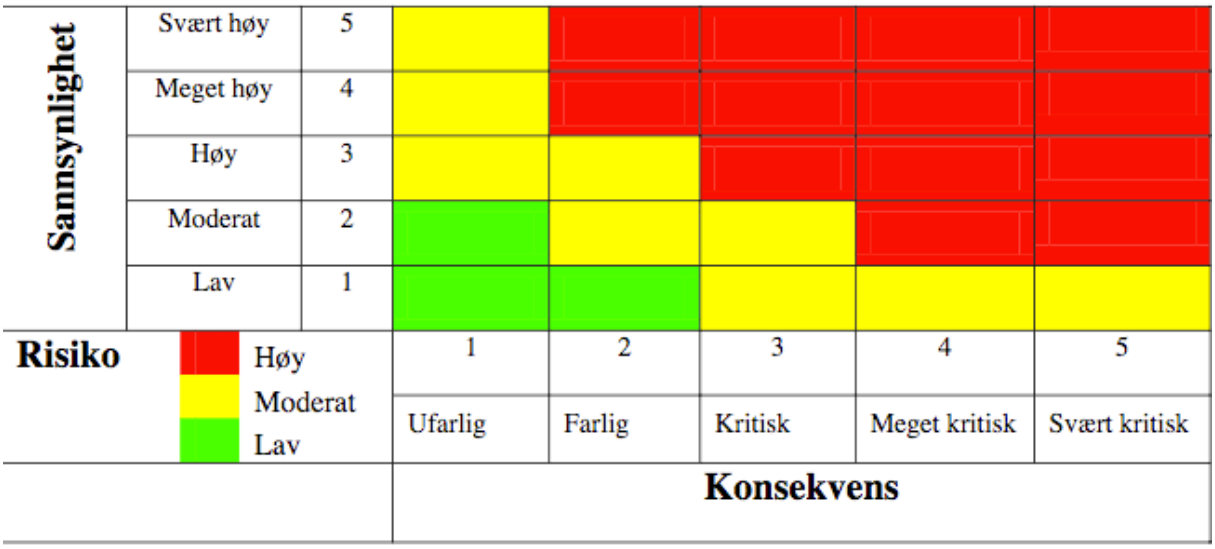
4.1.1 Sikkerhet og risiko

Sikkerhet er definert i NS 583X-serien som ”*reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare*”. Denne definisjonen stammer fra samfunnsvitenskapelig akademia og har sitt utspring i den originale latinske betydningen “frihet fra bekymring, frykt angst, og fare…”. I følge Joakim Barane er sikkerhet en reell eller oppfattet tilstand. Sikkerhet er altså en tilstand der man er, eller føler at man er trygg (FFI, 2015:120). Aven mener at en slik definisjon gjør det umulig å prate om ”graden av sikkerhet”, man kan kun si om noe er sikkert eller ikke (FFI, 2015:94). Begrepet ”sikkerhet” knyttes til forebyggende tiltak som har til hensikt å redusere sannsynligheten for at noe uønsket skal skje eller redusere konsekvensene ved uønskede hendelser. Videre kan sikkerhet være den evne et system har til å unngå skader og tap (Aven, et. al. 2004:17). ”Sikring” er bruk av sikringstiltak ved håndtering av risiko forbundet med tilsiktede uønskede handlinger (NS 5830:2).

I følge Manunta må man se sikkerhet i lys av konteksten rundt sikkerheten, fordi omstendighetene påvirker sikkerhetsfaktorene verdi, beskytter og trussel. Det er mange sikkerhetskontekster som spiller inn på sikring. Økonomisk, matematisk, psykologisk, sosiologisk, kriminologisk, juridisk, statlig og politisk sikkerhetskontekster. Når man snakker om sikkerhet i forhold til sikring av virksomhet, kan man ikke plassere sikkerhet i én av disse kontekstene. Sikkerhetsbegrepet i en sikringskontekst forstås ulikt av de mange aktørene som er involvert i sikringsprosessen. Hvis man for eksempel tenker på økonomisk sikkerhet, vil sikkerhet handle om at man ikke skal tape penger på eller gå i økonomisk underskudd som følge av ressursbruk på sikringstiltak. Hvordan man forstår sikkerhet påvirker hvilken

sikkerhetsmetodikk som anvendes, enten det er økonomi eller risikoanalyser (Manunta, 1997). Ledere og risikoanalytikere kan ha forskjellige oppfatninger om hva som er sikkerhet når det kommer til sikring. En risikoanalytiker kan mene at sikkerhet i forhold til sikring er tiltak som reduserer muligheten for at en TUH kan intreffe, eller konsekvensene av en TUH. En leder vil kanskje heller fokusere på det økonomiske aspektet ved sikkerhet, kostnad og nytte. Sikkerhet og risiko er to sider av samme sak. Der man har fullstendig sikkerhet finnes det ikke risiko, og der man har risiko finnes ikke fullstendig sikkerhet. I følge Stranden er det viktig å vite at en risikotilnærming til sikkerhet kun er én av flere måter for å oppnå sikkerhet, og sikkerhet er bare en av flere strategier for å håndtere risiko (FFI, 2015:130).

Barane påpeker at det er en klar forskjell på den teknisk-nautrvitenskapelige tilnærmingen til risiko som NS 5814 er basert på, og den samfunnsvitenskapelige/kriminologiske tilnærmingen NS 5832 er basert på (FFI, 2015:117). I NS 5814 defineres risiko som «uttrykk for kombinasjonen av sannsynligheten for og konsekvensene av en uønsket hendelse» (Rausand og Utne, 2009:22). NS 5832 bruker ikke sannsynlighetsbegrepet i definisjonen av risiko, og risiko defineres i NS 5832 som «*uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen*» (NS 5830:5). I NS 5832 brukes betegneslen ”ren risiko”, som betyr at risikoen kun inneholder potensialet for tap og ingen mulighet for gevinst. En annen risikobetegnelse er ”spekulativ risiko”, som er risiko der det er et potensiale for gevinst. Dette kan for eksempel være økt fortjeneste eller bedre evne til å levere varer og tjenester mer kostnadseffektivt (NS 5831:3). Risiko har derfor to sider. Ren risiko der potensialet kun er tap, og spekulativ risiko som kan føre til gevinst (Stranden). NS 5814 og NS 5832 fremstiller også risiko forskjellig. I NS 5814 fremstilles risikoen i en risikomatrise med sannsynlighet og konsekvens. NS 5832 fremstiller ikke risikoen visuelt, men som tekst i sikringsrisikoanalysen. Figuren nedenfor er risikomatrisen som brukes til å fremstille risiko etter NS 5814:

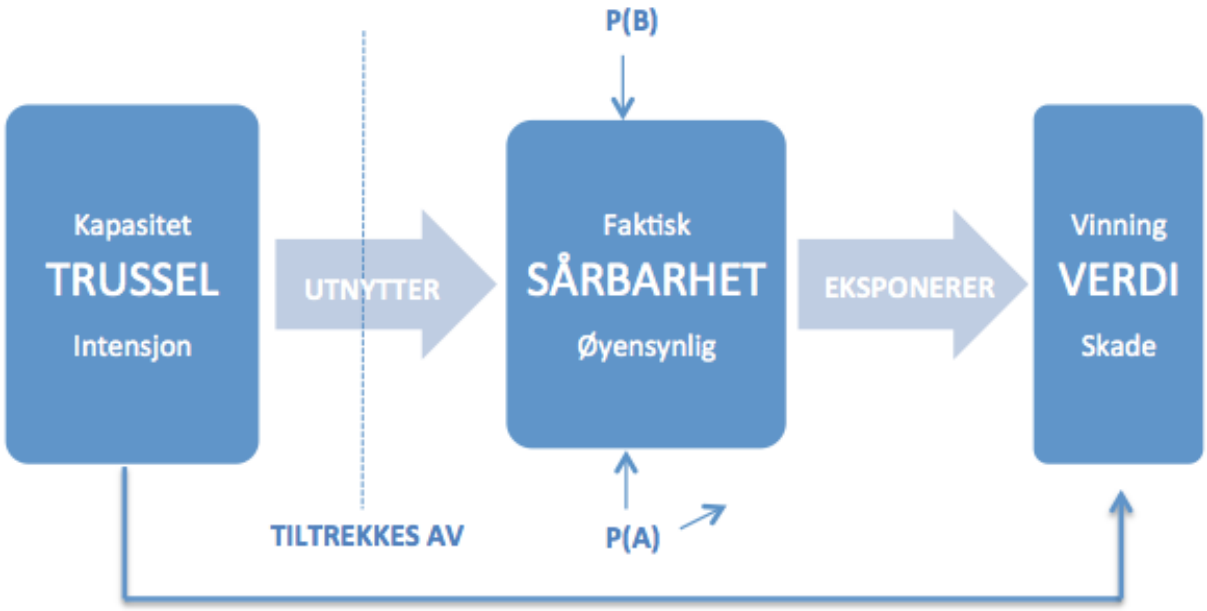


Figur 3 Risikomatrise for bestemmelse av risiko ut i fra tallverdier for konsekvens og sannsynlighet i NS 5814 (FFI, 2015:31).

Hendelser som plasseres i grønt område betegnes som "lav risiko", gult område som "middels risiko" og rødt område som "høy risiko". Det er hendelsene i gult område i figur 3 som betegnes som ALARP. Her må risiko reduseres, såfremt det ikke er urimelige misforhold mellom kostnad og sikringstiltakets nytte (Aven, 2007:118). Risikoen i NS 5814 beregnes gjennom en tradisjonell teknisk-naturvitenskapelig tilnærming, der sannsynligheten er frekvensbasert og kan tallfestet. Tallfesting av sannsynlighet kan for eksempel være at man sier at det er mellom 60 og 90 prosent sannsynlighet for at en terrorhandling vil skje i løpet av et år. I den engelske forståelsen av sannsynlighetsbegrepet benytter man seg av to ord: "probability" og "likelihood". Disse begrepene har forskjellig betydning i motsetning til det norske sannsynlighetsbegrepet. I norsk kontekst forstås probability som en frekvensbasert sannsynlighet, mens likelihood forstås som muligheten for at noe kan skje (FFI, 2015:16). NS 5814 baserer seg på "probability" og NS 5832 baserer seg på "likelihood".

Når man skal forklare risiko som forholdet mellom trussel mot verdi og verdiens sårbarhet overfor trusselen i henhold til NS 5832, kan man se til modellen nedenfor som er utarbeidet av Morten Bremer Mærli. Her er P(A) sannsynligheten for at et angrep skjer og P (B) er sannsynlighet for barrierebrudd gitt at et angrep har skjedd. P(A) er det vanskelig å si noe om fordi det er angriperen som "eier" denne sannsynligheten selv, og bestemmer når, hvor og hvordan et angrep skal skje. P(B) handler om sannsynligheten for et barrierebrudd gitt at man

utsettes for et angrep. Ved en grundig sikringsrisikoanalyse kan man si noe om muligheten for at barrierebruddet skjer ved å avdekke de sårbarhetene en verdi har i forhold til trusselen (Mærli, 2015).



Figur 4: Modell som viser risiko som en trussel som utnytter en sårbarhet som eksponerer en verdi, utviklet av Mærli.

I denne figuren forstås sårbarhet som forhold som reduserer eller begrenser evnen til å motstå aksjoner mot verdier, og trusselen bestemmes av verdiens egenskap kombinert med trusselaktørenes kapasitet og intensjon om å gjøre anslag mot verdien (Mærli, 2012). Risiko kan reduseres ved å minske verdien, noe som vil føre til mindre sikringskostnader. Videre kan risiko reduseres ved overvåkning av miljøet rundt verdiene som skal beskyttes for å identifisere trusler. Til sist, kan sårbarhetene som virksomhetene eier reduseres og utbedres (Mærli, 2012).

Det har lenge pågått en debatt om hvilken av de to standardene som passer best mot TUH. Det må understrekes at NS 5814 brukes til å si noe om risiko for både TUH og utilsiktede uønskede hendelser. Uenigheten handler i hovedsak om hvordan man forstår risiko, og her spiller sannsynlighet en sentral rolle. Aven mener at sannsynlighet er mer enn bare én ting, og at det er fundamentale forskjeller mellom "frekvensbasert sannsynlighet" og "kunnskapsbasert sannsynlighet". Den kunnskapsbaserte sannsynligheten uttrykker usikkerhet

og analytikers grad av tro, og er ikke det samme som frekvensbasert sannsynlighet. I følge Aven er det er viktig å kunne si noe om graden av kunnskap som sannsynlighetsberegningen baserer seg på (FFI, 2015:93). I følge Røed "*bruker man sannsynlighet for å få frem et poeng*". Han sier videre at PST brukte sannsynlighet i en pressekonferanse (FFI, 2015:99). Haneborg påpeker at årsaken til at PST brukte sannsynlighet i pressekonferansen, var at et gradert dokument var lekket. Haneborg sier at man bruker sannsynlighet i etterretningsgrunnlaget, men at man da snakker om "likelihood" – altså "muligheten for". Sannsynligheten sier ikke noe om "*hvor, når eller hvordan"*, når man snakker om at det er 60-90 prosent sannsynlighet for at et terrorangrep skjer i Norge ila ett år. Videre mener Haneborg at de store nasjonale sannsynlighetsberegningene for om en TUH vil inntreffe eller ikke, spiller liten rolle for virksomheter som er opptatt av om en TUH kan skje i "her i denne virksomheten" (FFI, 2015:107).

Under paneldebatten i FFI-forum "Må bli bedre på å kommunisere risiko", stilte Mærli et spørsmål til panelet om hva "kunnskapsbasert sannsynlighet" innebærer. Panelets svar var at kunnskapsbasert sannsynlighet henviser til alle former for sannsynlighet. Altså sannsynligheten for at man lykkes i et angrep, men også sannsynligheten for at en hendelse vil inntreffe hvis man velger sannsynlighet som en egen parameter. Men det kunnskapsbasert sannsynlighet faktisk betyr, er at man benytter ulike typer fagfolk. Disse bruker sin kunnskap fordi de har god kjennskap til trusselen eller verdiene objektet besitter. Deretter vil de samlet komme frem til en type angivelse av sannsynlighet. Man bruker ikke nødvendigvis en frekvensbasert sannsynlighet, men en sannsynlighet som er basert på den kunnskapen man besitter. Dette viser at det er noe subjektivt over angivelsen av sannsynlighet svarer panelet (FFI-forum, 2015). Mærli mener at hovedproblemet med kunnskapsbasert sannsynlighet er at den verken definerer hvilken type sannsynlighet man snakker om, eller skiller mellom to former for sannsynlighet som alltid er tilstede ved et angrep: P(A) – sannsynligheten for at et gitt mål blir angrepet og P(B) – sannsynligheten for barrierebrudd, gitt et angrep (mot et mål). P(A) er det angriperne som eier, for det er de som bestemmer hva som skal angripes, hvordan og hvorfor. P(B) eier objekteieren, og denne sannsynligheten er omvendt proposjonal med investeringen i sikringstiltak. Med kunnskapsbasert sannsynlighet slås P(A) og P(B) sammen, og det er dette eksperter sammen skal finne ut av. Dette betyr at de tar på seg å vurdere hvorvidt et gitt objekt vil bli angrepet P(A), noe som med andre ord er en indirekte

trusselvurdering. Det er PST som det må være opp til å komme med slike antakelser, og det bør være opp til ledelsen å bestemme risikoaksept og sikringsmål ut i fra hvilke trusselaktører med tilhørende kapasiteter som sikringstiltakene skal stanse (Mærli, epost, 2016).

I følge Haneborg ”eier” DSB samfunnsrisikoen og den tradisjonelle risikotankegangen med sannsynlighet og konsekvens som NS 5814 er tuftet på (FFI, 2015:102). Videre mener Haneborg at selv om DSB ikke bruker frekvens, så presenterer de tall og prosenter på sannsynlighet (FFI, 2015:105). I rapporten ”Nasjonalt Risikobilde” definerer DSB sannsynlighet som hvor trolig det er at en hendelse skal inntreffe (likelihood), og det brukes et tidsintervall som mål på dette. Hvis sannsynlighet brukes uten en angivelse av tid, vil risikovurderingen i følge Midtgaard, fungere som et øyeblikksbilde. Dette gjør det mer krevende å si noe om en hendelse skal inntreffe. Midtgaard sier at ”*DSB er nøye på at man ikke sier at det skjer én gang hvert 300 år, men én gang i løpet av 300 år*” (FFI, 2015:108). Årsaken til at tidsintervaller brukes er for å konkretisere eller tallfeste sannsynligheten for at en hendelse kalt X kan skje i løpet av 100 år, mens hendelse Y kan skje i løpet av 1000 år. Midtgaard mener at man da kan si at hendelse X er mer sannsynlig enn Y. DSB sier ikke at de ”anslår” sannsynlighet, men at de ”angir” den. DSB er også eksplitte på å beskrive usikkerhet i veiledere de gir ut. En trusselvurdering kan endre seg raskere enn en risikovurdering, fordi verdier og sårbarheter holder seg mer stabile enn trusler. Midtgaard anbefaler at man utvider tidshorisonten med noen år eller tiår (FFI, 2015:108). I følge Stranden er det umulig å si noe om en hendelse vil ramme en virksomhet eller ikke, men man kan si noe om hva som skjer hvis man blir rammet (FFI, 2015:130). Barane mener at sårbarhetsvurderingen vil si noe om sannsynligheten for at en angriper lykkes gitt et angrep. Barane stiller seg kritisk til at det angis sannsynlighet for at en bestemt virksomhet blir utsatt for en TUH. Man må være klar over at 99 prosent av alle risikoanalyser gjennomføres på virksomhetsnivå. Ledere er som regel mest interessert i å vite sannsynligheten for angrep mot egen virksomhet. De er mindre opptatte av den totale samfunnsrisikoen. (FFI, 2015:119).

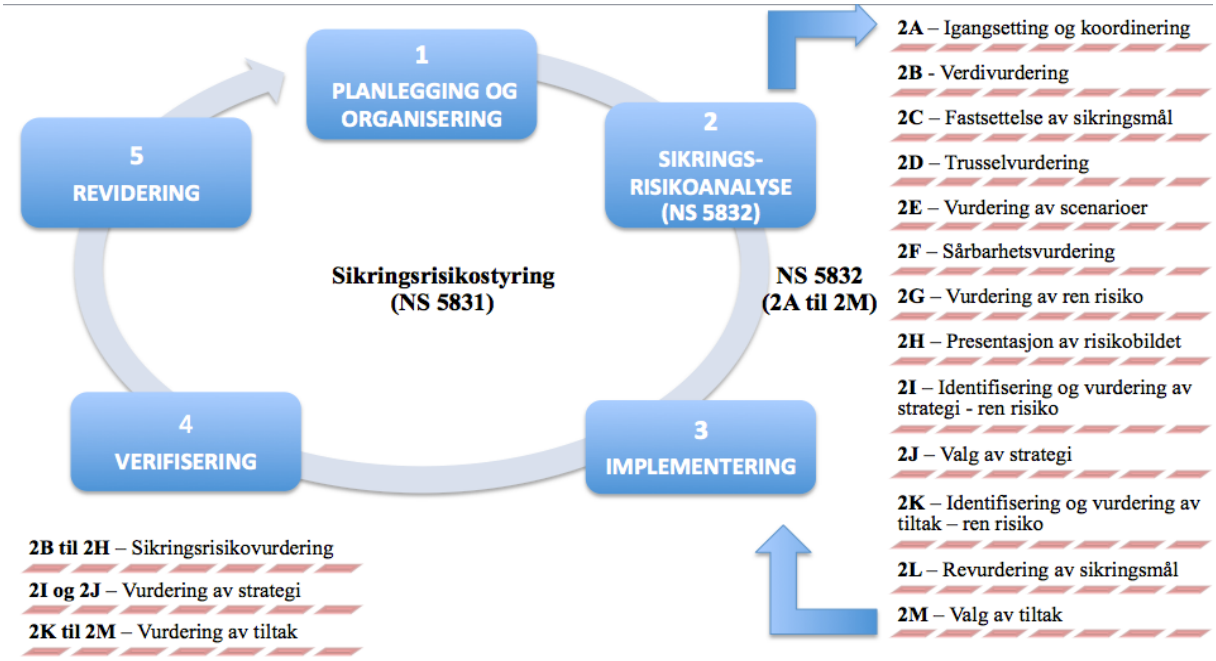
Når DSB velger å angi et tidsintervall, for eksempel at en terrorhandling skjer i løpet av “300 år”, kan man spørre seg i hvilken grad dette er interessant for en “vanlig virksomhet”. Midtgaard tenker at det ville være lettere å utvide tidshorisonten for en risikovurdering, da trusselbildet endrer seg raskt, og verdier og sårbarheter er mer stabile. “Et trusselbilde er et

øyeblikksbilde" sier Midtgaard. Er det slik å forstå at et trusselbilde ikke er et øyeblikksbilde hvis man utvider tidshorisonten i risikovurderingen? Spørsmålet blir videre hva som blir forskjellen på å utvide tidshorisonten for en risikovurdering, og det å oppdatere trusselvurderingen i takt med endringer i trusselbildet. Hvis man allerede har en systematisk og grundig utført sikringsrisikoanalyse, så vil oppdatering av trusselbildet bli mindre omfattende sier Mærli (Mærli, epost, 2016). Kan det tenkes at ved å oppdatere trusselvurderingen i en sikringsrisikoanalsye, så vil man i det minste ha et mer presist "øyeblikksbilde" for hver gang man gjør dette, i motsetning til å "modifisere" ett øyeblikksbilde til å skulle vare over en lengre tidshorisont.

Til syvende og sist er det valgfritt hvilken tilnærming og risikoforståelse man vil bruke mot tilsiktede uønskede handlinger. Et problem ved at NS 5832 ikke bruker begrepet sannsynlighet, er at hendelser som ledere oppfatter som lite sannsynlige, kan bli beregnet som høy risiko i NS 5832 (IP-1). Hvis verdier har store sårbarheter og konsekvensene av et mulig scenario er store, kan risikoen for hendelsen bli beregnet til å være høy. For ledere med begrenset risikoforståelse, vil dette kunne fremstå som ulogisk, og motviljen til å bruke ressurser på sikringstiltak mot slike hendelser blir større.

4.2 Hvordan foregår sikring i dag?

Det er i oppgaven valgt å ha med sikringsrisikostyringsmodellen som er basert på NS 5832, og er publisert i "Veileder for terrorsikring" (2015). Årsaken til dette er at figuren kan fungere som et bakteppe for å visualisere hvilke steg sikringsrisikostyringsprosessen består av. Nederst i venstre hjørne av figuren ser man at NS 5832 er delt inn i tre prosesser: 1) sikringsrisikovurdering, 2) vurdering av strategi, og 3) vurdering av tiltak.



Figur 5: Sikringsrisikostyringsmodellen (NS 583X-serien) fra "Veileder i terrorsikring" (PST, et. al. 2015:15).

4.2.1 Sikkerhet er et lederansvar

"Sikkerhet er et lederansvar" er sikkerhetsråd nr. 1 i "Veileder for terrorsikring" (2015). Det er viktig at virksomhetens leder er oppdatert på risikobildet og har kjennskap til hvilke tiltak som skal iverksettes for å redusere risikoen. Det er tre essensielle prinsipper som må være tilstede for å oppnå god sikringsrisikostyring:

1. ***Forankring*** hos virksomhetens ledelse. Ledelsen må sette sikkerhetsmål, bevilge nødvendige ressurser og evaluere sikkerhetstilstanden årlig.
2. ***Forpliktelse*** til å utvikle klare retningslinjer og klare føringer for sikkerhetsarbeidet. Ansvar må fordeles for å ivareta at oppgaver gjennomføres og sikkerhetsarbeidet må dokumenteres.
3. ***Forståelse*** av sikkerhet på alle nivåer i virksomheten. Dette må gjøres gjennom kompetanseheving, bevisstgjøring, motivere slik at forståelsen for sikkerhetsarbeidet øker (Sikkerhetsstyring, 2015:3).

Informant 1 (IP-1) opplever at det i mange tilfeller er vanskelig å få en styringsgruppe eller ledere til å engasjere seg og få eierskap til sikringsprosessen, særlig når det gjelder deltakelse i sikringsrisikoanalyser. Det er ofte driftsavdelingen som har tatt initiativet til å gjennomføre

sikringsrisikoanalysen, og så skriver lederne raskt under på noe uten å ha satt seg nøye inn i resultater og sikkerhetstråd. Prosessen stopper opp hvis man ikke får involvert lederne. Hvis ikke toppledelsen involverer seg, får de heller ikke den forståelsen som er nødvendig for å ta så optimale beslutninger som mulig. Ip-1 håper at man om noen år har kommet dit at lederne forstår hvor viktig det er å engasjere seg. Per nå er det virksomheter som er veldig dyktige med sikkerhet hvis initiativet kommer fra ledelsen, men hvis selve involveringen mangler, kan sikringsrisikoanalysen bli forankret på et for lavt nivå i virksomheten, og da har man i følge IP-1 et problem (IP-1).

I følge Informant 2 (IP-2) er det veldig varierende om ledere er involvert i prosessen eller ikke, og det går ofte på hva slags viksomhet det er snakk om. I følge IP-2 er noen av de mindre virksomhetene overraskende oppdatert og ”fremme i skoene” når det kommer til sikkerhetsarbeid og sikringstiltak. Årsaken er at det er lettere i mindre virksomheter, fordi beslutningsveien ikke er så lang. Det er ikke langt opp til ledelsen som kan vurdere om man skal bruke midler, og det er dermed lettere å få gjennomført sikringstiltak. Hvis ledelsen er opptatt av sikkerhet, så ligger forholdene til rette for god sikring av virksomheten. På den annen side, har mindre virksomheter ofte ikke så store verdier, og de økonomiske konsekvensene av å investere i sikringstiltak blir ikke så store som i de større virksomhetene (IP-2). En av de største utfordringene er at mange føler at det er en veldig stor ”treghet i systemet” helt fra toppen. IP-2 sier at hvis man for eksempel ser i Sikkerhetsloven, så er objektsikkerhetsforskriften tatt inn ganske tidlig, der det blant annet står om bilsperrer og pullerter. Hadde objektsikkerhetsforskriften blitt fulgt, så hadde ikke bombebilen den 22. juli hatt mulighet til å stå der den stod. Det er en form for innebygd treghet i Staten på veldig mange måter, og her spiller økonomi en sentral rolle, sier IP-2.

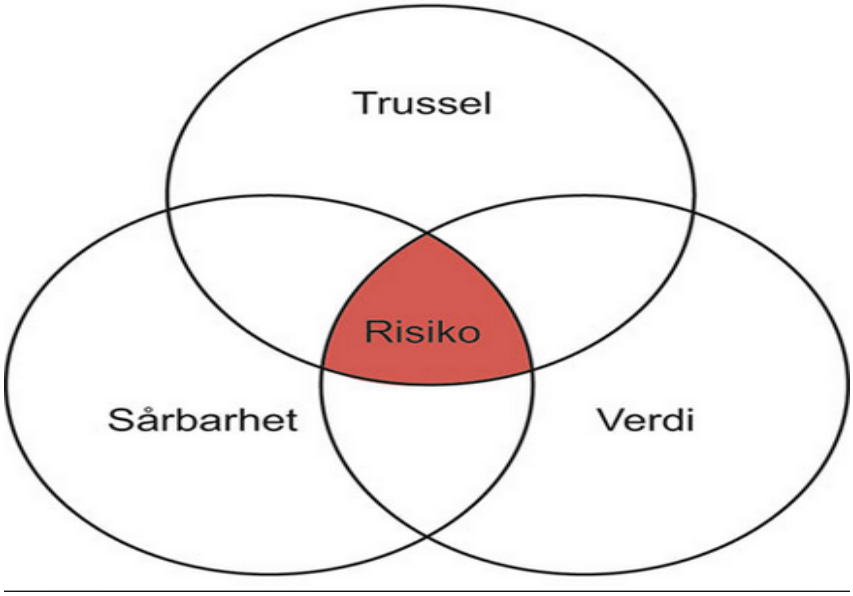
I FFI-forums paneldebatt ”Må bli bedre på å kommunisere risiko” sier Leif D. Riis, avdelingsleder for analyse og sikring i Forsvarsbygg, at sikring er et ledelseansvar, og det er virksomhetens leder som er ansvarlig for at det er tilstrekkelig god sikkerhet i virksomheten. Riis sier av egen erfaring at hvis ikke de som jobber med sikkerhet får engasjert toppledelsen, kommer det ikke til å skje veldig mye innenfor sikkerhetsområde (FFI-forum, 2015). For å få et godt resultat, må security inn i virksomhetens mål. Dette medfører at ledelsen også vil bli målt på dette punktet (FFI, 2015:115).

4.2.2 Sikringsrisikoanalyse

I arbeidsgruppen som utarbeidet NS 5831 og NS 5832, var det representanter fra NSM, PST, NSR, Standard Norge, Statoil og Forsvarsbygg (FFI, 2015:102). Sikkerhetsråd nr. 2 i VT (2015) er at det skal gjennomføres en sikringsrisikoanalyse av virksomheten. Sikringringsrisikoanalysen NS 5832 består av tre faser: 1) sikringsrisikovurdering, 2) vurdering av strategi, og 3) vurdering av tiltak. Når man skal vurdere risiko mot TUH, kan det være nyttig å beskrive risiko som en funksjon av verdi, trussel og sårbarhet. Dette gjør NS 5832, og denne omtales derfor som «trefaktormodellen». Faktorene verdi, trussel og sårbarhet er i NS 5832 definert som:

- Trussel: *«mulig uønsket handling som kan gi negative konsekvens for en entitets sikkerhet»* (NS 5832:2014:4).
- Verdi: *«ressurs som hvis den blir utsatt for en uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen»* (NS 5832:2014:4).
- Sårbarhet: *«manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for en uønsket påvirkning»* (NS 5832:2014:5)

Risiko er i NS 5832 et uttrykk for forholdet mellom trusselen (T) mot en gitt verdi (V) og denne verdiens sårbarhet (S) overfor den spesifiserte trusselen:



Figur 6: Trefaktormodellen (NOU:2012:14).

Figur 6 viser hvordan verdi, trussel og sårbarhet utgjør risiko i NS 5832. Det er ikke nødvendigvis slik at det er likevekt mellom trussel, verdi og sårbarhet. Trusselbildet er ofte i større grad utenfor utenfor virksomhetens kontroll, og det fører til at virksomheten må fokusere mer på egne sårbarheter og verdier (Sikkerhetsstyring, 2015:12). NS 5832 er ikke tiltenkt å erstatte andre standarder for risikoanalyse, men den er ment å være et alternativ til disse, da den særlig ivaretar risiko mot TUH. Omfanget av analysen vil variere i forhold til analyseobjektets karakter, tid og ressurser. Målgruppen for standarden er analytikere som har tilgang til data og informasjon, samt har tilstrekkelig tid og kompetanse til å gjennomføre trinnene i analysen. NS 5832 er i hovedsak kvalitative vurderinger, men frekvensbasert tallmateriale kan brukes som et supplement til kvalitative vurderinger (NS 5832:1). Vurdering av muligheten for gevinst er ikke tatt med i NS 5832. I en helhetlig vurdering bør muligheten for gevinst og muligheten for tap vurderes sammen, noe man kaller spekulativ risiko (NS 5832:2). I følge IP-1 er det lagt inn en økonomivurdering midt i NS 5832 for å synliggjøre at sikkerhet koster, men at hvis man ser det i lys av et livsløpsperspektiv og driftkostnadsmessig, vil man spare inn det sikkerheten i utgangspunktet kostet.

IP-2 jobber i hovedsak med å tilby og implementere fysiske sikringstiltak for virksomheter og mottar derfor risikoanalyser som er utarbeidet av virksomheten selv eller et konsulentselskap på vegne av virksomheten. Disse risikoanalysene skal gi IP-2 grunnlag for å kunne rådgi og

implementere riktige sikringstiltak for virksomheten. Konsulentselskapene som utfører risikoanalyse for virksomheter har ofte plikt til å gjennomføre en fullstendig risikoanalyse, og denne blir ofte veldig stor og omfattende. Når IP-2 mottar en risikoanalyse med mange verdier, blir det vanskelig og uoversiktlig å ha helt klart for seg hvilke verdier som er viktigst å sikre. Innenfor IP-2 sitt arbeidsfelt passer NS 5832 best når man skal jobbe med ren security, da NS 5814 blir for omfattende og inneholder mye som er lite relevant for for IP-2 sine arbeidsoppgaver. Safety pleier som regel alltid å bli prioritert foran security, da det blant annet er et stort fokus på brannfare og brannforskrifter. Om man bare kunne tenke security, ville oppgaven blitt enklere. Men i og med at safety ofte prioriteres først blir dette mer krevende. Selv en risikoanalyse etter NS 5832 kan bli for omfattende, og IP-2 savner mindre omfattende og mer konkrete risikoanalyser. På denne måten blir lettere å se hvilke verdier som er viktigst å sikre. Da blir det enklere å gi råd om effektive og riktige sikringstiltak til virksomheten. Satt på spissen, kunne man ønske seg én risikoanalyse per verdi i en virksomhet. IP-2 mener at kvaliteten på risikoanalysen blir bedre dersom man fokuserer på de verdiene som er viktigst for virksomheten.

I følge Mærli, har virksomheter ofte manglende oversikt over de verdier som har behov for sikring. Dette er et dårlig utgangspunkt for sikring, og det blir vanskeligere å identifisere sårbarhetene (Mærli, 2012:6). Hvis man skal følge NS 5832 prosessen, blir det i følge Ip-1 en rigid øvelse som krever mange arbeidstimer. Enkelte ser på prosessen som en enkel, nesten skjematisk utfylling, mens andre ser prosessen som svært krevende hvis man skal gjøre den grundig. Det er viktig å tenke på i hvilken kontekst NS 5832 skal brukes i hvert enkelt tilfelle. Bruken må tilpasses virksomhetens behov (IP-1). Gjennomføringen av NS 5832 skal uansett være stegvis, logisk og transparent (Mærli, epost, 2016). Thomas Haneborg sier at NS 5832 har et stort fokus på verdier, og mener også at en grundig verdivurdering kan tydeliggjøre hva som bør sikres og hva som ikke trenger sikring. *"Da er det enklere som objekteier å prioritere hva du skal investere i av sikringstiltak, slik at man kan bedre styre risikoen"*. Det at verdieeieren bidrar i verdivurderingen er essensielt, da utenforstående ikke får like god systemforståelse som verdieier selv (FFI, 2015:103-105).

Teoriene "Situasjonell kriminalitetsforebygging" (SCP) og "Rutineaktivitetsteorien" fokuserer begge på at man skal redusere muligheten for at en kriminell handling kan skje. Det

fremgår i kriminalitetstriangelet at tre betingelser må være tilstede for at en kriminell handling kan gjennomføres: 1) en motivert gjerningspersonen, 2) fravær av kapable beskyttere og et 3) passende mål. Hvis man kobler dette kriminalitetstriangelet mot NS 5832, kan man si at en motivert gjerningsperson er trusselen, et passende mål er verdien og fravær av kapabel beskytter er sårbarheten. Hvordan skal man kunne redusere muligheten for at de tre betingelsene er tilstede samtidig? Hvis man kun skal fokusere på gjerningspersonen, blir dette vanskelig. Når, hvor og hvordan en gjerningsperson bestemmer seg for å utføre en kriminell handling er usikkert. PSTs bekymringssamtaler med personer de mener er i ferd med, eller som allerede er blitt radikalisert, kan være et tiltak som søker å redusere en potensiell gjerningspersons motiv for en kriminell handling. På den andre siden fordrer en slik bekymringssamtale at PST har informasjon om at denne personen kan utgjøre en form for trussel. Slik informasjon foreligger ofte ikke. Haneborg mener at det i trusselvurderingen er viktig å si ”jeg bryr meg ikke om hvem som utfører handlingen eller hva som er motivasjonen deres”. Man må se på handlemåten og kapasitetene en trusselaktørene har, og hvordan trusselaktøren kan nå målet (FFI, 2015:106). Det er begrenset hva man kan gjøre for å redusere motivasjonen til en potensiell gjerningsperson, hvis man ser bort i fra hvilken effekt manipulering av beskyttere og målet vil kunne ha. Rutineaktivitetsteorien tar for gitt at det er en motivert gjerningsperson tilstede, og videre at det er beskytter og mål man bør gjøre noe med. Muligheten for en kriminell handling kan reduseres enten ved å se til at man har kapable beskyttere og/eller gjøre målet mindre attraktivt.

Situasjonell kriminalitetsforebygging (SCP) er strategier for å gjøre kriminalitet vanskeligere å gjennomføre-, mer risikofylt- og mindre gunstig for en gjerningsperson. Det handler om å være i forkant, ved å ha tiltak på plass som kan avskrekke eller hindre en gjerningsmann. Tiltakene kan være alt fra fysiske sikringstiltak til opplæring av ansatte i sikkerhetsrutiner. Sikringstiltak som fungerer i et område mot én kriminalitetskategori, vil kanskje ikke fungere på samme måte et annet sted. NS 5832 bruker scenarioer for å identifisere verdiers sårbarheter overfor trusler. Ved å bruke scenarioer i trusselvurderingen, legger man til en tenkt ”situasjonell kontekst” som bidrar til å kartlegge hvordan omstendighetene påvirker verdi, trussel og sårbarhet i virksomheten, og dermed har man bedre forutsetninger for å tilpasse sikringstiltak til virksomhetens behov.

To like hus i samme boligfelt kan for eksempel ha forskjellig sikringsbehov mot innbrudd.

Det ene huset har en slik beliggenhet at naboer og forbipasserende har innsyn på tomten og huset forøvrig. Det andre huset ligger mer skjult til med høye hekker. Man kan først tenke at huset som ligger åpent og tilgjengelig er mest utsatt for innbrudd, da det andre huset ikke synes fra veien og at det dermed er mindre sjanse for at huset blir betraktet som et mål. Hvis man kobler omstendighetene rundt husene med modusen til potensielle innbruddstyver, så viser det seg at hus som ligger isolert er et mer attraktivt mål for innbruddstyver fordi det er mindre sjanse for å bli oppdaget, og dermed mer spillerom til å gjennomføre handlingen. Huset som ligger skjult er ikke gjenstand for "menneskelig overvåkning" (naboer og forbipasserende) slik som det andre huset er, og burde også med det ha behov for bedre sikring. To like hus, men forskjellig sikringsbehov på grunn av de situasjonelle omstendighetene rundt hver av dem. Det å bruke scenarioer i NS 5832 og trusselvurderingen kan kobles til Manuntas operasjonelle definisjon av sikkerhet, der (Si) brukes for å forstå sikkerheten til virksomheten i lys av hvordan situasjon og omstendigheter rundt påvirker trusler, og virksomhetens verdi og sårbarhet. Prinsippene i rutineaktivitetsteorien og SCP er gjennomgående i NS 5832. Rutineaktivitetsteorien tar for gitt at det er en motivert gjerningsperson, og for å unngå muligheten for at en kriminell handling kan inntreffe, må verdiene være tilstrekkelig beskyttet. For å vite hva man skal beskytte er identifisering av verdier essensielt. Ved bruk av scenarioer får man vurdert verdienes sårbarheter i forhold til truslene, og man har med dette muligheten til å iverksette tiltak for å redusere sårbarhetene. Bruk av scenarioer vil aldri være "vantette", da det er umulig å si når, hva, hvordan og hvorfor, men det er det beste kortet man har.

4.2.3 Sikringsrisikovurdering

Det er tre viktige vurderinger i sikringsrisikovurderingen: 1) verdivurdering, 2) sårbarhetsvurdering, og 3) trusselvurdering. Formålet med en verdivurdering er å kartlegge virksomhetens viktigste verdier. Verdien kan være materielle og ikke-materiell. Materielle verdier kan for eksempel være virksomhetens infrastruktur eller arbeidernes liv og helse, mens ikke-materielle verdier kan være virksomhetens omdømme og rykte. Kartleggingen må være systematisk og skal vurdere konsekvenser og negativ påvirkninger. Trusselvurderingen skal beskrive trusselaktørers intensjon og kapasitet, og dette skal skape et trusselbildet for de verdiene som man vil beskytte. NSM anbefaler at man deler truslene inn i terrorhandlinger, alvorlig kriminalitet, spionasje og sabotasje (NSM, 2016:14). Når verdivurderingen og

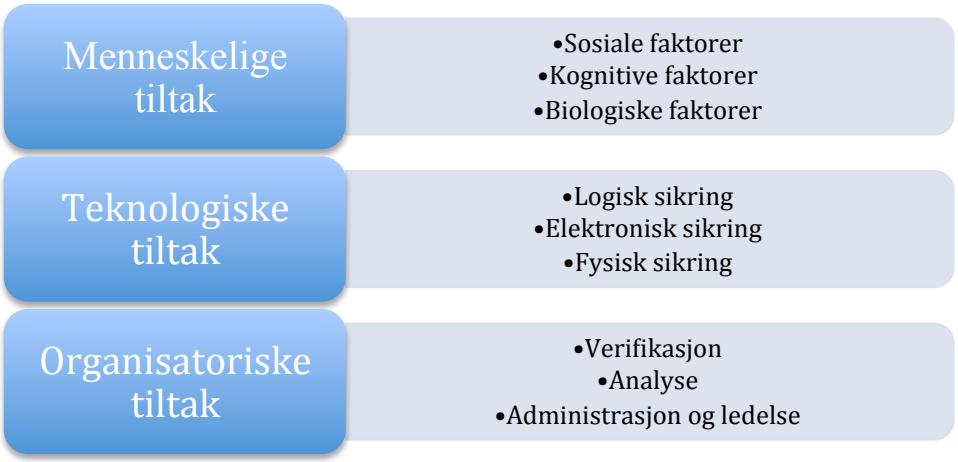
trusselvurderingen er gjort må mulige scenarioer identifiseres og velges. Scenarioene skal beskrive hvordan trusselaktører kan skade verdiene. Til sist har man sårbarhetsvurderingen som har til hensikt å identifisere forholdet mellom iverksatte sikringstiltak og trusselaktørers intensjon og kapasitet (NSM, 2016:19). Av alle norske virksomheter hadde 4 prosent innhentet PSTs åpne trusselvurdering, og av disse 4 prosentene var det 66 prosent av virksomhetene som som hadde brukt trusselvurderingen til å vurdere aktuelle trusler mot egen virksomhet. Av de virksomhetene som hadde vurdert aktuelle trusler mot egen virksomhet, iverksatte 59 prosent av dem tiltak (Krisno, 2015:11). Dette er interessante tall, fordi de virksomhetene som brukte den åpne trusselvurderingen til å vurdere seg selv, så ble det implementert sikringstiltak i 6 av 10 tilfeller. Som Mærli sier, trigger kjente risikoer sikringstiltak, eller i alle fall interesse for det (Mærli, 2012:6). Kan det tenkes at PSTs åpne trusselvurdering gir trusselen det "ansiktet" beslutningstakere trenger å se for å ville investere i sikringstiltak? Det blir kanskje lettere å rettferdiggjøre bruk av ressurser på sikringstiltak, hvis man har en oppfatning av hva man sikrer seg mot. Å velge scenarioer i en trusselvurdering er en vanskelig disiplin. PSTs trusselvurdering bidrar til å skape bevissthet om visse trusselaktører. Det er likevel viktig at de som utfører risikoanalyser for virksomheter har kompetanse og kunnskap til å være innovative når det kommer til generering av scenarioer og identifisering av trusseaktører. "Realistisk fantasi" kan brukes for å beskrive dette.

4.2.4 Strategier for å håndtere risiko

Etter en sikringsrisikovurdering må man velge en eller flere strategier for å redusere den identifiserte risikoen i virksomheten. Det finnes flere strategier for å håndtere srisiko. I sikringsrisikostyringsmodellen er vurdering av strategi satt til å være 2I – "Identifisering og vurdering av strategi – ren risiko" og 2J – "Valg av strategi". Håndtering av risiko er tiltak som gjennomføres for å oppnå akseptabel grad av identifisert risiko. Virksomheter står som regel overfor 4 strategier for å håndtere risiko. Virksomheten kan unnvike, overføre, akseptere eller redusere/fjerne risikoer. Det er viktig å vite at man også kan bekjempe risiko, men dette blir ofte oversett. Hvis strategien er å redusere eller fjerne ren risiko, bør tiltakene bestå av menneskelige, teknologiske og organisatoriske sikringstiltak (Stranden). Det er viktig at virksomheten tenker helhetlig ved sikring, og at sikringstiltakene er integrert i hverandre. Virksomheters grunnsikring bør være et system bestående av ulike barrierer, systemer for

deteksjon, verifikasjon og reaksjon (Mandt, 2015). Det er viktig at sikringstiltak som er testet og montert etter anerkjente standarder brukes. Sikringstiltak kan ha flere funksjoner:

- Virke avskrekkende slik at en potensiell angriper avstår fra å angripe eller velger et annet mål.
- Forsinke en angriper, noe som kan gi en mulighet til å varsle, trekke seg unna til et trygt sted, evakuere og gi en reaksjonsstyrke bedre forutsetninger til å håndtere situasjonen.
- Være med på å redusere konsekvensene av et angrep (Mandt, 2015).



Figur 7: MTO - sikringstiltak basert på "Risikovurdering for sikring" (NSM, 2016).

Menneskelige sikringstiltak er tiltak som påvirker persepsjonen, vurderingsevne, kunnskap, atferd og reell evne til å bruke teknologiske sikringstiltak og følge organisatoriske sikringstiltak. Sårbarheter ved menneskelige tiltak kan for eksempel være manglende sikkerhetsbevissthet i virksomheten og ansvarsfraskyving.

Organisatoriske sikringstiltak er tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, rutiner, adferd og/eller anvendelse av andre sikringstiltak. I det organisatoriske foreligger det mange potensielle sårbarheter. De vanligste er at det avsettes for lite ressurser til sikkerhet, mangel på kompetanse i sikkerhetsarbeid og at sikkerhet er dårlig forankret i ledelsen.

Teknologiske sikringstiltak kan deles opp i tre kategorier:

- Fysiske sikringstiltak er fysiske barrierer som hindrer eller forsinker uønsket adgang

til verdier.

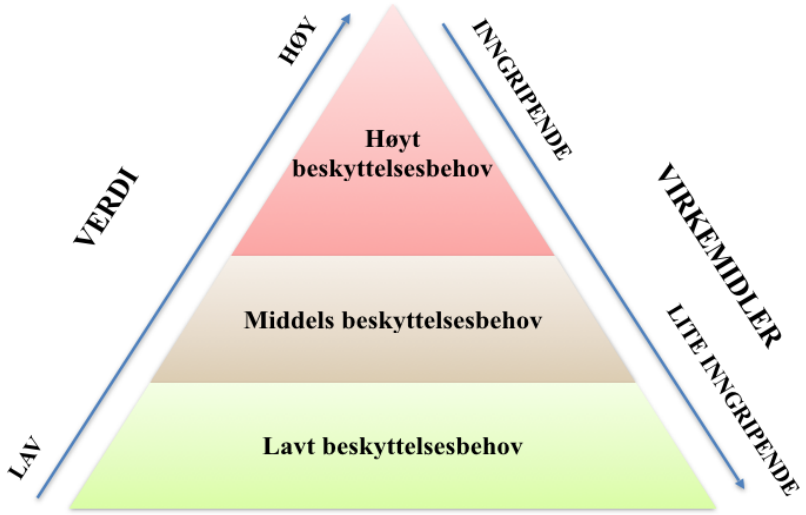
- Elektroniske sikringstiltak er tiltak som bruker elektronisk utstyr og løsninger for å støtte, supplere, eller erstatte fysiske sikringstiltak.
- Logiske sikringstiltak er tiltak for sikring av informasjon som lagres eller overføres elektronisk.

Eksempler på sårbarheter ved disse tiltakene kan være manglende fysisk barrierer og dårlig IKT system (NSM, 2016:19).

Etter at det er gjort en beslutning om valg av sikringstiltak skal disse implementeres for å oppnå sikringsmålene. Det skal her settes en tidsramme for påbegynnelse og ferdigstilling av sikringstiltak (NS 5831:4). Det kan tenkes at det er i denne fasen ”tregheten i systemet” oppstår. I beslutningsmodellen til Aven (2008) er dette det siste leddet ”beslutning og implementering”. IP-2 vet om mange virksomheter som har en ferdigstilt risikoanlayse med anbefalte tiltak, men at det ikke skjer noe på grunn av ”tregheten i systemet” og økonomiske hensyn. IP-1 mener at det ville være interessant å se om det faktisk blir satt en tidsramme for pågynnelse og ferdigstilling av sikringstiltak i virksomheter etter at NS 5832 er utført. IP-1 sier at det er sjelden konsulentselskaper som har utført en risikoanalyse får komme tilbake til virksomheten i ettertid og evaluere hva som har blitt gjort, og hvordan de anbefalte tiltakene fungerer i praksis (IP-1). Det er viktig at man måler effekten av tiltakene opp mot hverandre, sikringsmålene og kostnaden av tiltakene (Sikkerhetsstyring, 2015:15). I følge IP-1 får man inntrykk av at en slik evaluering av implementerte tiltak sjelden blir utført. Hvordan skal en virksomhet som har fått en risikoanalyse, selv være i stand til å evaluere sikringstiltakene?

4.2.5 Inngripende sikring

Når det gjelder hvor inngripende det forebyggende sikkerhetsarbeidet kan være, skal det etter Sikkerhetsloven § 6 ikke nyttes mer inngripende midler og metoder enn det som fremstår som nødvendig i forhold til den aktuelle sikringsrisiko og omstendighetene for øvrig. Det skal særlig tas hensyn til den enkeltes rettssikkerhet (Sikkerhetsloven, 2015).



Figur 8: Sammenhengen mellom verdi og virkemidler i sikkerhetsarbeidet (Mandt, 2015)

Figur 8 viser forholdet mellom verdi og virkemidler – høy verdi tillater inngripende virkemidler. *"Security measures of whatever kind must ultimately defer to the concept of human freedom"* (Manunta, 1998:40). Tiltak må veies opp mot åpenhet og tilgjengelighet (Sikkerhetsstyring, 2015:13). Under konferansen, "Designing out crime", ble viktigheten av å implementere sikringstiltak allerede i prosjekteringsfasen og byggfasen understreket. På en slik måte kan man planlegge for et åpent og estetisk samfunn ved å knytte sikkerhetstiltak og arkitektur sammen. Kunstfigurer og benker kan for eksempel fungere som kjøretøybarrierer, uten at dette nødvendigvis påvirker tilgjengeligheten og åpenheten for publikum. I følge IP-2 kan man ikke og skal man ikke sikre alt, for det skal jo være åpent og tilgjengelig også. Sykehus og akuttmottak er eksempel på objekter som skal sikres godt. Det å sikre slike objekter med fysiske og elektroniske sikringstiltak er fryktelig vanskelig, særlig fordi det er menneskene som er i fokus. Folk må kunne bevege seg rundt (IP-2). Vanskeligheten av å sikre sykehus påpeker også av IP-1.

4.2.6 Grunnsikring

Grunnsikring er sikringstiltak som ivaretar en virksomhets sikringsbehov ved normaltilstand (NS 5832:2), og er sikkerhetsråd nr. 4 i "veileder for terrorsikring" (2015). Sikringstiltak er tiltak for å redusere risiko forbundet med tilsiktede uønskede handlinger (NS 5830:3) Øyvind Mandt og Eli Sætersmoen (i samarbeid med Joakim Barane og Ronald Barø), har begge

skrevet hvert sitt innlegg i NSMs sikkerhetsblogg om sikring av virksomheter mot tilsiktede uønskede handlinger.

Øyvind Mandt hevder at er god grunnsikring viktigere enn noensinne for norske virksomheter. Dette er en forutsetning for å sikre mot terror. Eli Sætersmoen stiller spørsmåltegn ved om norske virksomheter er godt nok forberedt på terror eller andre alvorlige kriminelle handlinger. *«Man må løsrive seg fra forestillingen om at man kan forutsi sannsynligheten for at det utenkelige skal skje»* (Sætersmoen). Grunnsikring er bærebjelken i enhver virksomhets sikringstiltak, og det er grunnsikringen som er det daglige sikkerhetsnivået som skal beskytte virksomheten mot tilsiktede uønskede handlinger. For å finne et balansert og godt grunnsikringsnivå, er det avgjørende at norske virksomheter utfører en grundig sikringsrisikoanalyse der verdier, trusler og sårbarheter identifiseres og sikringsambisjon fastsettes. Sikringstiltak må basere seg på risikovurderinger. Å implementere sikringstiltak som skal redusere sårbarhetene til en virksomhet kan være svært tidkrevende og kostbart. Det er ikke kostnadseffektivt å justere tiltakene fra dag til dag, og sikringstiltakene er ofte ment til å vare i 15-20 år (Sætersmoen, 2015).

FFI gjorde en studie der de fant at de fleste sikkerhetsbrudd skyldtes organisatoriske sårbarheter, og mange av disse har med styring å gjøre. Gode organisatoriske sikringstiltak er en forutsetning for å få full effekt av teknologiske tiltak og redusere menneskelige sårbarheter (Risiko, 2016:7). Sikkerhetskultur og organisatoriske tiltak vil være avgjørende for sikkerhetsarbeidet i en virksomhet, da det ikke hjelper med gode teknologiske sikringstiltak hvis disse ikke følges opp og håndteres riktig (Mandt). Sikring for sikringens skyld er ikke av det gode. For enkelte handler sikring om synlige og fysiske sikringstiltak. Dette er viktig, men sikring skapes gjennom daglig virke og vaktsomhet, i samspillet mellom menneske, teknologi og organisasjon. Små organisatoriske justeringer kan bety mye for hvor god sikringen er i praksis (Mærli, 2012:6).

Terroranslag som rammer uten forvarsel vil kunne medføre stor skade, selv ved god grunnsikring. Virksomheter må regne med å klare seg selv i de første minuttene av et anslag, og her har kvaliteten på grunnsikringen mye å si for hvor store konsekvenser anslaget får. Fysiske sikringstiltak vil i de fleste tilfeller kun ha en forsinkende effekt på en angriper, og

disse er spesielt viktige når virksomheter skal sikres mot terrorhandlinger. I NS 5832 er det tatt med et tidsregnskap. Det vil si at man kalkulerer hvor lenge en barriere vil motstå et angrep, og hvor lang tid det tar før en reaksjonsstyrke blir varslet og ankommer stedet. Poenget med dette er at sikringstiltaket skal holde helt til en reaksjonsstyrke er på stedet. Hvis denne tiden er for kort, bør sikringstiltaket utbedres. Glassruten i bakgården på Nokas-bygget var for eksempel langt mer motstandsdyktig og effektivt enn det ranerne hadde beregnet, og politistyrker fikk bedre tid til å respondere på ranet. Gullsmedforretninger har for eksempel krav til at barrierer skal beskytte verdier en gitt tid. I gullsmeder og andre forretninger er det også skallsikring, der hvert av sikringslagene skal tåle en viss påkjenning. Man kan tenke seg at de ulike verdiene i en gullsmed er sikret på forskjellige nivåer. De mindre verdiene ligger kanskje åpent og synlig i butikklokalet, mens de største verdiene er lagt i en safe på bakrommet.

I et foredrag holdt av en operasjonsleder fra Politiet, fremkom det at mange av de som utførte risikoanalyser for viktige objekter, hadde antakelser om politiets responstid. Det fremkom under foredraget at man må være forsiktig med å ha en slik tidsberegning for politiets responstid med i analysen, fordi responstiden avhenger av hvilke og hvor store ressurser som er tilgjengelig. Hvis politressursene er opphengt i en annen hendelse, må objektets sikkerhetsbarrierer kunne motstå et angrep i lengre tid enn først beregnet. Dette førte til at risikoanalysene måtte utføres på nytt, med den informasjonen tatt i betrakning (IP-2). I artikkelen "Stortinget måtte passe seg selv" i VG, fremkommer det at det tok to og en halv time før Stortinget fikk politibeskyttelse etter terrorangrepet 22. juli (Johnsen, 2011).

I følge Mandt opplever NSM at virksomheter har fysisk sikring i varierende grad. Mange virksomheter har manglende verdi- og skadevurdering som ligger til grunn for de valgte sikringsløsningene, noe som påvirker den helhetlige sikkerhetsstyringen og risikoen, men også kvaliteten og effektiviteten på sikringstiltakene. Hvis ikke sikringstiltakene har dokumentert effekt, vil dette vanskeliggjøre forståelsen for reelle sikringstiltak og sikringstiltakene vil også kunne være for inngripende. Det er tid- og kostnadskrevende å prosjektere sikringstiltak, og det er vanskelig å rette opp feil sikringsløsninger. Mandt påpeker videre at i svært mange virksomheter vil man være avhengig av ekstern og objektiv rådgivningskompetanse for å unngå dårlige beslutninger om sikringsløsninger (Mandt, 2015).

I et skriv til Stortinget fremholder Justis- og beredskapsminister Anders Anundsen at det fortsatt er samfunnskritiske objekter som ikke er tilstrekkelig grunnsikret mot terrorangrep i Norge. Det er først og fremst privateeide objekter som ikke er sikret. I mai 2014 sa Anundsen at det var alvorlig at skjermingsverdige objekter ikke var sikret, og to år etter er det fortsatt ikke gjort (Johnsen, 2016).

Kjetil Nilsen, direktør NSM, skriver i Sikkerhetsfaglig Råd (2015) at de statlige fagmiljøene innen fysisk sikkerhet er relativt små og spredte i ulike etater med ulikt hjemmelsgrunnlag. Dette bidrar til at det er utfordrende for fagmiljøet å holde seg oppdatert på utviklingen i feltet. Det er tids- og kostnadskrevende å prosjektere fysiske sikringstiltak for virksomheter, og NSM har erfaring med at mange virksomheter har lav kompetanse når det kommer til anskaffelse av fysiske sikringstiltak. Mange virksomheter er avhengige av uavhengig og profesjonell veiledning for å gjøre riktig valg av løsninger, og lite tilgjengelig ekspertise gjør dette vanskelig (Nilsen, 2015:30). Det blir derfor et paradoks når det i veileder for terrorsikring (2015) står at «*der virksomheter mangler egen prosesskompetanse innen sikringsrisikoanalyse, kan det være nyttig å skaffe denne kompetansen eksternt»* (VT, 2015:16). I følge Nilsen har ikke NSM i tilstrekkelig grad kunnet gi målrettet rådgivning mot sivil sektor, da ressursene brukes opp på enkeltsaksbehandling av leverandørklareringer (Nilsen, 2015:31). I følge IP-2 var det tidligere nærmest umulig å samarbeide med andre innen sikkerhetsfagfeltet, fordi man satt på "hver sin tue", og tildels skapte vanskeligheter for hverandre. IP-2 mener at man i de siste årene har blitt flinkere til å samarbeide, samt å få kontakt med andre fagaktører og kompetanseområder, som for eksempel brannrådgivere. Det har blitt en økt forståelse for at man sammen må hjelpe sluttbrukere i sikring av virksomheter (IP-2). Det har gått nærmere 5 år siden 22. juli, og man må fortsatt erkjenne at det er mange skjermingsverdige objekter som fortsatt ikke er sikret. Dette underbygger utsagnet til IP-2 om at det er en innebygd treghet i staten. Man kan spørre seg om hvor realismen ligger i at "vanlige" virkomheter skal ha tilstrekkelig grunnsikring, når ikke engang de virksomhetene som har samfunnskritiske funksjoner er sikret.

4.2.7 Sikkerhetstesting

Det er viktig å få testet om de sikringstiltakene virksomheten har eller skal implementere faktisk fungerer. Sikkerhetsråd nr. 7 i veiledningen er at ”ingen plan er bedre enn selve gjennomføringen”. Sikringstiltak må testes og verifiseres opp mot at disse bidrar til oppnåelsen av sikringsmålene, og at de er effektive. Slik verifikasjon kan foregå som følge av inntrengningstesting, revisjon og øvelser (NS 5831:4). Virksomheten må revidere sikringsmålene opp mot den sikringsambisjonen virksomheten har, og her må det vurderes om man har råd til å innføre sikringstiltakene, eller om man må akseptere høyere risiko på grunn av økonomi etc (FFI, 2015:135). Som nevnt skal det ikke brukes for inngripende metoder, og sikkerhetstesting skal foregå på en etisk og forsvarlig måte. Verifikasjon og sikkerhetstesting er viktig for å avdekke og forstå hvilke sårbarheter det er i en virksomhet, og dette er nødvendig for å velge riktige sikringstiltak. Uvarslede tester vil bedre enn noe annet vise ”tingenes reelle tilstand” i virksomheten (VT, 2015:26). Sikringsøvelser burde vært langt mer fremtredende i sikringsarbeidet, der det fokuseres på testing av de forebyggende sikringstiltakene.

Ip-1 sier at det på generelt grunnlag er absolutt mindre vanlig med testing av den fysiske sikkerheten. Dette er noe som i følge IP-1 burde prioriteres i større grad. Det er få selskaper som tilbyr sikkerhetstesting av fysiske sikringstiltak, foruten noen selskaper som har spesialisert seg på å gjøre innbruddsforsøk. Det er imidlertidig veldig få som ser nytten av dette i de middels store virksomhetene i Norge. Innenfor IKT-sikkerhet er det vanligere med en software test. I større prosjekter som Regjeringskvartalet, vil det trolig bli gjort inntrengings- og penetreringstest. Det skal i alle fall kun brukes sikringstiltak som er godkjent av en standard. IP-1 er ikke sikker på om det er noen rutiner for om man skal teste ulike sikringstiltak mot hverandre. Selskapet IP-1 jobber, for har aldri fått returnere til en virksomhet for å se om sikringstiltakene de har anbefalt faktisk har blitt implementert, og om de fungerer. De møter ofte motvilje hos virksomheter, som ikke vil gi innsyn i sine sikkerhetssystemer. I følge IP-2 blir det enkelte steder utført sikkerhetstester og penetreringstester, men dette er mer unntaket enn regelen. Tidligere hadde sikkerhetstestingen høyere kvalitet og var mer utbredt. Den gang var det større kontantbeholdning i bankene. Det ble stadig holdt ransøvelser og opplæring i prosedyrer. Dette førte til at man fikk testet både ansatte og om hele systemet fungerte som det skulle. Det er få virksomheter som har ressurser

og kapasitet til å gjøre sikkerhetstester. Store virksomheter som Statoil og Telenor, har tatt innover seg at sikkerhetstesting er viktig. Disse selskapene har ofte veldig kompetente sikkerhetsfagfolk, men slik kompetanse finnes ikke overalt (IP-2). Mangel på sikkerhetstesting drar i følge Stranden, usikkerheten opp i stor grad. Sikkerhetstesting er mest effektivt for å sjekke sikkerheten, men kan også bli for inngripende, og det er begrensninger i hvor langt man kan dra testen (Stranden).

For å skulle sjekke om sikringstiltak fungerer etter hensikt bør sikringstiltakene testes. Hvis man ønsker å sikre seg mot en TUH, så er ingenting bedre enn å bli "utsatt" for en TUH, innenfor de rammene det lar seg gjøre. Da ser man hvordan sikringstiltakene fungerer i praksis, og sårbarheter kan avdekkes. Det er ikke nødvendigvis testing av fysiske sikringstiltak, men for eksempel adgangskontroll og identifikasjons-sjekk i resepsjonsområdet i en virksomhet. Hvis det er slik at uvedkommende kan komme seg inn i en virksomhet uten å måtte vise identifikasjon, eller at de stanses i et adgangskontrollsystem, kan dette avdekkes ved en inntrengningstest. For å rette opp en slik sårbarhet, kan det være nok med å små organisatoriske justeringer. Et eksempel kan være at de ansatte i resepsjonen får en muntlig påminnelse om hva de gjeldene prosedyrene for adgangskontroll.

NTNU og SIMlab har sammen åpnet en ny testrigg for bombeeksplosjoner og andre ekstreme påkjenninger. Testriggen er viktig for å bygge fagkompetanse innen sikring i Norge, og forskjellige aktører kommer sammen om testing og kunnskapsbygging i det fysiske sikringsfagfeltet. Prosjektet er nødvendig for å oppfylle myndighetskrav om tilpassede løsninger og kontrollert pengebruk. Dette kan tyde på at det er en økende satsing på sikkerhetstesting. Å danne en felles arena for kompetanseutveksling er også et viktig tiltak, særlig innenfor fysisk sikring, da Nilsen (2015) påpeker at fagmiljøet er lite og fragmentert. Det blir et spørsmål om det kun er de store og viktige virksomhetene som får benyttet seg av denne testriggen, men det gjenstår å se.

4.2.8 Krav til forebyggende sikkerhetstjeneste i virksomheter

I dag er det få lover og forskrifter som regulerer risikovurderinger mot kriminalitet generelt. Dette er i motsetning til helse, miljø og sikkerhet (HMS), der det er en rekke lover og

forskrifter som stiller krav til risikovurderinger (Kriminalitetsanalysen, 2015:11). Forebyggende sikkerhetstjeneste i virksomheter er planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet (Sikkerhetsloven §3, 1998). Private og offentlige virksomheter som ikke er underlagt Sikkerhetsloven, må forholde seg til organisasjonens ledelse og sikkerhetsmål. Noen ganger kan ikke virksomheten selv bestemme om en verdi skal beskyttes. Departementer, sektormyndigheter, offentlige krav og avtaler kan gi virksomheter plikt til å beskytte verdier, for eksempel verdier som kan være attraktive terrormål (NSM, 2016:11). Spesielle virksomheter som banker, apoteker og skipshavner, er eksempler på virksomheter som blir ilagt krav til sikkerhet av sektormyndighetene. ISPS-koden (International Ship and Port Facility Security Code) er et slikt krav. ISPS-koden ble vedtatt av FN´s sjøfartsorganisasjon IMO for å bedre sikkerheten for både skip i internasjonal fart og havneanlegg som tar i mot slike skip. I Norge er det Kystverket som har ansvaret for å implementere ISPS-regelverket som gjelder for havner og havneanlegg (Kystverket, 2016). Sjøfartsdirektoratet har ansvar for å implementere den delen av ISPS-regelverket som gjelder ombord på skip. ISPS-regelverket ble i hovedsak utarbeidet som en følge av den økte trusselsituasjonen etter 11. september og faren for terrorangrep mot skip og havneanlegg. Selvom terrorangrep mot norske skip og havneanlegg kan virke fjernt, er det større usikkerhet knyttet til trusselsituasjonen enn tidligere. Sikringstiltakene etter ISPS-koden har også vist seg å ha en forebyggende effekt mot andre kriminelle handlinger som tyveri og hærverk innenfor havneområdet som er omfattet av ISPS. IP- 1 sier at andre typer virksomheter må forholde seg primært til internkontrollforskriften og arbeidsmiljøloven. Her er det lite fokus rettet mot tilsiktede uønskede handlinger, og disse handler i større grad om HMS og utilsiktede uønskede hendelser (IP-1).

Næringslivets sikkerhetsråd (NSR) og OPINION har gjennomført Kriminalitets- og sikkerhetsundersøkelsen i Norge (Krisno, 2015). Krisno er en undersøkelse som har blitt utført syv ganger i tidsrommet 2006-2015. Den bygger på en spørreundersøkelse av 2500 offentlige (500) og private (2000) virksomheter. KRISNO (2015) dokumenterte at bare 23 prosent av virksomheter har en skriftlig risikovurdering. I de siste årene har det vært en økning av skriftlige risikovurderinger i offentlige virksomheter, men i privat sektor er antallet risikovurderinger forholdsvis stabilt. Det er en stor utfordring at virksomheter over tid har klart å tilpasse seg og sine dokumenter til myndighetenes krav om utføring av risikoanalyse.

Kontrolletatene ser en økende trend med en utbredt og økende bruk av forfalskede dokumenter og uriktige opplysninger. Ved manglende dokumentasjon kan det skje at aktører produserer dokumenter og dokumentasjon og informasjon som ikke gjennspeiler de reelle forholdene (Krisno 2, 2015:13). Krav til risikoanalyser kan i følge Stranden bli veldig populistisk. Stranden understreker viktigheten av at man ikke må gjøre en risikoanalyse hvis det ikke er hensiktsmessig. Det at virksomheter er pålagt å gjennomføre en risikoanalyse er i mange sammenhenger ofte basert på dårlig politisk ledelse som gjør det til et politisk krav (FFI, 2015:135). Årsaken er jo at risikoanalyser skal legge et godt beslutningsgrunnlag, og utfører man risikoanalyser bare for å utføre dem så kan dette føre til dårlige, uhensiktsmessige og kostbare sikringstiltak (FFI, 2015:136)

4.2.9 Kompetanse i forebyggende sikkerhetstjeneste

«Everybody who knows anything about security is aware that he does not know everything about security. The field is a huge one, and the problems are always changing…» (Wright, 1972: XI, Manunta, 1997:5). Det er kun når man vet hva sikkerhet er at man faktisk kan utvikle sikkerhetsplaner som tilfredsstiller virksomheters krav (Manunta, 1997:2)

Sikkerhetsråd nr. 3 i veilederen (2015) er at det blant annet skal være upekt en sikkerhetsleder. Et av spørsmålene i Krisno (2015) var om virksomhetene hadde én eller flere ansatte som jobbet fulltid med kriminalitetsforebygging og/eller sikkerhet. Offentlige virksomheter, og særlig offentlig administrasjon, har totalt sett flere fulltidsansatte i slike stillinger enn det private virksomheter har. Den viktigste faktoren som som bidrar til om virksomheter har fulltidsstillinger innen kriminalitet og sikkerhet er virksomhetens størrelse. Under offentlig administrasjon var det mange virksomheter med over 100 medarbeidere, og 23 prosent av disse hadde besatte fulltidsstillinger. I andre offentlige bransjer gjaldt ikke dette. Når private og offentlige virksomheter med over 100 ansatte ble målt opp mot hverandre, viste det seg at de private virksomhetene hadde flere besatte fulltidsstillinger, 24 prosent mot 16 prosent i offentlige virksomheter. IP-1 sier at selv store virksomheter som har sikkerhetssjefer og/eller intern sikkerhetsorganisasjon hyrer konsulentselskaper til å utføre risikovurderinger, gjerne fordi de ikke har tid eller kapasitet til å gjøre dette selv. Ofte er sikkerhetssjefen et slags kontaktpunkt og bidrar i verdivurderingen og objektkartleggingen, og i noen tilfeller er dette gjort før konsulentselskapet er kommet inn i bildet (IP-1).

Virksomheter må ofte leie inn konsulentselskaper med sikkerhetsfaglig kompetanse for å få utført risikoanalyser. Konsulentselskaper velges i mange tilfeller etter anbudskonkurranser, og selger/tilbyr i hovedsak kunnskap og problemløsninger til virksomheten som kunde. Andersen sier at virksomheter betaler for en problemsløsning, i forhold til hvor dyrt det er å ikke løse problemet. Hvor stort problemet er påvirker betalingsvilligheten. Ledere for konsulentselskaper har det fellestrekk at de klager over at kunders valg av konsulentselskap til syvende og sist handler om timespris og det billigste anbudet. Pris blir en kvalitetsfaktor. På "toppnivå" handler det mindre om pris, men heller om at konsulentselskapet har erfaring og kan vise til tidligere gode problemløsninger, og har kundens tillit (Andersen, 2010). Ved anbudskonkurranser handler det om troverdigheten til dem som presenterer resultatet (IP-1). Anbudskonkurranser har et problem ved at det ofte leies inn konsulentselskaper etter lavest pris, uten at kvalitet vektlegges (Andersen, 2010). Dersom en virksomhet bruker et konsulentselskap uten tilstrekkelig kompetanse, kan også sikkerhetsrådene bli dårlige. Det er ikke noe poeng i å anbefale investering i skuddsikre vinduer for 10 millioner, dersom ikke vindusrammene holder samme kvalitet (Stranden).

I følge Manunta (1997) kan nøkkelen til fremtidig suksess oppsummeres med tre ord: "utdanning, utdanning og utdanning"(Manunta, 1997:5). *"Vi har ingen utdannede personer på høyt akademisk nivå innen dette faget fordi vi har ingen retning og det er få utdanningsretninger innen dette faget i Norge per dags dato"* sier Haneborg (FFI, 2015:102-3). Det er viktig å stille kompetansekrav til de personene som deltar i risikoanalyseprosessen. For det første må man ha god kompetanse i risikoanalyse. For det andre må man ha god kunnskap om virksomheten som skal analyseres. Arbeidsgruppens sammensetning er viktig for kvaliteten på analysen, og her er praktisk erfaring særlig viktig. Risikoanalyser blir ikke bedre enn de som utformer disse analysene sier Bakke-Hanssen (FFI, 2015:115). Stranden mener også kompetansekrav til analytikere er viktig, og at faget skal gå i den retning at det blir tydelig at security er et eget fagområde, og ikke noe alle kan ha kjennskap til (FFI, 2015:136).

4.2.10 Terminologi

Det er i NS 5832 og NS 5814 ulike betydninger av helt sentrale begreper. De viktigste begrepene er listet opp i tabell 3:

Tabell 4: Begrepsforståelsen i NS 5814 og NS 5832.

NS 5832		NS 5814	
Sikringsrisiko-styring:	«en prosess for å fatte overveide beslutninger basert på identifisert risiko, med mål om å oppnå en akseptabel grad av risiko…» (NS 5831:3).	**Risikostyring**:	«identifisere, analysere og vurdere mulige risikoforhold i et system eller virksomhet, samt å finne frem til og iverksette tiltak som kan redusere mulige skadevirkninger» (FFI, 2015:21).
Sikringsrisiko-analyse:	«Sikringsvurdering samt vurdering av tiltak» (NS 5832:4).	**Risikoanalyse:**	«en systematisk fremgangsmåte for å beskrive og/eller beregne risiko…» (FFI, 2015:21)
Sikringsrisiko-vurdering:	«helhetsvurdering basert på verdivurdering (eller konsekvensvurdering), trusselvurdering og sårbarhetsvurdering, med mål om å angi en entitets risiko i en definert sikringsmessig kontekst» (NS 5832:4)	**Risikovurdering:**	«en samlet prosess som består av de tre trinnene planlegging, risikoanalyse og risikoevaluering» (FFI, 2015:21).
Risiko:	«uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (NS 5830:5).	**Risiko:**	«uttrykk for kombinasjonen av sannsynligheten for og konsekvensene av en uønsket hendelse» (Rausand og Utne, 2009:22).

En av årsakene til at det er forskjellig begrepsbruk i NS 5814 og NS 5832, er at arbeidsgruppen som utarbeidet NS 5832 kontaktet Språkrådet. Arbeidsgruppen vill være tro mot ordboksdefinisjonene av ordene ”analyse” og ”vurdering”. *Vurdering* brukes der man beskriver ”hva betyr egentlig dette for oss”? *Analyse* blir brukt om en prosess der man ”bryter ned informasjon til sine enkelte bestanddeler og setter dem sammen for å avdekke en mening” (Barane, FFI, 2015:121). Arbeidsgruppen utarbeidet NS 5830 – *”Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – terminologi”* for å fastsette terminologi til bruk i fagområdet security. I NS 583X-serien var i følge Midtgaard DSB mest kritisk til at arbeidsgruppen som utarbeidet NS 5832 gav etablerte og definerte begreper i andre standarder nytt innhold. Dette var grunnen til at DSB gav NS 5832 motstand, fordi dette ville vanskeliggjøre kommunikasjon om risiko og risikoanalyser. Det ble en løsning at man i NS

583X konsekvent brukte sikringsrisiko istedet for risiko. Dette er et helt nytt begrep, som ble innført til tross for at det var en del innvendelser fra andre aktøerer i sikkerhetsfagmiljøet, blant annet DSB (FFI, 2015:110). Når begrepene sikrings/risikovurdering og sikrings/risikoanalyse brukes om hverandre, og innholdet i dem er så forskjellig som i NS 5814 og NS 5832, blir det vanskelig å skille begrepene fra hverandre. Det at man bruker ”sikring” foran begrepene er essensielt for å forstå at det er NS 5832 og security man snakker om, men selv fagpersoner og rapporter er inkonsekvente på dette området. Slik Barane poengterer, oppleves det som om begrepene brukes om hverandre i praksis.

Det har vært umulig å være konsekvent i bruken av de sentrale begrepe, fordi begrepene brukes om hverandre både i litteraturen og i det sentrale fagmiljøet. Bare det å si ”tilnærminger til risikovurdering” slik det er skrevet i FFI-rapporten, fører til en usikkerhet. Et annet eksempel er Krisno (2015), der ”risikovurdering” brukes konsekvent, uten at det utrykkes om dette begrepet hører til NS 5814, NS 5832, begge deler eller en annen tilnærming. Det står at ”bare 23 prosent av alle virksomheter har en skriftlig risikovurdering”, men hva er risikovurdering i denne sammenhengen? I Krisno (2015) står det at 4 prosent har innhentet PSTs åpne trusselvurdering. Dette tyder på at i alle fall disse 4 prosentene har gjort en risikovurdering mot TUH. I ”Håndbok: Risikovurdering for sikring” (NSM, 2016), står det klart og tydelig at håndboken gjelder gjennomføring av risikovurdering med fokus mot TUH, og at den baserer seg på NS 5832. I håndboken står det videre: ”sikringsrisikovurdering, heretter omtalt som risikovurdering” (NSM, 2016:5). Dette gjør det helt tydelig det er risikovurderingen i NS 5832, men hvorfor ikke kalle det ”Håndbok for sikringsrisikovurdering”? Ble ikke ”sikringsrisikovurdering” og resten av terminologien i NS 5830 utarbeidet for å tydeliggjøre et skille mellom safety og security. Det at ”sikringrisiko” ble brukt i stedet for risiko var jo i følge Midtgaard en av grunnen til at DSB ikke gav motstand mot terminologien lenger (FFI, 2015:110)

Hvorfor forholder man seg ikke bare til ”sikrings-begrepene” slik at man unngår misforståelser som kan oppstå praksis? Konsekvent bruk vil føre til et tydelig skille mellom begrepsforståelsen i NS 5814 og NS 5832, og det var vel dette man i utgangspunktet var ute etter. Er noe av årsaken at sikrings-begrepene blir lange og tunge å bruke i skrift og dagligtale? Eller er det på grunn av at risikoanalyse og risikovurdering er inngrodde begreper som det vil ta tid å avvende seg med i NS 5832. Stranden håper at security skal bli et tydelig

og eget fagfelt (FFI, 2015:136), og da kan det tenkes at det ikke er så farlig med hvilken benevnelse man velger å bruke.

4.2.11 Penger og politikk

Sikkerhet spiller en signifikant rolle i samfunnspolitikken -og økonomien, men sikkerhet er også et uoversiktlig fagfelt. Det råder mistillit og manglende konsensus mellom hovedaktører som rådgivere, analytikere og beslutningstakere. Det strides om ressursbruk og prioriteringer av tiltak. I følge Manunta (1997) kan topplederes syn på kommersiell og industriell sikkerhet noen ganger være lite flatterende (Manunta, 1997:1):

> *«Security is a non-productive, a highly expensive capital item, extremely costly to install and maintain, always seems to need updating, is forever giving false alarms, and, since we have insurance, who really needs it anyway?»* (Handbook of Security, supply. 25: 8.2-01, Manunta, 1997:1).

På den andre siden tviler sikkerhetsfagfolk på toppledernes kompetanse og beslutningsevne når det kommer til sikkerhetsspørsmål (Manunta, 1997:1):

> *«Corporate executives who are skilled at making profits often appear to be naive consumers when it comes to decisions about security expenditures»* (Jenkins, 1985:xxiii, Manunta, 1997:22).

I følge Ip-1 er sikkerhet absolutt en ekstra kostnad, men det er jo en del av utfordringen når man skal kommunisere NS 5832 på en god måte. Det er lagt inn en økonomivurdering i NS 5832 for å synliggjøre at sikkeret koster penger, men at det i et livsløpsperspektiv og driftkostnadsmessig er slik at virksomheten sparer inn det sikringstiltakene kostet. Sikkerhetsrådgivere må kommunisere at noen få investeringer vil kunne medføre betydelig innsparing, både i forhold til å redusere tap hvis det skjer noe, men også i forhold til omdømme og andre verdier. Det er viktig å få frem at sikkerhet ikke bare er negativt, men at det også handler om en mulighet til å bygge omdømme. Man får også en mulighet til å vise at virksomhetens verdier tas på alvor. Dette vil kunne gi virksomheten et rykte i bransjen at virksomheten er profesjonell. Når det skal investeres i sikkerhet, er det viktig at den

virksomheten man rådgir vet forskjellen på ulike sikringstiltak. Det finnes for eksempel mange forskjellige adgangskotrollsystemer, kjøretøysbarrierer og utforminger av resepsjonsområder. Det kan være en idé at man skal kunne bygge videre på allerede eksisterende sikringstiltak etter behov, slik at ikke sikringstiltak må byttes ut etter to år i drift. Det blir i så fall en veldig stor kostnad virksomheten kunne vært foruten. Det er ikke sånn at en virksomhetsleder representerer "fienden" dersom investeringsviljen i sikkerhet er liten. Det handler om å finne den "gyldne middelvei", slik at man kan oppnå akseptabel sikring, og at "virksomhetslederne får sove om natten" med tanke på kostnaden. Man kan ikke beskytte seg mot alt. Det handler om at man skal legge sikkerheten på et nivå som er høy nok, og så blir det et spørsmål om hvor dette nivået skal ligge sier IP-1. Rapp understreker at en av faktorene at risikoanalyser må tilpasses virksomhetens totale ressurser, slik at analysen blir anvendbar i praksis (FFI, 2015:129).

IP-2 vet om mange virksomheter der risikoanalyser er gjennomført og alt ligger tilrette for iverksettelse av sikringstiltak. Likevel blir det "stående og henge" på grunn av økonomien, og ingenting blir gjort. Det er jo heller ikke sånn at man bør sikre alt, og virksomheten må jo overleve, men IP-2 opplever det slik at det ofte er minimumskravet til sikring som blir valgt **(**IP-2). Økonomi er en av de største grunnene til at det er "innebygd treghet" mange steder når det kommer til beslutningstaking ved sikkerhetsspørsmål (IP-2).
NOU 2000:24 – *"Et sårbart samfunn":* "*Dagens samfunn er mer sårbart enn før. Forhold som bidrar til at vi står overfor nye sårbarhets- og sikkerhetsutfordringer er blant annet:*

- *De teknologiske endringene i samfunnet.*
- *Den økende kompleksiteten i samfunnet.*
- *Det økende kostnads- og effektiviseringspresset.*
- *Reduksjonene i bemanningen i mange virksomheter.*
- *Utsetting av offentlige tjenester til kommersielle virksomheter"* (NOU 2000:24:6).

Økende kostnads- og effektivitetspress og reduksjon i bemanning, er to av årsakene som fører til et mer sårbart samfunn. Et mer sårbart samfunn gjør at usikkerheten og uforutsigbarheten for å bli utsatt for tilsiktede uønskede handlinger blir større. Norges engasjement i internasjonale konflikter kan føre til at Norge blir et direkte mål for terror. Utvalget i NOU har hatt mandat til å til å fremme tiltak som kan bedre tryggheten i Norge. Virksomheter og myndigheter må gå igjennom budsjetter, noe som kan bety omprioriteringer innenfor gjeldene

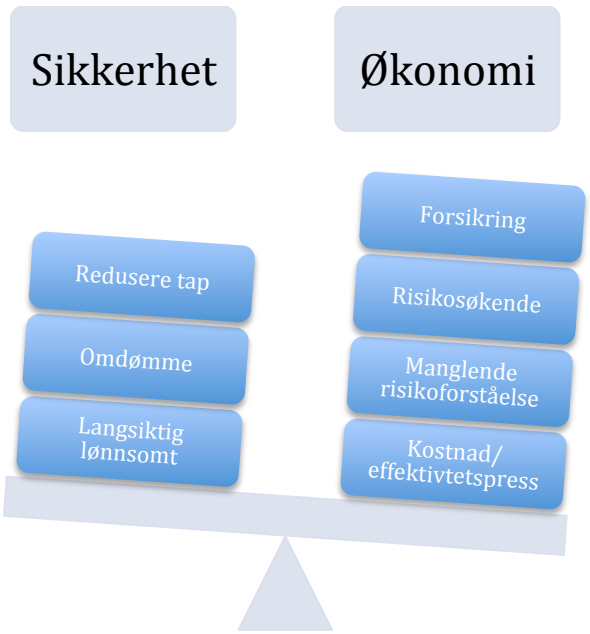
budsjettrammer. Hvor store utgiftene vil bli er avhengig av politikken i samfunnssikkerhet (NOU 2000:24:7). Den reelle kostnaden av investering i sikkerhet må ses opp mot det man sparer på å hindre at ulykker og tilsiktede uønskede handlinger skjer (NOU 2000:24:298).

I en kronikk skriver Eirik Bjorheim Abrahamsen, førsteamanuensis ved UiS, at hovedutfordringen i sikkerhetsstyringen er hvordan man skal balansere kostnadene ved sikkerhetstiltak og sikkerhetsaktiviteter på den ene siden, og mulige tap, ulykker og katastrofer på den andre siden. Ressurser til sikringstiltak er begrenset, og det er derfor viktig å måle effekten av ulike sikringstiltak. I vurderingen av sikringstiltaket bør man se tiltaket i lys av hvordan det påvirker allerede implementerte tiltak og organisasjonen forøvrig. Selv om tiltaket isolert vurderes til å ha god effekt, så er det ikke sikkert det er like effektivt i samspill med de andre tiltakene, noe som kan føre til uheldig ressursbruk og overinvestering. Det investeres ofte i sikringstiltak uten at det tas hensyn til om det finnes et forsikringsmarked. Abrahamsen spør seg om investeringer i sikkerhet skal reduseres hvis det er mulig å investere i forsikringsordninger. Mange vil hevde at forsikring ikke skal påvirke sikkerhetstiltak, da det er en prinsipiell forskjell mellom investering i forsikring mot investering i sikringstiltak. Forsikring gir kompensasjon for ulykke, mens sikringstiltak kan hindre selve ulykken. Økonomifag kan bidra til økt kunnskap når det gjelder sikkerhetsstyring. Dette kan kan føre til et bedre sikkerhetsnivå enn tidligere med mindre ressursbruk. Tverrfaglighet vil forbedre sikkerhetsstyringen (Abrahamsen, 2010)

Kjetil Nilsen, direktør for NSM, sa under NSMs årlige sikkerhetskonferanse (2016) at mange virksomheter ser på sikkerhet som en kostnad, men at det også kan representere en investering. Det er flere land som satser på sikkerhet for å tiltrekke seg internasjonale aktører i næringslivet. Som følge av den økte arbeidsledigheten i oljesektoren, står Norge overfor store omstillinger. Etter Nilsens mening er sikkerhet en forretningsmulighet. Sikkerhet kan bli en næring som ikke bare sikrer verdier, men også utnytter muligheter og skaper verdier i fremtiden (Simonsen 2016). *«Sikkerhet er god forretning, det lønner seg. I oljeindustrien har man lært at katastrofer er svært kostbare. Synes du sikkerhet er dyrt, prøv en katastrofe»* sier Sven Ullring (NSM, 2012:15). Etter helikopterstyrten utenfor Turøy de 29. april, 2016, stod det på Dagbladets forside tirsdag 3 mai: «*Sikkerhet må ikke ofres på økonomiens alter*». Ulykken fant sted én dag etter at rapporten til Petroleumstilsynet ble fremlagt: «*Kartlegging av risikobildet i petroleumsvirksomheten er et varsko. De indikerer at noe kan være i ferd*

med å skje med sikkerhetsnivået». Helikopterulykken som kostet 13 mennesker livet. I rapporten antydet Petroleumstilsynet at det er en sammenheng mellom de økonomiske nedgangstidene i petroleumsbransjen og en økt risiko for ulykker (Dagbladet, 2016).

Er virksomhetens betalingsvillighet liten, men til tross for at de fokuserer på god sikkerhet, vil det være ekstra viktig at de begrensede ressursene blr maksimalt utnyttet. Haneborg poengterer at "det er til slutt tallene som rår" (FFI, 2015:104). "I praksis så er det få virksomheter som har ressursene til å gjennomføre en faglig og god risikovurdering" (Krisno 2, 2015:11). Mærli sier at en viktig å erkjennelse er, paradoksalt nok, at sikring synes best når den feiler eller utfordres (Mærli, 2012:7). Hvorfor skal man bruke penger på å redusere risiko, når grunnen til at virksomheten har gjort suksess nettopp er ved å ta risiko spør IP-1 s?



Figur 9: Vekting mellom økonomiske og sikkerhetsmessige hensyn.

Figuren søker å illustrere hvordan sikkerhetsmessige- og økonomiske hensyn må veies opp mot hverandre. I oppgaven fremkommer det at de økonomiske hensynene veier tyngst. Det er ofte minimumskravet til sikkerhetnivå som blir brukt. Økonomiske hensyn og treghet i beslutningsprosessen fører til at sikringsarbeidet stopper opp når alt egentlig ligger til rette for å implementere identifiserte sikringstilak (IP-2). ALARP-prinsippet handler om at man skal redusere risikoen så langt det er praktisk mulig, men at hvis kostnaden av å redusere risikoen

overstiger nytten, anses risikoen som akseptabel. Det kan tenkes at ALARP-prinsippet ofte ikke følges, hvis det er slik fagpersoner har inntrykket av virksomheter ofte legger sikkerhetsnivået etter minimumskrav til sikring. Det tyder på at analytikere og sikkerhetsrådgivere kommer lengst ved å ha en pragmatisk tilnærming når gunstigheten av sikkerhet skal fremmes for virksomheters ledere. Stranden sier at man skal være sparringspartnere med virksomheten i risikoanalyseprosessen. Videre må man legge sikkerhetsnivået på et nivå som gjør at lederne kan ”sove godt om natten”, ved at de føler beslutningen om bruk av penger på sikkerhet er innenfor ALARP-området, og at de ikke har brukt unødvendig mye ressurser på å oversikre virksomheten.

Mennesker er ikke fullstendig rasjonelle (IP-1), men rasjonelle nok til å søke å få maksimalt utbytte av en beslutning. Og her kommer det økonomiske perspektivet inn. Hva er gevinsten av å investere i sikkerhet? For konsulentselskaper og sikkerhetsrådgivere er det utfordrende å fremstille sikkerhet som en gunstig investering med fremtidig avkastning. Når verdien av sikkerhet ikke vises, blir det ufordrende å skulle ”selge” inn viktigheten av sikkerhet til virksomheters ledelse. Dette fører til at det nærmest blir nødvendig å bruke sikkerhet som en kommersiell vare med tanke på å øke eller ivareta virksomheters omdømme, seriøsitet og profesjonalisme. Som Nilsen sier så kan sikkerhet være en forretningsmulighet og skape verdier i fremtiden.

I følge Veileder i terrorsikring (2015) er det å ha gjort gode forberedelser både innen forebyggende sikkerhet og beredskap et kollektivt samfunnsansvar, som enhver virksomhet bør ivareta (VT, 2015:3). Dette er det ideelle, men likevel like urealistisk som Statens vegvesens ”nullvisjon” av antall dødsulykker i trafikken. Til syvende og sist kan man spørre seg: ”Hvem er sikkerhet egentlig viktig for?” Det er viktig for de konsulentselskapene som skal gjøre profitt på å selge sikkerhet til virksomheter. Det er viktig for en virksomhets ømdømme og seriøsitet, og videre at sikkerhet kan redusere konsekvensen av en TUH. Det er viktig med god sikring av virksomheter, i den forstand at tilstrekkelig sikring inngår som en del av et kollektivt samfunnsansvar. Her er målet å beskytte og skape trygghet for befolkningen. Det kan tenkes at profitt og omdømme veier tyngre enn samfunnsansvaret.

4.3 Hvordan tas beslutninger i forhold til sikring?

4.3.1 Beslutningstaking og usikkerhet

Det vil alltid vær usikkerhet ved risikovurderinger og risikoanalyser. Det er viktig å forstå denne usikkerheten, slik at beslutningsgrunnlaget blir mer troverdig for ledelsen. Når det er snakk om sikring mot TUH, er det snakk om usikkerhet knyttet til hva som kan ramme virksomheten, hvilke skader og konsekvenser, effekten av tiltakene og hva som blir tilstanden under og etter hendelsen (NSM, 2016:5). I praksis har det blitt brukt mange forskjellige forståelser av sannsynlighet til å rangere forhold innen usikkerhetsområder. Noen ganger har man tilstrekkelig historisk data med tallmateriale som oppfyller kriteriene for å benytte en tradisjonell teknisk tilnærming til risiko. Andre ganger har man ikke statistisk tallmateriale i det hele tatt og må bruke det man kaller *ren bedømmelse*. Krysningspunktet mellom statistisk sannsynlighet og ren bedømmelse kalles *estimert sannsynlighet*, da man har noe tallmateriale, men ikke nok til å oppfylle kriteriene for statistisk metode. Tilnærminger og metoder for risikovuderinger og risikoanalyser må uansett tilpasses data- og informasjonsgrunnlaget. Innenfor sikring mot TUH menes sannsynlighet som ”muligheten for” (likelihood). Man gjør for eksempel en rangering av hvilke scenarioer som det er mulighet for. Det samme gjelder rangering de mest aktuelle trusselaktører, i hvilken grad de kan lykkes, og hvor stor skade de kan påføre virksomheten (NSM, 2016:5).

Det er viktig å forklare usikkerhet ved å få frem om at man har manglende informasjon om en trussel, og at man beskriver hvorfor man kom frem til et bestemt risikonivå. Stranden har ingen tro på å forenkle resultatet (FFI, 2016:135). I følge Røed må man være ydmyk når man presenterer risikobildet til ledere og si: *”dette er det vi vet, dette er det vi tror, og dette antar vi”* (FFI, 2015:101). Dette kan skape et ærlig beslutningsgrunnlag for ledere fordi usikkerheten ved vurderingen kommer frem. Røed er skeptisk til risikoakseptkriterier fordi en i praksis flytter beslutningene fra leder til analytiker. Det mest ideelle hadde vært å ha en metode som tvinger ledere til å sette seg inn i beslutningsgrunnlaget før man tar en beslutning sier Røed (FFI, 2015:101). Bakke-Hanssen mener at NS 5832 passer best fordi den i større grad involverer ledelsen og bidrar dermed til en bedre risikoforståelse (FFI, 2015:112). Haneborg påpeker at NS 5832 ansvarliggjør beslutningstaker ved at beslutningstaker må sette seg inn analysen (FFI, 2015:105).

Haneborg påpeker at det er viktig at virksomheten selv bidrar i verdivurderingen og er med i prosessen slik at analytikerne kan ha en rolle som sparringspartnere. Det er uansett usikkerhet i produktet etter endt analyse (FFI, 2015:106). Den store utfordringen med NS 583X-serien er vurderingen av risiko og presentasjonen av risikobildet, da tilnærmingen bare har verdi, trussel og sårbarhet. Det er i følge Bakke-Hanssen hvordan man skal presentere risikobildet at kampen mellom de ulike tilnærmingene ligger (FFI, 2015:112). Barane sier at hvis noen hadde kommet opp med en måte å fremstille risiko etter NS 5832 på en forståelig måte, så ville han vært veldig interessert i det, for det er utfordrende (FFI, 2015:122).

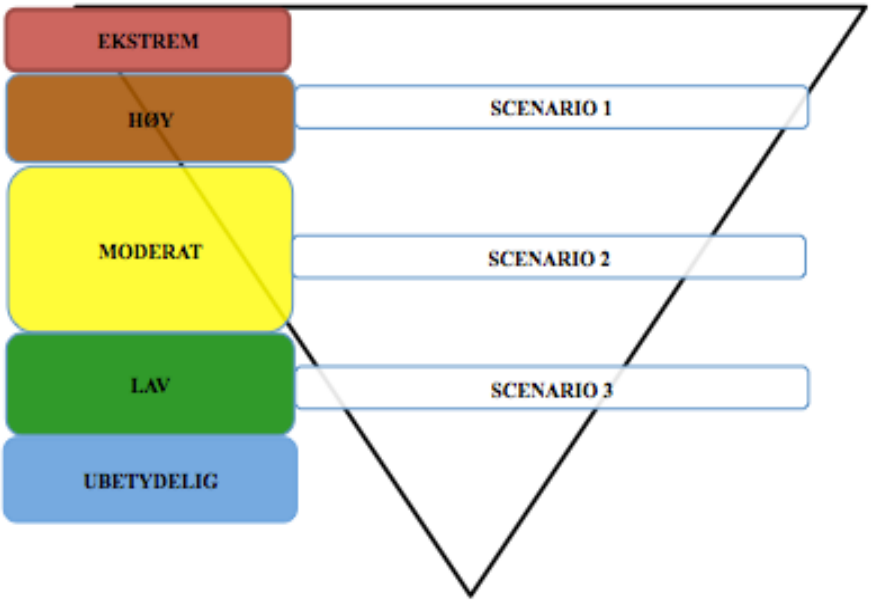
Stranden støtter Avens mening om at man må legge vekt på usikkerheten og hvordan man kan redusere usikkerhet (FFI, 2015:136). Når det gjelder kommunikasjon av usikkerhet så har man lite kunnskap om hvordan dette faktisk foregår i praksis. Det foreligger ingen klare standardiserte retningslinjer og fremgangsmåte for hvordan dette kan gjøres. I følge Aven (2013) finnes det ulike metoder som kan bidra til å vurdere styrken på kunnskap. En av dem er at hvis en eller flere av disse betingelsene er tilstede, er kunnskapen svak:

1. Antakelser er veldig forenklet.
2. Data er ikke tilgjengelig eller upålitelige.
3. Det er mangel på enighet/konsensus mellom eksperter.
4. Fenomenet som er involvert er ikke godt forstått; modeller er ikke eksisterende, eller er er kjennetegnet av å gi dårlige predikasjoner. (Aven, 2013:138).

Disse stegene kan brukes av analytikere for å si noe om kunnskapsstyrke ved de vurderingene som er gjort i risikovurderingen. Røed påpeker at det er viktig å være tydelig på hva man mener med begrepet usikkerhet. Det er ikke noe som heter sann risiko. Når man vurderer risiko, er det jo egentlig usikkerhet man vurderer. Usikkerhet er veldig sentralt i risikovurderinger, men er vanskelig å ta hensyn til i praksis. Man kommer langt med å karakterisere bakgrunnskunnskapen, og om den er god eller dårlig (FFI, 2015:102).

4.3.2 Visuell fremstilling av risiko i NS 5832

Det å fremstille og visualisere risiko i NS 5832 har vist seg å være en vanskelig oppgave, og hvordan dette bør gjøres er stadig gjenstand for diskusjon i sikkerhetsfagmiljøet. Presentasjon av risikobildet bør inneholde en visuell fremstilling som skaper oversikt, samt en tilhørende rapport som beskriver vurderingene knyttet til hver risiko (NSM, 2016:23). I kurset "Innføring i sikringsrisikoanalyse" viste kursleder Roy Stranden frem en modell som skal visualisere risiko i NS 5832:

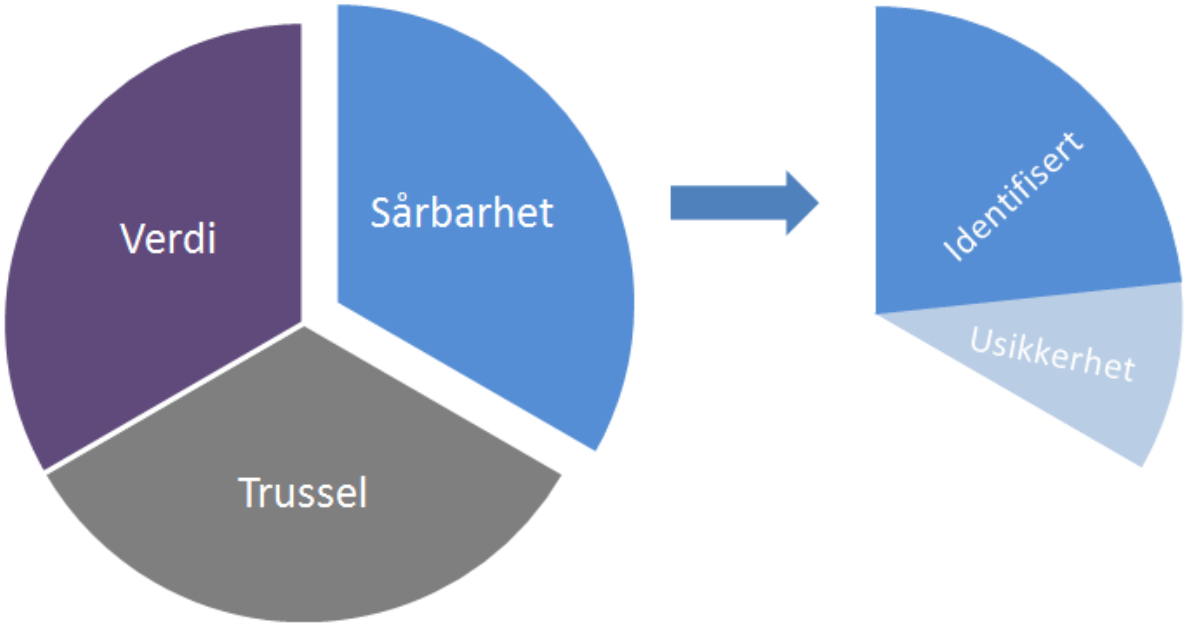


Figur 10: Fremstilling av risikobildet i kurset "Innføring i sikringsrisikoanalyse" (Kurs/Stranden).

I figur 10 er scenarioene rangert i henhold til hvor stor risiko som er forbundet til dem.

Stranden mener at man må være konkret og beskrive risiko knyttet til ulike aktiviteter, dersom man skal lykkes med å formidle resultatet av risikoanalysen. Man tjener på å nyansere begrepene, slik at man ikke beskriver terror i sin helhet, men ulike typer terrorhandlinger. Videre påpeker Stranden viktigheten av å forklare hvilket informasjonsgrunnlag som ligger til grunn for vurderingen, og usikkerheten ved om man har avdekket alle relevante faktorer og tolket dette riktig. Det å vektlegge usikkerheten er noe av det viktigste i risikoanalysen, for eksempel å ta med i konklusjonen at det har vært lite tid til rådighet og at informasjonsgrunnlag har svakheter (FFI, 2015:136). Det viktigste ved en fremstilling av risiko er at risikobildet skal si noe om "hva betyr dette for deg og din virksomhet" sier Barane (FFI, 2015:121).

I kurset "Innføring i sikringsrisikoanalyse" fikk deltakerne mulighet til å forsøke å lage en egen fremstillingen av risiko etter NS 5832. Figur 11. er et forsøk på å visualisere hvor mye usikkerhet det ligger i hver av vurderingene, og er ment til å være et supplement til figur 10. Det er analytikeren selv som anslår usikkerheten ved risikovurderingen, og usikkerheten visualiseres ved at man deler kakestykket i to og velger en størrelse på usikkerheten i kakestykket. Figuren er kun ment å fungere som et bakteppe før lederne leser rapporten.



Figur 11: Forslag til visuell fremstilling av usikkerhet/mangel på kunnskap ved risikovurdering i NS 5832.

Kakediagrammet i figur 11 er usikkerheten ved sårbarhetsvurderingen brukt som et eksempel på å visualisere usikkerhet. De som gjennomfører risikovurderingen må si noe om hvor stor usikkerhet de mener det er i hver av vurderingene. Som Stranden sier så må analytikeren si noe om informasjonsgrunnlaget risikovurderingen er basert på, og rammefaktorer som tid til rådighet og ressurser. Beslutningstakere og ledere får et visuelt bilde av hvor stor usikkerhet det anslås å ligge i hver av vurderingene. Å sette et mål på usikkerhet er umulig, og det er dette denne figuren til dels gjør. Likevel vil en slik figur skape en forventning til hva som er skrevet i sluttrapporten. Lederne ser at det er mye usikkerhet ved sårbarhetene, og vil

forhåpentligvis ha et ønske om å lese analytikerens begrunnelsen for dette. Figuren har til hensikt om å vekke interesse og en forventning til hva rapporten inneholder.

Som et tankeeskperiment og et forsøk på å forklare figuren er det nedenfor skrevet en tenkt monolog av en analytikers muntlige og visuelle fremstillig av figur 10 og 11 til ledelsen:

Tabell 5: Tentativ verbal fremstilling av risikovurdering

En tentativ fremstilling av risikobildet i figur 10 og figur 11 med tilhørende visualisering av usikkerhet i verdi-, trussel-, og sårbarhetsvurderingene		
1	**Risikoanalytiker:**	"Det vil alltid være usikkerhet rundt de vurderingene vi har gjort i risikovurderingen. Vi har gått igjennom vurderingene og forsøkt å visuelt fremstille hvor mye vi tror vi har identifisert av trusler, verdier og sårbarheter, og hvor mye usikkerhet/mangel på kunnskap vi mener det ligger i hver av vurderingene".
2	**Verdi:**	"Vi mener at vi kjenner til verdiene i virksomheten, da verdivurderingen har vært grundig og virksomhetens ansatte og ledere har bidratt til dette. Det foreligger derfor lite usikkerhet rundt verdivurderingen som dere ser i kakediagrammet. Vi har rangert verdiene: 1) IKT-løsninger, 2) viktige bedriftsdokumenter, og 3) elektroniske apparater".
3	**Trussel:**	"Det er fordi det er vanskelig å kunne si noe presist om truslene, men ut i fra den informasjonen vi har i dag, har vi satt vinningskriminelle som den mest aktuelle trusselen mot denne virksomheten. Kunnskapsgrunnlaget som ligger til grunn for vår vurdering er PSTs åpne trusselvurdering, samt at vi har hatt dialog med politidistriktet. Politiet fikk ga oss informasjon om at det har vært en økning av vinningskriminalitet mot virksomheter og butikker i den siste tiden. Ut i fra denne informasjonen har vi utarbeidet et scenario på bakgrunn av gjerningspersonenes modus".
4	**Scenario 1**	"Gjerningspersonene er profesjonelle og har stor kapasitet. Modus er bruk av kjøretøy for å kjøre inn dør eller bruk av avansert brekkverktøy. I butikker blir det stjålet store mengde tobakk og kontanter, mens i virksomheter er det i hovedsak elektroniske apparater og andre verdier som blir bortatt".
5	**Sårbarhet**	"Som dere ser i figur 11 er det i kakediagrammet ca. 1/3 usikkerhet i sårbarhetsvurderingen. Dette er i hovedsak fordi vi mener at noen verdier har manglende sikring, og at noen av de sikringstiltakene dere allerede har, ikke er testet".
6	**Oppsummering og sikkerhetsråd:**	"Vi har satt risikoen som høy for scenario 1 – vinningskriminalitet. Dette er på bakgrunn av den totale estimerte risikoen for virksomheten i risikovurderingen. I følge politiet er modus at gjerningspersonene bruker kjøretøy og avansert brekkverktøy for å komme seg inn i lokalene. Virksomheten deres har ikke dører som vil kunne motstå en slik påkjenning. For å kunne motstå en må dere bytte ut dørene alle dørene, samt at rammerverket rundt dørene må testes. Kostnaden for disse tiltakene estimeres til å koste 400 000 kr.

		Dette vil være gunstig for dere hvis dere ønsker å beskytte alle de identifiserte verdiene i virksomheten. Hvis dere ikke ønsker å investere så mye i sikringstiltak, så anbefaler vi at dere konsentrerer dere om å sikre verdien som ble satt som prioritet 1 – IKT-løsningene. Disse er plassert i et rom i kjelleren uten tilstrekkelig sikring. Estimert verdi for å sikre rommet er 70 000 kr".
6	**Revisjon av sikringsmål:**	"Den minste kostnaden for å sikre deres viktigeste verdi er 70 000 kr. Det er helt opp til dere om dere skal investere i sikringstiltakene, eller om dere skal akseptere risikoen".

5. Konklusjon

Denne masteroppgaven har hatt som formål å kartlegge mulige årsaker som bidrar til at virksomheter ikke sikrer seg mot TUH. De største årsakene til at virksomheter ikke sikrer seg mot TUH er organisatoriske svakheter, der de vanligste sårbarhetene er at det avsettes for lite ressurser til sikkerhet, og at sikkerhet er dårlig forankret i ledelsen. Sikkerhet er et lederansvar, men i undersøkelsen fremkom det at sikkerhet ofte er dårlig forankret i virksomheters ledelse. Det er vanskelig å få ledelsen til å engasjere seg og få eierskap til sikringsprosessen, og spesielt sikringrisikoanalyser. Det hjelper lite med en god og grundig sikringsrisikoanalyse hvis ikke ledelsen deltar. Dette fører til at de ikke får den risikoforståelsen som er nødvendig for å ta gode beslutninger ved valg av strategi for å håndtere risiko. I mange virksomheter tar beslutningsprosessen etter endt risikoanalyse lang tid. Ledere mangler ofte beslutningsevne og handleskraft til å operasjonalisere og implementere anbefalte sikringstiltak. Dette fører til at sikringsprosessen stopper opp. Virksomheter velger ofte sikringsnivå etter minimumskravene til sikkerhet. På bakgrunn av dette overholdes ikke ALARP-prinsippet som innebærer at risiko skal reduseres så langt som mulig, så lenge ikke kostnaden av å implementere sikringstiltaket overstiger nytten. Det er ofte vanskelig for virksomheter å se nytten av sikkerhet mot TUH, og safety prioriteres ofte foran security. Verdien av sikkerhet blir ikke tydelig før den utfordres. Sikringstesting av forebyggende sikringstiltak vil være en måte å vise verdien av sikkerhet, men sikringstesting er så lite utbredt at dette skjer sjeldent. At slike metoder ikke brukes er en mulig årsak som bidrar til at virksomheter ikke sikrer seg.

Denne konklusjonen er basert på mange momenter fra empirifremstilling og drøfting. Disse momentene har jeg oppsummert i Tabell 6.

5.1 Forslag til videre forskning

Det ville vært interessant å gjøre en studie der man sammenligner risikoanalyser der det er brukt sikringstesting med risikoanalyser der dette ikke er brukt, for å sammenligne resultatene av disse. Videre ville det vært spennende å se nærmere på den prosessen som skjer i en virksomhet etter at et konsulentselskap har utført en risikoanalyse. Det blir nevnt i oppgaven at virksomheter ofte er motvillige til å gi konsulentselskaper innsyn i hvilket sikkerhetsarbeid som er gjort etter risikoanalysen. Her går mye potensiell læring og kunnskap tapt ved at

sikkerhetsrådgivere ikke får evaluere og måle effekten på sikringstiltakene som de har anbefalt til virksomheten.

Tabell 6: Funn og antakelser

F2 – Hvordan foregår sikring i dag?		
1	**Manglende involvering og forankring av sikkerhetsarbeid i ledelsen.**	Viktigheten av at sikkerhet er forankret i ledelsen og at ledere involverer seg i risikoanalyser er poengtert flere ganger i intervjuer. Det fremstår som tydelig at det fortsatt er vanskelig å få ledere til å delta i risikoanalyseprosessen og at her er det et stort forbedringspotensiale.
2	**A) Ledelsen i virksomheter har manglende evne til å operasjonalisere risikoanalyser:** **B) Mindre virksomheter – kortere beslutningsvei – implementerer tiltak:**	Ledelsen i virksomheter mangler ofte beslutnings- og gjennomføringsevne til å operasjonalisere risikoanalyser til sikringstiltak. Det at mange objekter av samfunnskritisk betydning fortsatt ikke er sikret mot terror etter 22. juli understreker dette. Det er en stor treghet i systemet. I noen virksomheter ligger alt til rette for at sikringstiltak skal iverksettes, men dette skjer ikke. Ofte skyldes dette økonomiske prioriteringer. Noen mindre virksomheter er overraskende ”fremme i skoene” når det kommer til sikkerhetsarbeid og sikringstiltak. Hvis ledelsen er opptatt av sikkerhet så er ikke beslutningsveien og vurderingsfasen så lang, og det er dermed lettere å få gjennomført sikringstiltak. Videre har mindre virksomheter ikke så store verdier, og de økonomiske konsekvensene av å investere i sikringstiltak blir ikke så store som i de større virksomhetene.
3	**Safety prioriteres foran security og risikoanalyser blir for omfattende:**	Safety prioriteres foran security, og dette gjør risikoanalyser omfattende og utfordrende med tanke på security. Det hadde vært enklere hvis man kunne forholde seg til ren sikkerhet, men det er sjeldent. Konsulentselskaper har ofte plikt til å utføre fullstendige risikoanalyser. Det blir utfordrende for de som skal operasjonalisere de sikkerhetsråd og anbefalinger som er resultatet av risikoanalyser, hvis analysen er for stor og omfattende. Det kan føre til at det er vanskelig å avgjøre hvilke verdier som er viktigst å sikre.
4	**Risikoanalytikere mister kontakt med risikoanalysen:**	De som utfører risikoanalyser for virksomheter mister kontakt med risikoanalysen etter at den er utført. De som har utført risikoanalyse for virksomheter møter ofte motvilje i forhold til det å evaluere hvilke tiltak som er blitt implementert etter analysen og om tiltakene fungerer etter hensikt. Risikoanalytikere vet ofte ikke om det er iverksatt tiltak etter endt analyse. Risikoanalytikere ville lært mer hvis de fikk være med på å evaluere det som skjer etter at de har levert fra seg risikoanalysen.
5	**Manglende bruk av sannsynlighet i NS 5832 ”skremmer ledelsen”:**	Det at NS 5832 tillater at handlinger som etter NS 5814 hadde fått ”lav” sannsynlighet, i NS 5832 får ”høy” risiko, kan skremme ledere fra å benytte denne. Når scenarioer får høy risiko, bør det implementeres tiltak, og dette har ledere motforestillinger i mot i forhold til at det er ”lav” sannsynlighet for at handlingene vil inntreffe etter NS 5814.
6	**Tidsregnskap i risikoanalyser:**	Det viste seg at den beregnede responstiden som ble gjort i risikoanalyser ikke tok hensyn til at reaksjonsstyrker kunne hindres og dermed bruke langt lenger tid til objekt enn det analytikerne anslo.

7	**Lite bruk av sikkerhetstesting av fysiske sikringstiltak:**	Sikkerhetstesting mot IKT-systemer er en vanlig praksis i dag, men det er lite utbredt med inntrengnings- og penetrasjonstesting av fysiske sikringstiltak. Det er et større fokus på reaktive krise- og beredskapsøvelser enn det er på sikringsøvelser og testing av forebyggende tiltak. Sikringstesting vil vise ledelsen i virksomheter "sikkerhetens verdi". Sikkerhetstesting avdekker sårbarheter ved verdiene, og det blir da lettere å prioritere riktige sikringstiltak.
8	**NS 5832 inkluderer ledelsen i sikringsrisikoanalyseprosessen:**	NS 5832 involverer ledelsen i større grad, da ledelsen skal delta i verdivurderingen og sikringsmål, samt revidere sikringsmålene etter endt risikoanalyse. I NS 5832 "må" ledere sette seg inn i sikringsrisikoanalysen og lese den, da den ikke har en visuell fremstilling av risiko.
9	**Manglende rådgivningstilbud i fysisk sikring:**	NSM innrømmer at de ikke har kapasitet til å rådgi mange virksomheter i fysisk sikring. Videre at virksomheter har manglende kompetanse i anskaffelse av fysiske sikringstiltak og at mange trenger uavhengig og profesjonell veiledning for å gjøre riktige valg av tiltak. Slik ekspertise er lite tilgjengelig.
10	**Bedre samarbeid i sikkerhetsfagmiljøet:**	Det har i de senere årene blitt et bedre og mer helhetlig samarbeid mellom ulike fagaktører i sikkerhetsfagmiljøet. Det er blitt et felles fokus på å hjelpe sluttbruker.
11	**PSTs åpne trusselvurdering fremmer iverksettelse av sikringstiltak:**	Det var 66 prosent av virksomhetene som innhentet PSTs åpne trussel som vurderte trusler mot egen virksomhet. Av de virksomhetene som vurderte trusler mot egen virksomehet, så var det 59 prosent av disse som iverksatte sikringstiltak. Det er 6 av 10. Når man så på alle virksomheter som totalt hadde utført risikovurderinger, så var det 4 av 10 som hadde iverksatt tiltak. Det kan tyde på at trusselvurderingen fremmer iverksettelse av sikringstiltak i virksomheter.
12	**Utfordringer med begreper:**	"Risikovurdering, sikringsrisikovurdering, risikoanalyse og sikringsrisikoanalyse" brukes om hverandre. Hvilken betydning begrepene ha uttrykkes ofte ikke eksplisitt i artikler, rapporter og undersøkelser.
13	**Forfalskning av risikoanalyser:**	Et økende krav til utføring av risikoanalyser i virksomheter har ført til at kontrollmyndigheter i større grad avdekker dokumenter som er forfalsket. Videre er det viktig å være klar over at ikke alle virksomheter trenger å gjennomføre risikoanalyser, og disse blir ilagt krav om å gjennomføre dette.
14	**ALARP-prinsippet følges ikke:**	Virksomheter legger seg ofte på et minimums sikringsnivå på grunn av økonomiske- og andre hensyn. Prinsippet om at identifiserte tiltak skal implementeres for å redusere risiko så langt som mulig, såfremt det ikke foreligger et dokumentert misforhold kostnader/ulempe og nytten av tiltaket. Når minimum sikringsnivå brukes i virksomheter så er dette ikke i tråd med ALARP-prinsippet. Betalingsvilligheten i sikkerhet er generelt liten.
15	**NS 5832 forankret i samfunnsvitenskaplig teori:**	NS 5832 bygger på mange av de samme prinsippene som kommer frem i kriminologiske "mulighetsteorier", som rutineaktivitetsteorien og SCP. Det sammenfallende er fokuset på å redusere muligheten for en kriminell handling ved å manipulere verdier og sårbarheter/mål og beskyttere. Mulighetsteoriene fremmer også bruk av sikringstiltak for å redusere risiko for kriminelle handlinger.

16	**Utdanning i security:**	Teoretikere og fagpersoner mener at det er få personer som er utdannet innen securityfaget, og at det er manglende utdanningstilbud i Norge når det gjelder security.
17	**Oppsummering:**	De vanligste organisatoriske sårbarhetene i en virksomhet er at det avsettes for lite ressurser, manglende sikkerhetskompetanse og dårlig forankring i ledelsen. Hvis både ressurser og forankring i ledelsen mangler, så blir grunnsikring ikke tilstrekkelig, og det er tross alt grunnsikringen som skal være det daglige sikkerhetsnivå, men som også skal beskytte virksomheten mot TUH.

6. Litteraturliste

Abrahamsen, E. B. (2010, 21.10). Økonomifaget – en fare for sikkerheten? *Forskning.no*. Hentet fra: http://forskning.no/meninger/kronikk/2010/10/okonomifaget-en-fare-sikkerheten

Johnsen, A., B. (2011, 23.12). Stortinget måtte passe seg selv. *VG*. Hentet fra: http://www.vg.no/nyheter/innenriks/terrorangrepet-22-juli-politikk-og-samfunn/stortinget-maatte-passe-seg-selv/a/10024933/

Johnsen, A., B. (2016, 17.05). Erkjenner hull i terrorsikkerheten. *VG*. http://www.vg.no/nyheter/innenriks/terrorisme/erkjenner-hull-i-terrorsikkerheten/a/23683814/

Andersen, E. (2010). *Fra McKinsey til Grandiosa - når er dyre råd gode?* ISCO Communication. Hentet fra: http://www.iscogroup.no/kunder/isco/iscogroup.nsf/1/10031?open&cat=

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

Aven, T., Røed, W., Wiencke, H. (2008). *Risikosanalyse.* Universitetsforlaget AS.

Aven, T. (2004). *Grunnleggende om risiko, kost-nytte, risikostyring og beslutningstaking.* Forskningsrådet. Hentet fra: http://www.forskningsradet.no/csstorage/vedlegg/153536%20Grunnleggende%20om%20risiko2.pdf

Aven, T. (2007). *Risikostyring.* Universitetsforlaget AS.

Aven, T. (2013). Practical implications of the new risk perspectives. *Reliability Engineering and system safety, vol. 115, s. 136-145.* Hentet fra: http://www.sciencedirect.com/science/article/pii/S0951832013000550

Backe, T. (2015, september). *Hvordan vurderer vi risiko?* Samfunnssikkerhet. Hentet fra:

http://www.samfunnssikkerhetnorge.no/beredskap/hvordan-vurderer-vi-risiko?utm_source=bowsprit

Barane, J., E. (2014). *Kronikk: Et rasjonelt valg – om trefaktortilnærmingen til sikringsrisiko.* Næringslivets sikkerhetsråd. Hentet fra: http://www.proakt.no/et-rasjonelt-valg-om-trefaktortilnaermingen-til-sikringsrisiko/

Boyesen, M. (2003). *Risikopersepsjon – En innføring i fagfeltet*. Direktoratet for sivilt beredskap (DSB). Hentet fra: http://www.dsb.no/Global/Publikasjoner/2003/Tema/risikopersepsjon%20-%20en%20innf%C3%B8ring%20i%20fagfeltet.pdf

Clarke, R., V. 1997. *Situational Crime Prevention: Successful case studies.* Second edition, Guilderland New York. Hentet fra: http://www.popcenter.org/library/reading/pdfs/scp2_intro.pdf

Clarke, R., V. & Felson, M. 1998. *Opportunity makes theif: Practical theory for crime prevention.* Research, Development and Statistics Directorate. Hentet fra: http://www.popcenter.org/library/reading/pdfs/thief.pdf

Cohen, L., E., & Felson, M. (1979), *Social change and crime rate trends: A routine activity approach.* University of Illinois, Urbana.
Hentet fra: http://www.personal.psu.edu/exs44/597b-Comm%26Crime/Cohen_FelsonRoutine-Activities.pdf

Covello, V. T., Mumpower, J. (1985). *Risk Analysis and Risk Management - An Historical Perspective.* Risk Analysis: An International Journal, vol 05, no 2, s. 103-120. Hentet fra: http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.1985.tb00159.x/full

Dagbladet. 2016. *Sikkerhet først*. Hentet (03.05.16) fra: [http://www.dagbladet.no/2016/05/03/kultur/meninger/leder1/dbmener/turoyulykken/44092589/]

Dahl, A., A. (2015). *Sikkerhetskonferansen 2015: Sikkerhetsgraderte anskaffelser.* NSM. https://www.nsm.stat.no/globalassets/dokumenter/sikkerhetskonferansen-2015/graderte-anskaffelser-sikkerhetskonferanse-2015-dahl.pdf

Dalland, O. 2007. *Metode og oppgaveskriving for studenter,* Oslo, Gyldendal Akademiske

Dubreuil, H. G., Bengtsson, P. H., Bourreller, R., Foster, S., Gadbois & Kelly, G. N. (2011). *A report of TRUSTNET on risk governance – lessons learnt.* Journal of Risk Research. Hentet fra: http://www.tandfonline.com/doi/pdf/10.1080/13669870110039916

DSB. (2009). *Kontroll med risiko gir gevinst.* [Brosjyre]. Hentet fra: http://www.dsb.no/Global/Publikasjoner/2008/Andre/risikobrosjyre.pdf

Felson, M. & Clarke, R., V. (1998), *Opportunity Makes the Thief: Practical theory for crime prevention.* Research, Development and Statistics Directorate.
Hentet fra: http://www.popcenter.org/library/reading/pdfs/thief.pdf

FFI. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger.* (00923). Hentet fra: https://www.ffi.no/no/Rapporter/15-00923.pdf

FFI-forum. (18.06.2015). *Må bli bedre på å kommunisere risiko*. Hentet fra: https://www.ffi.no/no/Aktuelle-tema/Sider/M%C3%A5-bli-bedre-til-%C3%A5-kommunisere-risiko.aspx

Flesvik, J., E. (2014). *Om sannsynlighet for terror.* Dagens Næringsliv. Hentet fra: http://www.dn.no/meninger/debatt/2014/12/01/2158/Terror/om-sannsynlighet-for-terror

Gunningham, N., Grabosky, P. and Sinclair, D. (1998). *Smart Regulations: An institutional perspective*». Law and Policy, vol 19, no 4, s. 363-414.

Hoff, G., Krunenes, M. (2013). *Hvordan formidle kvantitative risikoanalyser til offshorearbeidere?* (Mastergradavhandling, Universitetet i Stavanger). Hentet fra: http://brage.bibsys.no/xmlui/handle/11250/184858

Hoffman, J., F. (2015). Samfunnssikkerhet of risikoaksept. *Samfunnssikkerhet*. Hentet fra: http://www.samfunnssikkerhetnorge.no/beredskap/samfunnssikkerhet-og-risikoaksept

Hoffman, J., F. (2015). PST mener demokratiet må tåle terror: - Vi kan ikke overvåke oss til sikkerhet. *NRK*. Hentet fra: http://www.nrk.no/norge/pst-mener-demokratiet-ma-tale-terror-1.12654238

Hughes, S. (2004). *Cost-Effective Application of the ALARP Principle*. Safety Engineering Group. Hentet fra: http://diglib.shrivenham.cranfield.ac.uk/resources/20%20Hughes%20-%20Cost%20Effective%20Application%20Of%20The%20ALARP%20Priciple.pdf

Indrelid, J. (2015). *Bygninger med sikringsbehov – Planllegging av sikre bygg.* (Mastergradavhandling, NTNU Trondheim).

International Organization for Standardization. (2010). *Risk management — Principles and guidelines* (3100:2009). Hentet fra: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode,* Høyskoleforlaget

Johannessen, A., Tufte, P. A., Christoffersen, L. (2010). *Introduksjon til samfunnsvitenskaplig metode.* Abstrakt forlag.

Karlsen, G., R. (2010). *Det regulerte arbeidsmiljø: Implementering av HMS i et differensiert organisasjonslandskap*. Oslo: Universitetsforlaget.

Kystverket. (2016). *Fakta om havnesikring.* Hentet fra: http://www.kystverket.no/Maritim-infrastruktur/Havnesikring/Fakta/

Mandt, Ø. (2015). *Objektsikkerhet i et samfunnsperspektiv.*NSM. Hentet fra: http://www.nbef.no/fileadmin/Kursprogrammer/2015/1550157_Risk_Management/Mandt_Objektsikkerhet_NBEF_seminar_26_11_15.pdf

Mandt, Ø. (2015, 5. Januar). *Grunnsikring er viktigere enn noensinne.* Hentet fra: https://www.nsm.stat.no/blogg/viktig-med-grunnsikring/

Manunta, G. (1997). *Towards a security science through a specific theory and methodology*. Scarman Center for the Study of Public Order: University of Leicester. Hentet fra: https://lra.le.ac.uk/bitstream/2381/27756/1/1997ManuntaGPhD.pdf

Mærli. B., M. (2012). *Risikobasert sikring (security) og risikoreduksjon – Notat 8/2 til 22. juli-kommisjonen.* Det Norske Veritas. Hentet fra: http://docplayer.no/14219493-Notat-8-12-risikobasert-sikring-security-og-morten-bremer-maerli-forsker-det-norske-veritas-risikoreduksjon-08-03-2012-www-22julikommisjonen.html

Mærli, M. B. (2012) *Sårbar sikkerhet*. Stat og Styring, volum 22. Hentet fra: https://www.idunn.no/stat/2012/02/saarbar_sikkerhet

Mærli, M., B. (2014). *Usanssynlig sannsynlig.* Dagens Næringsliv. Hentet fra: http://www.dn.no/meninger/debatt/2014/11/23/2058/Terror/usannsynlig-sannsynlig

NOU 2000:24. (2000). *Et sårbart samfunn — Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Regjeringen. Hentet fra https://www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/?q=&ch=1

NSM. (2016). *Risiko 2016: Kan sikkerhet styres?*. Hentet fra: http://www.nsr-org.no/getfile.php/Dokumenter/Eksterne%20publikasjoner/nsm_risiko_2016.pdf

NSM. (2015). *Veileder i sikkerhetsstyring.* Hentet fra: https://nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf

NSM, PST, POD. (2015). *Terrorsikring: En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger.* Hentet fra: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder_terrorsikring_2015_enkelts_final.pdf

NSM. (2012). *Veileder for objektsikkerhetsforskriften*. Hentet fra: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-objektsikkerhet-v1.1.pdf

NSM. (2012). *Årsmelding 2011*. Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/arsrapporter/arsmelding_nsm_2011_video.pdf

NSM. *Åpnet testrikk i dag*. Hentet fra: https://www.nsm.stat.no/aktuelt/apning-simlab/

NSM. (2016). *Risikovurdering for sikring.* Hentet fra: https://www.nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf

NSM (2014). *Veileder i objektsikkerhetsforskriften*. Hentet fra: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-for-objektsikkerhetsforskriften-1.2.pdf

NSM. (2014, 6. Januar). *Støtter forskning om objektsikekrhet.* Næringslivets sikkerhetsråd. Hentet fra:

http://www.nsr-org.no/aktuelle-saker/stoetter-forskning-om-objektsikkerhet-article399-110.html

NSR. (2015). *Kriminlaitets- og sikkerhetsundersøkelsen i Norge (Krisno).* Hentet fra: http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/Krisino/krisino_2015_utskrift.pdf

NSR. (2015). *En strategisk kriminalitetsanalyse basert på Krisno 2015.* Hentet fra: http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/Veiledninger%20og%20orienteringer/kriminalitetsanalyse_utskrift.pdf

Nilsen, K. (2015). S*ikkerhetsfaglig råd*. NSM. Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/nsm-sikkerhetsfaglig_raad_2015_web.pdf

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

PST. (2014). *Åpen trusselvurdering 2014.* Politiets sikkerhetstjeneste. Den sentrale enhet. Hentet fra: http://www.pst.no/media/67044/PSTs_tv2014.pdf

Rapp, C., Endragard, M., Maal, M., Riis, L., D. (2015). *Må bli bedre på å kommunisere risiko*. FFI-forum. Hentet fra: http://www.ffi.no/no/Aktuelle-tema/Sider/M%C3%A5-bli-bedre-til-%C3%A5-kommunisere-risiko.aspx

Rapp, C. (2014). *Terror vanskelig å forutse.* Dagens Næringsliv. Hentet fra: http://www.dn.no/meninger/debatt/2014/11/24/2159/Terror/terror-vanskelig--forutse

Rausand, M., & Utne, I., B,. (2009). *Risikoanalyse – teori og metoder.* Trondheim: Tapir akademisk forlag.

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

Ringdal, K. (2013). *Enhet og mangfold.* Fagbokforlaget.

Schermerhorn, R., J. (2007). *Management.* Ninth Edition. Wiley
Hentet fra: http://www.differencebetween.net/business/difference-between-management-and-governance/

Sennewald, A., T. (2011). *Effective Security Management*. Fifth edition. Elsevier Inc.

Sikkerhetsloven. (2015). *Lov om forebyggende sikkerhetstjeneste.* Hentet fra: https://lovdata.no/dokument/NL/lov/1998-03-20-10

Simonsen, A. R. (2016). Sikkerhet er et konkurransefortrinn! *Næringslivets sikkerhetsråd*. Hentet fra: http://www.nsr-org.no/aktuelle-saker/sikkerhet-er-et-konkurransefortrinn-article767-110.html

Sætersmoen. (2014, 22. oktober). *Hvor godt er norske virksomheter forberedt på terror eller andre alvorlige handlinger?* Hentet fra: https://www.nsm.stat.no/blogg/hvor-godt-er-norske-virksomheter-forberedt-pa-terror-eller-andre-alvorlige-kriminelle-handlinger/

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

Standard Norge. (2014). Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikostyring. *Norsk Standard (NS) 5831:2014.*

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

Terrorangrepet 11. september 2001. (2015). *Store Norske Leksion.* Hentet fra: https://snl.no/Terrorangrepet_11._september_2001

Terrorangrepene i Norge 2011. (2015) *Store Norske Leksion*. Hentet fra: https://snl.no/Terrorangrepene_i_Norge_2011

van Asselt, M. B. A., Renn, O. (2011). *Risk Governance*. Journal of Risk Research. Hentet fra: http://www.tandfonline.com/doi/pdf/10.1080/13669877.2011.553730

7. Vedlegg

Vedlegg A - Sentrale aktører

For å få en oversikt over hvilke aktører som er mest fremtredende og hvilket arbeid de har bidratt med i securityfagfeltet, er disse nevnt under. I denne oppgaven er de mest sentrale aktørene sikkerhetsmyndigheter, institusjoner, forskningsgrupper og enkeltpersoner med kunnskap om og en form for funksjon i securityfagfeltet i Norge. De aktørene som er mest sentrale i oppgaven er listet opp under, samt relevant litteratur disse aktørene har utarbeidet:

Politiets sikkerhetstjeneste (PST) er en del av den norske politietaten og er direkte underlagt Justisdepartementet. PSTs primæroppgave er å forebygge og etterforske kriminelle handlinger mot rikets sikkerhet, hvorav terrorisme, spionasje og organisert kriminalitet er de mest alvorlige handlingene. PST gir årlig ut en *"Trusselvurdering"*, der det årlige og aktuelle trusselbildet i Norge presenteres. PST har sammen med Nasjonal sikkerhetsmyndighet (NSM) og Politidirektoratet (POD) vært med på å utarbeide og utgi veilederen "*Terrorsikring"*(2015). Denne veiledningen er ment for å veilede virksomheter som ikke er underlagt sikkerhetsloven i hvordan de skal sikre seg mot terrorisme. Veiledningen blir betegnet som et "verktøy" som gir retningslinjer for forebyggende sikkerhetsarbeid. Det presiseres i veiledningen at den også kan brukes mot andre kriminelle handlinger.

Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet og er administrativt underlagt Forsvarsdepartementet. NSM har en rekke oppgaver. En av de viktigste oppgavene er rådgivning og veiledning i forhold til de virksomheter, organisasjoner, departementer og myndigheter som trenger det blant annet innenfor datasikkerhet, personellsikkerhet og objektsikkerhet. Eksempler på tjenester som NSM tilbyr er sikkerhetsanalyser, fysisk sikring, inntrengingstester og informasjonssikkerhet. NSM er en stor aktør i sikkerhetsfagfeltet i Norge, og står for en rekke publikasjoner og veiledninger som søker å fremme godt sikkerhetsarbeid i virksomheter. For denne oppgaven er de viktigste publikasjonene: *"Veiledning i sikkerhetsstyring"*(2015)*, "Veiledning i*

verdivurdering"(2009), *"Veileder for i objeksikkerhetsforskriften"*(2014), *"Risiko"*(2016), *"Veiledning i objektsikkerhet"* og "*Risikovurdering for sikring"*(2016).

Forsvarets forskningsinstitutt (FFI) er et tverrfaglig institutt som jobber innenfor en rekke akademiske disipliner, deriblant matematikk, økonomi, statsvitenskap, medisin og fysikk. FFI har utarbeidet rapporten "*Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger"*(2015). Denne rapporten ble skrevet etter anmodning fra Forsvarsbygg med den hensikt å vurdere forskjellige tilnærminger til risikovurdering mot tilsiktede uønskede handlinger. I rapporten er det lagt spesielt vekt på standardene NS 5814 og NS 5832.

Forsvarsbygg (FB) er Norges største offentlige eiendomsaktør og er engasjert innen bygging drift, utleie og salg av eiendom. På oppdrag fra Forsvarsdepartementet forvalter, drifter og vedlikeholder mesteparten av alle bygg og anlegg som det norske Fosvaret bruker. FB etablerte i 2012 Nasjonalt kompetansesenter for sikring av bygg (NKSB) som statens rådgiver for beskyttelse og sikring av eiendom, bygg og anlegg mot eksplosjonsulykker, spionasje, kriminalitet og terrorhandlinger. De tjener i hovedsak Forsvaret, men gir også rådgivning i privat og offentlig sektor. NKSB er en egen enhet i FB og er oppdragsfinansiert. og leverer også rådgivningstilbud til offentlig og privat sektor.

Næringslivets sikkerhetsråd (NSR) ble opprettet av sentrale organisasjoner i næringslivet for å bekjempe kriminalitet i og mot næringslivet, og er en medlemsorganisasjon. De jobber gjennom et samarbeid mellom politiet, sikkerhetsmyndigheter og næringslivet. NSR gir råd til virksomheter om sikringstiltak mot blant annet terrorisme, spionasje, organisert kriminalitet, bedrageri og korrupsjon. NSR er også en arena for kompetanseutvikling, de arrangerer blant annet en rekke kurs og konferanser. NSR har gitt ut en rekke publikasjoner og undersøkelser som for eksempel "*Kriminalitet- og sikkerhetsundersøkelsen i Norge*" (KRISNO). KRISNO er en kvantitatv undersøkelse som har blitt utført og publisert syv ganger i tidsrommet 2006-2015. De er basert på spørreundersøkelser hvor utvalget er ledere og sikkerhetsansvarlige i 2500 offentlige (500) og private (2000) virksomheter. KRISNO er utført i samarbeid med OPINION som er et selskap som blant annet leverer meningsmålinger og markedsanalyser.

Direktoratet for samfunnssikkerhet og beredskap (DSB) har ansvar for samfunnssikkerheten som omfatter nasjonal, regional og lokal beredskap og trygghet. DSB er direkte underlagt Justis- og beredskapsdepartementet og fører tilsyn med beredskapsarbeidet i departementene. DSB har mange oppgaver. Noen av dem er å utarbeide et nasjonalt risikobilde, planlegge og gjennomføre øvelser, samt innføre tiltak for å bedre samfunnssikkerheten. Rapporten *"Nasjonalt Risikobilde"* (2015) tok blant annet for seg skoleskyting og tiltak mot dette.

Norsk Standard har enerett på å publisere og fastsette norske standarder. Det er høyt kvalifiserte fagpersoner som er med i et utvalg der standarden utarbeides. I denne oppgaven er det Norsk Standard (NS) 5814:2008 og NS 5832:2014 som er mest aktuelt. Man kan se på standardene som regler og bestemmelser for hvordan risikovurderinger bør foregå som en prosess. To andre standarder som tilhører NS 5832 er NS 5830 og NS 5831. Samlebetegnelsen på disse tre standardene er NS 583X-serien, og vil bli gjennomgått senere i oppgaven.

Vedlegg B - Sentrale fagpersoner i sikkerhetsmiljøet

Morten Bremer Mærli	Stortingets Administrasjon	Stortinget
Roy Stranden	Director of Security/CSO	Schibsted Media Group
Terje Aven	Professor	Universitetet i Stavanger (UiS)
Carsten Rapp	Avdelingsdirektør for Avdeling for sikkerhetsstyring	Nasjonal sikkerhetsmyndighet (NSM)
Thomas Haneborg	Seniorrådgiver	Politiets sikkerhetstjeneste (PST)
Kjetil Nilsen	Direktør	Nasjonal sikkerhetsmyndighet (NSM)
Joakim Barane	Seniorrådgiver og seksjonsleder security risk management	Falck Nutec
Stein Ove Bakke-	Seniorrådgiver	Nasjonalt kompetansesenter for

Hanssen		sikring av bygg, Forsvarsbygg (NKSB)
Ann Karin Midtgaard	Seniorrådgiver i Enhet for analyse	Direktoratet for Samfunnssikkerhet og Beredskap (DSB)
Maren Maal	Forsker	Forsvarets forskningsinstitutt
Willy Røed	Konsulent	Proactima
Sissel Haugdal Jore	Førsteamanuensis og leder av SEROS	Universitetet i Stavanger (UiS)
Øyvind Mandt	Seksjonssjef	Nasjonal sikkerhetsmyndighet (NSM)
Eli Sætersmoen	Daglig leder	Falck Nutec
Audun Vestli	Spesialrådgiver	COWI

Vedlegg C - Definisjoner i NS 583X-serien

1. Sikkerhet: reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare

2. Sikring: bruk av sikringstiltak ved håndtering av risiko forbundet med tilsiktede uønskede handlinger.

3. Uønsket hendelse: hendelse som kan utsette en verdi for en uønsket påvirkning.

Tilsiktet uønsket handling: uønsket hendelse som forårsakes av en aktør som handler med hensikt.

4. Sikringstiltak: tiltak for å redusere risiko forbundet med tilsiktede uønskede handlinger.

5. Grunnsikring: sikringstiltak som ivaretar en entitets sikringsbehov ved normaltilstand.

6. Teknologisk sikringstiltak: fysisk, elektronisk eller logisk sikringstiltak.

7. Fysisk sikringstiltak: fysisk barriere som hindrer eller forsinker uønsket adgang til verdier.

8. Elektronisk sikringstiltak: tiltak som bruker elektroteknisk utstyr og løsninger for å støtte, supplere eller erstatte fysiske sikringstiltak.

9. Logisk sikringstiltak: tiltak for sikring av informasjon som lagres eller overføres elektronisk.

10. Organisatorisk tiltak: tiltak i form av skriftelige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, rutiner, adferd og/eller anvendelse av andre sikringstiltak.

11. Menneskelig sikringstiltak: tiltak som påvirker persepsjon, vurderingsevne, kunnskap, adferd og reell evne til å bruke teknologiske sikringstiltak og følge organisatoriske sikringstiltak.

12. Beredskap: forberedt evne til på kort varsel å kunne øke sikkerhetsnivå, håndtere en uønsket hendelser eller tilstand, eller evne til å gjenopprette tilfredsstillende tilstand etter en uønsket hendelse eller tilstand.

13. Beredskapstiltak: forberedt tiltak som på kort varsel kan iverksettes for å øke sikkerhetsnivå, håndtere en uønsket hendelse eller tilstand, eller gjenopprette tilfredsstillende tilstand etter en uønsket hendelse eller tilstand.

14. Verdi: ressurs som hvis den blir utsatt for en uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen.

15. Verdivurdering: kartlegging og rangering av en entitets verdier.

16. Fare: mulig handling eller forhold som kan føre til en uønsket hendelse.

17. Trussel: mulig uønsket handling som kan gi negativ konsekvens for en entitets sikkerhet.

18. Reell trussel: trussel forbundet med en entitet som har en kjent intensjon og kapasitet til å true en annen entitets sikkerhet.

19. Potensiell trussel: trussel forbundet med en entitet som har en mulig intensjon eller kapasitet til å true en annen entitets sikkerhet.

20. Trusselaktør: entitet som forbindes med en trussel.

21. Trusselytring: ytring av intensjon om å skade eller på annen måte påvirke en entitet negativt, og som er egnet til å fremkalle frykt eller engstelse hos mottakeren.

22. Trusselutøver: entitet som fremsetter en trusselytring.

23. Trusselbilde: tidsavgrenset beskrivelse av identifiserte trusler mot en bestemt entitet.

24. Trusselvurdering: beskrivelse av en entitets trusselbilde og en vurdering av trusselaktørens intensjon og kapasitet.

25. Intensjon: vilje og hensikt til å utføre en handling.

26. Kapasitet: evne, herunder ressurser, kunnskap og ferdighet, til å utføre en handling.

27. Sårbarhet: manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for en uønsket påvirkning.

28. Sårbarhetsvurdering: vurdering av en entitets sårbarhet overfor identifiserte trusler.

29. Risiko: uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen.

30. Risikobilde: tidsavgrenset beskrivelse av en entitets risiko.

31. Risikovurdering: helhetsvurdering basert på verdivurdering (eller konsekvensvurdering), trusselvurdering og sårbarhetsvurdering, med mål om å angi en entitets risiko i en definert sikringsmessig kontekst.

32. Risikohåndtering: tiltak som gjennomføres for å oppnå akseptabel grad av identifisert risiko.

33. Konsekvensvurdering: vurdering av de potensielle konsekvensene for å en eller flere verdier dersom en uønsket hendelse skulle inntreffe.

34. Skadevurdering: vurdering av de negative konsekvensene for en eller flere verdier som følge av at en uønsket hendelse har inntruffet.