Risikostyring og sikkerhetsledelse

Masteroppgave

Innsiderisiko – hvordan påvirker sikkerhetsklarering vurderingen?

Skrevet av: Merete Hove

Universitetet i Stavanger – 2022

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I
RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER:

Vår/Høst 2022

FORFATTER:

Merete Hove

VEILEDER:

Jon Tømmerås Selvik

TITTEL PÅ MASTEROPPGAVE:

Innsiderisiko – hvordan påvirker sikkerhetsklarering vurderingen?

EMNEORD/STIKKORD:

innsider, innsiderisiko, innsidetrussel, risikovurdering, sikkerhetsklarering

SIDETALL:
71

STAVANGER ……2022-10-15…….
DATO/ÅR

FORORD

Hvis du leser dette, betyr det at jeg klarte å komme i mål med denne oppgaven og at den ble levert inn i tide. Oppgaven markerer slutten på nesten tre år med studier, i kombinasjon med full jobb. Dette var noe jeg overhodet ikke hadde sett for meg da jeg etter mange år i arbeidslivet startet med et fag, Risikoanalyse, for å få faglig påfyll og lære noe nytt.

Tusen takk til min arbeidsgiver som ga meg denne muligheten, og til kollegaer som har trodd på at jeg ville klare det. En spesiell takk til de to som hjalp meg med å holde motet oppe helt til siste slutt og som bidro med uvurderlige innspill og korrekturlesing den siste perioden, min gode venn og kollega, Anja, og min kjære bror og kollega, Tomas.

Det har vært en utrolig læringsrik og givende periode, med både opp- og nedturer underveis. Gjennom en pandemi med lange perioder på hjemmekontor ble det mange timer på samme sted foran PCen, og en spesiell takk rettes til de jeg jobbet sammen med på gruppeoppgaver underveis. Det var både strevsomme, lærerike og inspirerende timer og kvelder sammen på Teams.

Jeg ønsker å takke Jon Tømmerås Selvik som var min veileder på denne oppgaven. Jeg kunne vært flinkere til å holde kontakten underveis, men er takknemlig for de råd og innspill jeg fikk. Det var nok ikke enkelt å være min veileder når jeg har hadde så mange tanker i hodet og oppgaven dreide i en helt annen retning enn det som var utgangspunktet.

Jeg må også få takke venner og familie som hadde troen på at jeg skulle lykkes, og som har ventet tålmodig på sidelinja mens jeg har prioritert studier. Nå er jeg klar for å være sosial igjen, og det gleder jeg meg skikkelig til.

Den siste og aller største takken går til den gode støtten jeg har fått fra min datter og hennes far, Mona og Johnny. «*Enten går det bra, eller så går det over*» - og selv om *jeg* store deler av tiden har trodd noe annet, så gikk det faktisk bra.

Merete

SAMMENDRAG

Innsiderisiko har flere ganger blitt trukket fram av Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten (E-tjenesten) som en risiko med stort skadepotensial for både norske virksomheter og nasjonale sikkerhetsinteresser. Dette var tema også under en av debattene på NSMs sikkerhetskonferanse i mars 2022. Der ble spørsmålet stilt om sikkerhetsklarering er et tiltak som burde innføres for andre områder enn de som i dag omfattes av sikkerhetsloven. Sikkerhetsklarering er et kraftig virkemiddel og anses som den beste screening vi har av personer i Norge.

På denne konferansen var det forskning og sensitiv informasjon på universiteter som var tema, men dette kan overføres også til andre områder i samfunnet hvor viktige verdier håndteres og hvor det er risiko for at en person på innsiden kan påføre skade eller tap. På bakgrunn av dette har følgende problemstilling blitt studert: «*Hvordan kan bruk av sikkerhetsklarering påvirke vurderingen av innsiderisiko?*»

Denne problemstillingen besvares gjennom en litteraturstudie som har omfattet både fakta og empiri, samt drøfting av funnene i forhold til et teoretisk grunnlag i elementene som inngår i risikostyring og risikovurdering.

Studien har hatt en helhetlig tilnærming til innsidehandlingene som resulterer i skade og tap for en virksomhet. Innsidehandlingen som utløser en uønsket hendelse kan være ubevisst, bevisst, men med utilsiktet konsekvens, eller bevisst og med tilsiktet konsekvens. I alle disse tilfellene vil innsideren være enhver person som har eller har hatt tilgang til organisasjonens verdier.

Funn har vist at det er roller som bør være analyseobjektet når innsiderisiko vurderes i en virksomhet og at det er viktig å holde seg nøytral i forhold til hvem som innehar rollen for å styre klar av unøyaktigheter i analysen.

Det konkluderes med at det er samspillet mellom klareringsmyndighetens sikkerhetsklarering og virksomhetens oppfølging med autorisasjon og sikkerhetsmessig ledelse og kontroll som er det sterkeste virkemiddelet i forhold til å forebygge og motvirke uønsket innsideaktivitet.

INNHOLDSFORTEGNELSE

TABELLER

FIGURER

FORKORTELSER

Tabell 1 Forkortelser

Forkortelse	Beskrivelse
DSB	Direktoratet for samfunnssikkerhet og beredskap
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
CPNI	Centre for the Protection of National Infrastructure
DNV GL	Det norske Veritas og Germanischer Lloyd
DoD	Department of Defense
E-tjenesten	Etterretningstjenesten
EOS-utvalget	Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste
FFI	Forsvarets forskningsinstitutt
FSA	Forsvarets sikkerhetsavdeling
ISO	International Organization for Standardization
NATO	North Atlantic Treaty Organization
NOU	Norges offentlige utredninger
NS	Norsk Standard
NSM	Nasjonal sikkerhetsmyndighet
NSR	Næringslivets Sikkerhetsråd
NTNU	Norges teknisk-vitenskapelige universitet
PST	Politiets sikkerhetstjeneste
Ptil	Petroleumstilsynet
SEI	Software Engineering Institute
SKM	Sivil klareringsmyndighet
U.S.	United States
USA	Unites States of America
VTS	Verdi, Trussel, Sårbarhet

1 INNLEDNING

1.1 Bakgrunn

Innsiderisiko har ved flere anledninger blitt trukket fram av Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten (E-tjenesten) som en risiko med stort skadepotensial for både norske virksomheter og nasjonale sikkerhetsinteresser, og virksomheter oppfordres til å innarbeide innsiderisiko i sine risikovurderinger. «De beste kildene er personer som har tilgang til verdiene fra innsiden av virksomheten» skrev Erik Nyblom (2021), fagdirektør i NSM, i en kronikk i Dagens Næringsliv med henvisning til etterretningstjenestenes rekruttering eller plassering av spioner på innsiden av norske virksomheter.

Fremmede etterretningstjenester bruker store ressurser på å skaffe seg tilgang til informasjon eller andre verdier som er av betydning for den aktuelle staten, dette kan for eksempel være informasjon om norske beslutningsprosesser eller teknologi. En av framgangsmåtene som benyttes er rekruttering av både norske borgere og statens egne borgere bosatt i Norge som har tilgang til verdiene fra innsiden av en virksomhet (Meld. St. 5 (2020-2021), s. 77). Både NSM (NSM, 2022d), PST (PST, 2022) og E-tjenesten (Etterretningstjenesten, 2022) har fokus på at Norge er lang framme teknologisk på flere viktige områder som maritim-, forsvars-, romfarts- og petroleumsvirksomhet og dette er områder som også andre land forsøker å utvikle og som de derfor har interesser i. Norske forsknings- og utdanningsinstitusjoner er spesielt attraktive for utenlandske forskere fordi de i tillegg til å holde et høyt internasjonalt nivå, gir tilgang til laboratorier og forskningsinfrastruktur, og det er gode finansieringsordninger. Finansiering av og deltakelse i forskningsprosjekter er blant de tiltakene som etterretningstjenester fra fremmede stater benytter seg av for å få tilgang på kunnskap, informasjon og teknologi.

På Sikkerhetskonferansen mars 2022 (NSM, 2022c) holdt Tor Grande, prorektor ved Norges teknisk-vitenskapelige universitet (NTNU), et innlegg om dilemmaet mellom den akademisk friheten og sikkerhet innen akademia. Foredraget satte lys på utfordringer med balansen mellom kunnskapsdeling, eksportkontroll og nasjonale trusselvurderinger. Statististikken (Sarpebakken & Steine, 2022) viser at det ikke utdannes mange nok i Norge til å fylle forskerstillingene og det er derfor nødvendig å rekruttere utenlandske kandidater i stor grad. Tall viser at av de 1601 doktorgradene som ble avlagt i 2021 var 44% utenlandske

disputanter, noe som er den høyeste prosentandelen noensinne. De fleste utenlandske var innenfor områdene matematikk og naturvitenskap med 63% og teknologi med 60%.

Under den etterfølgende paneldebatten på Sikkerhetskonferansen 2022 (NSM, 2022b) stilte PST-sjef Hans Sverre Sjøvold spørsmål om sikkerhetsklarering bør innføres som en nødvendighet for å få lov til å jobbe med forskning som omfatter sensitiv informasjon, også på universiteter.

Som et forebyggende sikkerhetstiltak er sikkerhetsklarering aller mest effektiv i forhold til de som ikke innvilges en klarering og som av den grunn aldri får tilgang til skjermingsverdige verdier. Ifølge EOS-utvalget (2022) var det i 2021 2,4% som fikk negativt svar på sin klareringssøknad, hvilket betyr at de aller fleste av de som søker om en sikkerhetsklarering blir funnet sikkerhetsmessig skikket til å få tilgang til sikkerhetsgradert informasjon. Anders Bakke (2019) reflekterer over godheten og effekten av det å sikkerhetsklarere en person sett opp imot hvor få som ender med en negativ avgjørelse i sin artikkel om *sikkerhetsklarering som virkemiddel*. Bakke stiller også spørsmål ved tiltakets effekt i forhold til inngrep i den enkeltes personvern i forhold til hvor mye granskning av sitt privatliv enkeltpersoner skal måtte tåle i sikkerhetens interesse. Han er samtidig tydelig på at det er beslutning om iverksettelse av personkontrollen som er det avgjørende i forhold til personvernet, ikke selve klareringsavgjørelsen.

Ved å innføre sikkerhetsklarering på områder hvor dette ikke tidligere har vært et krav kan det føre til konsekvenser en ikke klarer å forutse. Det vil være noen som ikke kan få en sikkerhetsklarering, og av den grunn ikke vil få tilgang til informasjon hvor sikkerhetsklarering settes som et krav. Dette kan oppleves som urettferdig når årsaken er at personen har sårbarheter som kan utnyttes, og at det ikke skyldes noe kriminelt (Nyblom, 2021).

Sikkerhetstiltak etablert for å forebygge eksterne trusler mister ofte sin effekt om det er en på innsiden som med sine tilganger bevisst eller ubevisst skaffer den eksterne aktøren informasjon eller tilgang til verdiene og det oppfordres til å innarbeide vurdering av innsiderisiko i virksomhetens risikovurderinger (Meld. St. 5 (2020-2021), s. 77). Denne oppfordringen sammen med et ønske om å utvide bruken av sikkerhetsklarering til nye områder gjør det interessant å studere hvordan bruk av sikkerhetsklarering vil kunne påvirke innsiderisikovurderingen. Innsiderisikoen som virksomheter utsettes for anses som svært kompleks og derfor utfordrende både å vurdere og redusere. Risikoen kan være statisk ved at

det alltid vil finnes personer med tilgang til virksomhetens verdier, og som kan skade verdiene for eksempel ved svindel eller tyveri, og samtidig er den dynamisk ved at en persons motivasjon, prioritering og lojalitet i forhold til virksomheten kan endres (NSM, 2019d, ss. 9-10). Kompleksiteten og skadepotensialt er noe av grunnlaget for at regjeringen vil «øke den forskningsbaserte kunnskapen om motvirkning av innsiderisikoen» (Meld. St. 5 (2020-2021), s. 69).

1.2 Problemstilling

Innsiderisiko blir trukket fram i nasjonale trussel- og risikovurderinger som en risiko med potensielt store skadefølger, og det oppfordres til at innsidetrusselen tas på alvor og tas inn i virksomhetens risikovurderinger. Tiltak som kan benyttes for å forebygge uønskede innsidehandlinger er blant annet bevisstgjøring og oppfølging av personer som har tilgang til en virksomhets verdier. For virksomheter som er underlagt sikkerhetsloven benyttes også sikkerhetsklarering og autorisasjon for å hindre at personer med sårbarheter som kan utnyttes, får tilgang til sikkerhetsgradert informasjon. Sikkerhetsklarering er et velkjent forebyggende sikkerhetstiltak og anses å være myndighetenes «skarpeste våpen» i arbeidet med å hindre at en person som kan være eller er utsatt for å bli en innsider, gis tilgang til informasjon (Bakke, 2019, s. 82).

Sofie Nystrøm (NSM, 2022a), direktør for NSM, uttrykte under Sikkerhetskonferansen 2022 at det kan være nødvendig å tenke nytt i forhold til personell- og innsiderisiko og bruk av sikkerhetsklarering. Det vil være viktig framover å ha gode mekanismer for å ta inn ansatte med riktig profil i sentrale norske virksomheter. Dette må ses på i den nye sikkerhetspolitiske konteksten, og spesielt i forhold til Kina og Russland.

Sikkerhetsklarering er i dag forbeholdt de områder som sikkerhetsloven omfatter, men sett i forhold til en mulig utvidet bruk av sikkerhetsklarering på flere områder, kan en undersøkelse av hvordan dagens praksis påvirker vurderinger av risiko for innsidere være et bidrag i debatten og vurderingene framover.

Dette leder fram til oppgavens problemstilling:

- *Hvordan kan bruk av sikkerhetsklarering påvirke vurderingen av innsiderisiko?*

Det er i tillegg etablert tre forskningsspørsmål som skal bidra til å belyse denne problemstillingen:

1. Hvordan defineres en innsider?
2. Hvordan vurdere innsiderisiko i en virksomhet?
3. Hvilken effekt har sikkerhetsklarering på vurdering av innsiderisiko?

For å kunne besvare problemstillingen er det først nødvendig å innhente kunnskap om hvordan en innsider kan defineres. Definisjonen av en innsider kan ha innvirkning på hvordan innsiderisikoen vurderes og selv om sikkerhetsloven har fokus på sikkerhetstruende virksomhet, som i tilsiktede hendelser, kan risiko for at en person på innsiden forårsaker en hendelse med uønskede konsekvenser strekke seg ut over dette omfanget. Deretter må hvilke faktorer som bør være med i vurdering av innsiderisiko i en virksomhet avklares samt en metode for vurdering av innsiderisiko som ivaretar de identifiserte faktorene.

Til slutt kan kunnskapen fra de to første spørsmålene anvendes for å undersøke hvilken effekt sikkerhetsklarering kan ha på vurderingen av innsiderisiko. Sikkerhetsklarering anses som et av de beste tiltakene i forhold til forebyggende personellsikkerhet (NSM, 2011, s. 1), og sikkerhetsklarering er sannsynligvis «det beste ”screeningsverktøyet” av ansatte som finnes i Norge i dag» (NSM, 2011, s. 6).

1.3 Formål

Målet med denne oppgaven er å øke kunnskapen om *sikkerhetsklarering som et tiltak for å redusere innsiderisiko*. Denne kunnskapen kan være nyttig hvis utvidet bruk av sikkerhetsklarering skal vurderes i samfunnet utover omfanget av dagens sikkerhetslov.

Oppgaven vil også ta for seg metode som en virksomhet kan benytte ved vurdering av innsiderisiko.

1.4 Tidligere forskning

Det er ennå begrenset hvor mange offentlig tilgjengelige studier som finnes i Norge i forhold til innsidere. Av tilgjengelig informasjon som er benyttet som underlag til oppgaven kan nevnes:

- *Temarapport om innsiderisiko* (NSM, 2019d)
- *Grunnprinsipper for personellsikkerhet* (NSM, 2021)
- Veilederen *Sikkerhet i ansettelsesforhold - før under og ved avvikling* (PST et al., 2017)

Disse publikasjonene har fokus på tiltak som kan iverksettes (hva som kan gjøres) og hvorfor.

- *Håndtering av innsiderisiko* (DNV GL, 2019)

En prosjektrapport på oppdrag fra Petroleumstilsynet.

Av tidligere forskning i tilknytning til temaet finnes det et utvalg norske masteroppgaver:

- *Insider Threat* (Syvertsen, 2007)
- *The Norwegian Downsizing Approach in Terms of the Insider Threat - An interpretive study* (Benjaminsen, 2017)
- *Sikkerhetsstyringens utvikling* (Ringstad, 2020)
- *Hvordan holde innsidere på utsiden?* (Jacobsen, 2021)

1.5 Avgrensning

Denne oppgaven vil avgrense seg til personen som er på innsiden og tar ikke for seg eksterne trusselaktører som står bak en eventuell påvirkning fra utsiden i form av press, fristelser, manipulasjon eller annen form for utnyttelse for å oppnå egne mål. Den eksterne aktøren omtales i oppgaven som *tredjepart*.

Oppgaven tar ikke for seg de bakenforliggende årsakene til hvorfor eller hva som motiverer en person til å bli en ondsinnet innsider. Dette er et tema som blant annet Julie Dahl Jacobsen (2021) ser på i sin masteroppgave «Hvordan holde innsidere på utsiden?».

Denne oppgaven forholder seg til dagens sikkerhetsklareringsregime uten å stille spørsmål med hvilke data som innhentes og vurderes eller kriterier som benyttes for vurdering. Den vil heller ikke stille spørsmål med hvordan klareringsmyndigheten utfører sitt virke, men forholder seg til EOS-utvalgets rapporter etter oppfølging.

Oppgaven vil heller ikke ta for seg vurdering av den inngripen en klareringsprosess er i forhold til individets rettssikkerhet og hensynet til nasjonale sikkerhetsinteresser. Dette er et tema som belyses i artikler av Anders Bakke (2017) og Hans Petter Graver (2021). Oppgaven forholder seg til at det er pålagt å iverksette sikkerhetsklarering.

1.6 Oppgavens oppbygning

Kapittel 1: Beskriver oppgavens bakgrunn, problemstillingen og annen relevant forskning på området.

Kapittel 2: Gir en introduksjon til relevante teorier og begreper som benyttes i drøftingen

Kapittel 3: Beskriver valg av metode for studien, forskningsdesign, datainnsamling og -analyse, validitet og etiske refleksjoner.

Kapittel 4: Presenterer funn fra litteraturstudiene.

Kapittel 5: Drøfter funn fra litteraturstudier opp mot valgt teori.

Kapittel 6: Oppgavens konklusjon og forslag til videre arbeid.

2 TEORI

I dette kapitlet gjøres det rede for teorier og begreper som benyttes senere i oppgaven for å belyse problemstillingen. Det starter helt grunnleggende med å se på definisjoner for sikkerhet og deretter følger flere begreper som inngår når risiko skal vurderes, som bl.a. perspektiver på risiko, risikostyring, risikovurdering og risikoanalyse. I tillegg presenteres her tidligere forskning som har relevans for oppgaven.

Hensikten er å gi kunnskap som danner grunnlag for drøfting av de empiriske dataene.

2.1 Sikkerhet

Engen et al. (2016, s. 26) hevder at sikkerhet er et begrep som har flere definisjoner og dimensjoner. Sikkerhet som følelse er det å føle seg sikker og trygg, mens det å være i sikkerhet, eller å definere et system som sikkert er beskrivelse av en faktisk tilstand. En sikker tilstand kan påvirkes av faktorer utenfra som endring i farer og trusler og samtidig kan endringer i systemets beskyttelsesmekanismer (barrierer) føre til økt sårbarhet og redusere graden av sikkerhet. Samtidig påpeker Smith og Brooks (2013, s. 7) og Jore (2019, s. 168) at sikkerhet i tillegg kan ses på som en prosess for å redusere risiko og bygge resiliens og benyttes også om det å beskytte mennesker, informasjon og eiendeler for å hindre og redusere skade og tap.

2.1.1 Safety - Security

Det engelske språket har ordene *safety* og *security* som begge oversettes til *sikkerhet* på norsk, til tross for at ordene ikke har helt samme betydning. I 2000 tok «Willoch-utvalget» (NOU 2000:24, 2000, s. 307) fram noen sentrale begreper og definisjoner som del av sin utredning om samfunnets sårbarhet og beredskap. I denne utredningen ble safety definert som ««Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter» og security som «Sikkerhet mot uønskede hendelser som er et resultat av overlegg og planlegging» (NOU 2000:24, 2000, s. 307). Utvalget skilte ut security som de hendelsene som er et resultat av at en aktør begår en bevisst og tilsiktet handling, som også er planlagt (security). Alle andre hendelser ble plassert under safety begrepet.

I forbindelse med en nasjonal utredning om sikring av landets kritiske infrastruktur i 2006 gjennomførte Finn-Erik Vinje (NOU 2006: 6, 2006, ss. 226-230) en begrepsutredning hvor

han endte med et forslag om en tredeling av begrepet sikkerhet som en *mulig tilnærming* til utfordringen med nyansene mellom security og safety. Hans forslag var at *sikkerhet* kan benyttes som et overordnet begrep, et hypernym, for å dekke alle uønskede hendelser uavhengig av om de er utilsiktet (ikke villet) eller tilsiktet (villet). Safety, som benyttes for sikkerhet mot uønskede utilsiktede hendelser kan erstattes med det norske ordet *trygghet*, mens security, som benyttes i betydning sikkerhet mot uønskede tilsiktede hendelser, kan erstattes med *sikring*. For øvrig finnes det mange eksisterende synonymer i det norske språket, og på samme måte som sikkerhet og trygghet er synonymer, gjelder det samme for adjektivene sikker og trygg. Vinje omtaler selv resultatet av denne utredningen som en «ren skrivebordskonstruksjon». Dersom en tar i bruk ordene på den måten han foreslår vil ikke det nødvendigvis føre til at det daglige språket endres. Det vil derfor uansett være nødvendig å redegjøre for betydninger av begrepene *sikkerhet*, *trygghet* og *sikring* når de benyttes i sammenhenger hvor forskjellene er viktig for riktig forståelse.. I praksis viser det seg ofte at det er de engelske ordene som benyttes, enten alene eller sammen med norske begrep, for å unngå misforståelser og for å presisere betydningen (Busmundrud et al., 2015, s. 25).

I sin artikkel om konseptuell og vitenskapelig avgrensning for omfanget av security som en potensiell selvstendig vitenskap, belyser Sissel H. Jore (2019) utfordringene med at det er *intensjon* forskerne benytter til å skille mellom safety og security. Intensjon er en faktor som også vurderes innen safety feltet, da en person kan gjøre en handling bevisst (med intensjon), men konsekvensen av handlingen kan i noen tilfeller få et utilsiktet og mer alvorlig og negativ utfall enn forutsett da handlingen ble utført. Jore foreslår derfor i sin artikkel at security bør avgrenses til *ondsinnede,* tilsiktede og bevisste handlinger fra en aktør, da det er intensjonen om bevisst å forårsake skader og ødeleggelse som kjennetegner security truslene. En person som tar snarveier og ikke følger retningslinjene ved f.eks. å unnlate å ta på seg hjelmen eller refleksvesten har ikke som intensjon å påføre skade eller tap. Personen gjør en bevisst handling, men en eventuell hendelse som følge av denne handlingen vil kategoriseres som en safety hendelse.

Sammen med denne forståelsen av trusler mot sikkerhet (security) foreslår Jore (2019) en ny definisjon, som både tar opp i seg den ondsinnede intensjonen og som et tiltak for å bygge resiliens mot ondskapsfulle angrep «Security can be defined as the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people's deliberate, intentional, malicious acts, such as terrorism, sabotage, organized crime, or hacking» (Jore, 2019, s. 169). Denne er oversatt av Jacobsen (2021) til «*den oppfattede eller*

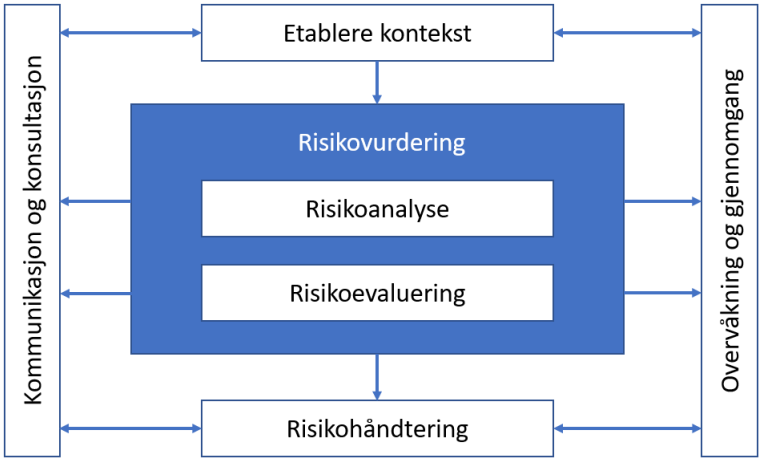
faktiske evnen til å forberede seg for, tilpasse seg, motstå og komme seg fra farer og kriser forårsaket av mennesker bevisste, forsettlige og ondsinnede handlinger som terrorisme, sabotasje, organisert kriminalitet eller hacking» (Jacobsen, 2021, s. 6).

2.1.2 Personellsikkerhet

Sikkerhet (security) kan deles inn i digital sikkerhet, personellsikkerhet, fysisk sikkerhet og sikkerhetsstyring (NSM, u.å.). Personellsikkerhet er en prosess for å sikre at en person ikke utgjør en sikkerhetsrisiko. Bakgrunnssjekk benyttes som en av tiltakene innen personellsikkerhet og baserer seg på evaluering av en persons karakter, egenskaper, bakgrunn og handlinger (Smith & Brooks, 2013, s. 194).

2.2 Risikostyring

«*Med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko*» (Aven, Risikostyring, 2015, s. 13).



Figur 1 – Risikostyringsprosess (Aven, 2015, s. 15)

Aven (2015, ss. 13-15) presenterer risikostyring som en prosess som følger en tradisjonell styringsprosess og metode, og risikostyringsprosessen er gjerne en integrert del av en virksomhets styringssystem. Risikostyringsprosessen kan framstilles som vist i Figur 1. Formålet med en risikostyringsprosess er å komme fram til et helhetlig underlag til beslutningsprosesser, for å sikre at balansen mellom utvikling og verdiskapning på den ene

siden, og ulykker, skader og tap på den andre siden, ivaretas. Risikostyring er ikke en prosess som bare skal finne fram til risikoreduserende tiltak. Ved å utarbeide et helhetlig underlag bidrar risikostyring til en risikoinformert beslutning, framfor en beslutning som ensidig baseres på høyeste risiko.

Hvilket risikoperspektiv en velger har stor betydning for risikostyringen og dette krever en forståelse for det grunnleggende om risiko (Aven, 2015, s. 37).

2.3 Perspektiver på risiko

«Den uttrykte risikoen er en måte å systematisere ens kunnskap om det usikre på» (Aven, 2015, s. 57) .

Aven (2015, s. 42) hevder at framtiden er det ingen som kan si noe sikkert om og begrepet risiko kan man si handler om framtiden og i stor grad om noe som *kan* skje og usikkerheten knyttet til dette. Risiko i denne konteksten, knyttet til aktivitet, består av de to komponentene *konsekvenser* av aktivitet og *usikkerhet* om konsekvensene. Til sammen utgjør de to komponentene risikoen. I det daglige språk brukes risiko ofte i sammenheng med at det kan komme til å skje noe negativt, men det kan også være en risiko for at konsekvensen kan bli positiv. Et eksempel på dette er fallskjermhopping som er en risikoaktivitet, men som samtidig medfører positive konsekvenser som opplevelsene av spenning og mestring, eller risikoen ved oppstart av en ny virksomhet som det kan være mulighet for å tjene penger på.

I en rapport fra FFI (Busmundrud et al., 2015) refereres det til at International Organization for Standardization (ISO) har utarbeidet en egen veileder med definerte begreper til bruk innen risikostyring for å legge til rette for en gjensidig forståelse på tvers av standarder. Risiko i veilederen fra ISO er definert som «*virkningen av usikkerhet på oppnåelse av mål*», som kan være både negative og positive utfall. Denne definisjonen benyttes blant annet i den såkalte ISO 27000-serien for informasjonssikkerhet og ISO 31000-serien for risikostyring og risikovurderinger (Busmundrud et al., 2015, s. 13). Bruken av risiko for både negative og positive resultater har ført til at det er innført et nytt begrep, *ren risiko*, som benyttes om risiko hvor det kun er to potensielle utfall, tap eller ikke tap, men ingen mulighet for gevinst. Ren risiko er gjerne et resultat av omstendigheter som ikke kan kontrolleres (Kagan, 2021) . Spekulativ risiko er vanligvis et valg hvor det er mulighet for både negativt og positivt resultat og er en kontrast til ren risiko (Downey, 2022).

Aven (2015, ss. 41-42) påpeker at det finnes flere perspektiver på hvordan risiko kan uttrykkes. Tradisjonelt i ingeniørmiljøene har det vært tap multiplisert med sannsynlighet (forventet tap) som kjennetegner risiko, mens økonomiperspektivet tar for seg forventningsverdien og usikkerheten rundt denne. Med økende forståelsen av risiko er det nå mer vanlig i ingeniørmiljøene å se på risiko som en kombinasjon av mulige konsekvenser og deres tilhørende sannsynligheter. Dette er nærmere økonomenes perspektiv, selv om det fortsatt er forskjeller siden det økonomiske perspektivet har forventningsverdien som sin referanse.

«Risiko er mer enn et regnestykke med to faktorer» (Midtgaard, 2021, s. 3) hevder leder av standardiseringskomiteen, Ann Karin Midtgaard, i sin presentasjon av revidert utgave av NS 5814. Opprinnelig revisjon av standarden definerte risiko som et «uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse" (Busmundrud et al., 2015, s. 3). For bedre å ivareta risikovurdering for tilsiktede uønskede hendelser ble NS 583x-serien utarbeidet med kun *sikringsrisiko* (security) som formål. I NS 5830 ble risiko definert som «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen", og sannsynlighet ble ikke omtalt (Busmundrud et al., 2015, s. 3). FFI (Busmundrud et al., 2015) har gjennomført en vurdering av tilnærming til risikovurdering for tilsiktede uønskede handlinger (security) med utgangspunkt i disse to norske standardene for risikovurdering som belyser og reflekterer over styrker og svakheter ved begge rammeverkene. FFI-rapporten har vært et bidrag til den nye revisjonen av NS5814 som ble utgitt i 2021. Den reviderte standarden tar kun for seg *ren risiko* og plasserer risikovurdering i virksomhetsstyringen, men uten å omfatte risikostyring. I NS5814:2021 defineres risiko som «usikkerhet knyttet til om en *uønsket hendelse* vil inntreffe og hvilke *konsekvenser* den kan få» med en merknad om at «usikkerhet kan uttrykkes gjennom *sannsynlighet*» (Midtgaard, 2021).

2.4 Risikovurdering

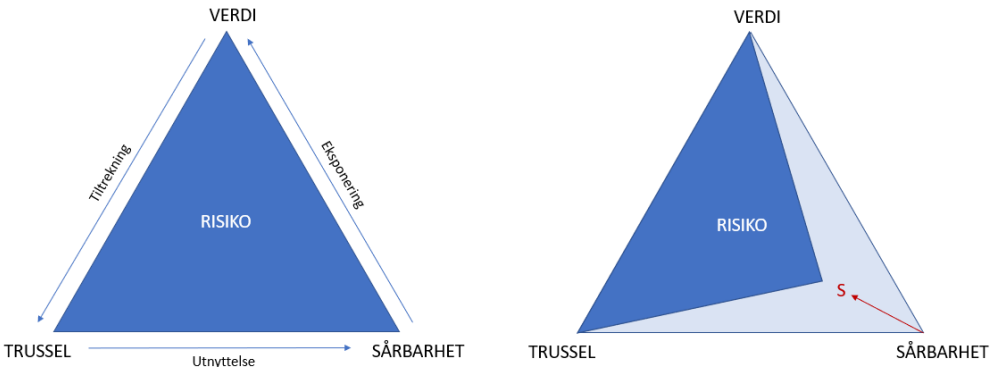
Som vist i Figur 1 omfatter risikovurdering både risikoanalyse og risikoevaluering, og den starter med risikoanalysen.

2.4.1 Risikoanalyse

Aven (2017, ss. 18-19) presenterer risikoanalyse som en systematisk framgangsmåte for å beskrive risiko gjennom å vurdere hvilke uønskede hendelser som kan inntreffe, hvor trolig det er at de inntreffer, og hvilke konsekvenser de kan få. I mange tilfeller gjøres risikoanalyser for å tilfredsstille krav som stilles i lovverk, fra myndigheter eller kunder, men målet med risikoanalysen er å komme ut med et underlag for å gi støtte til beslutningsprosesser.

Det er flere forskjellige metoder som kan benyttes og hvilken metode en bør velge er avhengig av faktorer som type system eller objekt som skal vurderes, hvor mye data som finnes, hvilke ressurser som er tilgjengelig og hvilken kunnskap som er tilgjengelig (Aven, 2017, ss. 18-19). En risikoanalyse som ikke blir ferdig i tide til beslutningen skal tas, oppfyller ikke hensikten, samtidig vil resultatet og nytteverdien påvirkes av hvor gode og realistiske forutsetningene for analysen er, informasjonen som er tilgjengelig og kunnskapen som finnes (Engen, et al., 2016, s. 81).

2.4.1.1 VTS-modellen



Figur 2 – VTS-modellen, motivert av (PST, 2022, s. 4) (NSM et al., 2015, s. 19)

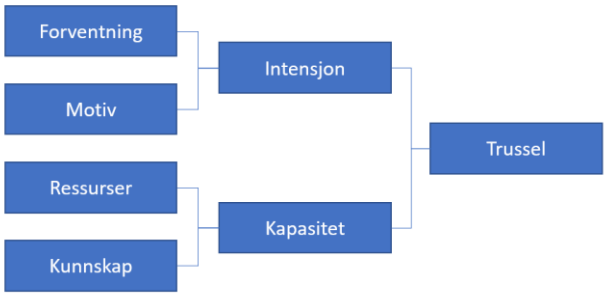
VTS-modellen (også kalt trefaktormodellen) er en modell som i første rekke er tenkt benyttet i risikoanalyser for *tilsiktede* uønskede handlinger. Modellen er basert på standarden NS 5832:2014 (Standard Norge, 2014) og tar for seg forholdet mellom trusselen mot en spesifisert verdi og denne verdiens sårbarhet i forhold til trusselen. NSM et al. (2015, ss. 18-19) illustrerer risikoen som vist i Figur 2, hvor trekantens areal er et uttrykk for risikoen for et scenario hvor verdi, trussel og sårbarhet er spesifisert. Målet er at risikoen reduseres så mye

som mulig, for eksempel ved å minske systemets sårbarhet som illustrert i trekanten til høyre i figuren. En økning av en av variablene i modellen vil på samme måte føre til økt risiko. Dersom trusselen fjernes, forsvinner risikoen helt (Njå et al., 2020, s. 259).

2.4.1.2 Verdi

NOU 2015: 19 (s. 44) beskriver verdi som et begrep som benyttes om noe som er verdifullt for noen, noe det er verdt å ta vare på og beskytte. Det blir gjerne sagt at noe har en større eller mindre verdi, og verdien er ofte avgjørende i forhold til vurderinger og beslutninger (NOU 2016: 19, 2016, s. 44). Både Njå et al. (2020, s. 258) og DSB (2019) hevder at verdiene kan være materielle som utstyr og fysiske objekter samt immaterielle som ideer, kultur og kunnskap. Sett i et virksomhetsperspektiv er det ofte liv og helse, økonomi, operativ evne, informasjon, miljø og omdømme som er de sentrale verdiene, mens kultur, samfunnsstabilitet og demokratiske verdier og styringsevne kommer inn som sentrale verdier på samfunnsnivå. Det bør gjøres en systematisk identifisering og vurdering av verdienes viktighet for en organisasjon i forhold til hvilke konsekvenser det får om de kompromitteres, endres eller ødelegges. I en virksomhet kan viktige verdier være fysisk materiell som er kritisk for produksjon, sensitiv informasjon, personell eller omdømme med mere.

2.4.1.3 Trussel



Figur 3 – Trusselkomponenter (Smith & Brooks, 2013, s. 65; oversatt)

Både Engen et al. (2016, ss. 87-89), Smith og Brooks (2013, ss. 64-66) og Busmundrud et al. (2015, s. 15) beskriver trusler og farer som årsak eller kilde til uønskede hendelser, og er noe som har mulighet til å påvirke noens verdier og forårsake skade eller tap. En trussel tiltrekkes av en verdi og er årsak til *tilsiktede* uønskede handlinger og skiller seg fra farer ved at det står

en eller flere mennesker bak, videre omtalt som en trusselaktør. Denne trusselaktøren har både en grad av intensjon og kapasitet til å utføre den ondsinnede handlingen. Intensjon er motivasjonen eller ønsket om og viljen til å utføre handlingen i kombinasjon med en forventning om å oppnå suksess eller å lykkes. Motivet for handlingen kan være å skade eller skape frykt, noe som er kjennetegn ved en terrorhandling, eller det kan også være et ønske eller begjær om oppmerksomhet, økonomisk vinning, eller en kombinasjon av flere motiver. Trusselaktørens kapasitet er avhengig av ressurser og kunnskap. Ressurser omfatter personell, utstyr og penger som må være tilgjengelige, mens kunnskap blant annet inkluderer kunnskap om verdien eller målet, hvilke tiltak som beskytter den aktuelle verdien, personell eller teknisk kunnskap. Sikkerhetstiltak begrenser det handlingsrommet en trusselaktør har for å lykkes, men en forsterkning av eller endring i eksisterende sikkerhetstiltak eller i andre rammebetingelser, kan også føre til at en trusselaktør tilpasser seg og endrer sine planer.

2.4.1.4 Barriere

Barrierer er de «tiltak og funksjoner som er planlagt for å bryte et uønsket hendelsesforløp» (Aven, 2017, s. 235). For å redusere risiko i en virksomhet etableres tiltak som skal forebygge at en uønsket hendelse inntreffer, såkalt *sannsynlighetsreduserende* barrierer, og tiltak som skal begrense effekten av en uønsket hendelse dersom den likevel skulle inntreffe, *konsekvensreduserende* barrierer. De sannsynlighetsreduserende barrierene er gjerne tiltak hvor funksjonen er å forhindre hendelsen, detektere at noe skjer, forsinke eller stoppe faren eller trusselen, mens tiltak for å redusere konsekvensene er funksjoner som responderer på hendelsen, begrenser skadeomfanget eller gjenoppretter normaltilstand (Aven, 2017, s. 16).

2.4.1.5 Sårbarhet

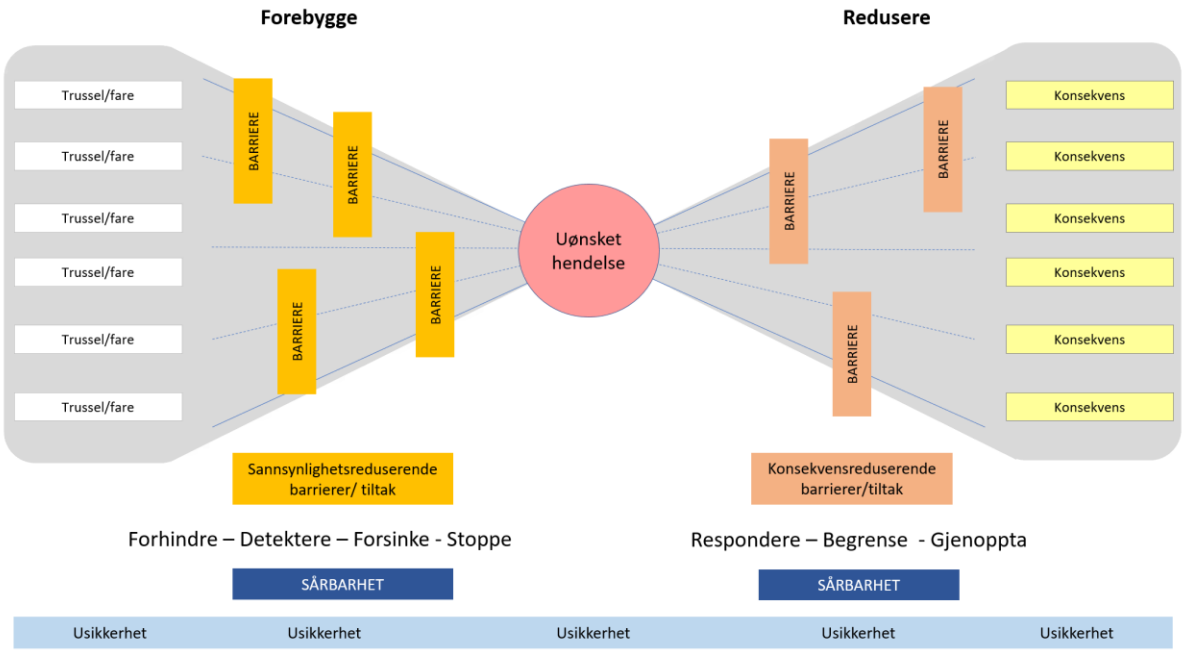
Aven (2017) definerer sårbarheten av et system som «kombinasjonen av aktivitetenes konsekvenser og usikkerhet, gitt at systemet utsettes for en initierende hendelse» (s. 39). Engen et al. (2016) beskriver dette med litt andre ord som «et systems forutsetninger for eller manglende evne til å fungere under og etter at det utsettes for en uønsket hendelse» (s. 47). Uten at en merker det er sårbarheter ofte reaktive egenskaper som utvikler seg i et system over tid. Robusthet betraktes ofte som det motsatte av sårbarhet, men er gjerne proaktivt, og noe en bygger inn i et system (Engen, et al., 2016, s. 47).

Smith og Brooks (2013) presenterer på sin side sårbarhet som det å være *eksponert* for fysisk eller følelsesmessig skade, eller som manglende robusthet eller evne til å tåle påkjenninger. Sårbarhetsvurderinger benyttes for å gi en bedre forståelse for interaksjonen mellom trusselen og sårbarheten. Mens sårbarhet fremhever hvor mottakelig en verdi er for et definert scenario, har risiko størst fokus på konsekvensenes alvorlighetsgrad gitt det definerte scenarioet (Smith & Brooks, 2013, ss. 67-68).

NS 5814:2021 tar inn over seg betraktningene fra både Aven, Engen et al. og Smith og Brooks, og som presentert av Midtgaard (2021) definerer NS 5814:2021 sårbarhet som «*analyseobjektets* manglende evne til å motstå *uønskede hendelser* eller varige påkjenninger, samt å opprettholde eller gjenoppta sin funksjon etterpå» (Midtgaard, 2021, s. 9).

En trusselaktør vil tiltrekkes av og utnytte sårbarheter ved et system for å oppnå sine mål og lykkes med sine handlinger, som for eksempel å trenge seg inn i en virksomhets datasystem ved å utnytte svakheter i brannmuren. Brannmuren er eksempel et sikkerhetstiltak iverksatt for å hindre at uvedkommende trenger seg inn i datasystemet, en barriere som skal redusere sannsynligheten for at et forsøk på inntrenging lykkes.

2.4.1.6 Sløyfemodellen



Figur 4 – Sløyfemodell (Bow-tie)

Sløyfemodellen (bow-tie) benyttes for å presentere risikoen i et helhetlig risikobilde, se Figur 4 (merk at i denne figuren er hendelsen illustrert som en *uønsket* hendelse, da det er det denne oppgaven omhandler). Modellen er internasjonalt kjent og benyttes blant annet i DSB (2019, s. 17) sitt rammeverk for utarbeidelse av krisescenarioer og i norsk standard for risikovurderinger (Midtgaard, 2021).

I midten av figuren vises den uønskede hendelsen, eller den *initierende* hendelsen i analysen (faren, trussel, muligheten). Etter å ha kartlagt hvilke verdier som er de viktigste gjøres en vurdering av hvilke uønskede hendelser som kan påvirke verdiene, hva som kan forårsake hendelsene (farer og trusler) og hvilke konsekvenser hendelsene kan føre til. Av disse scenariene velges det ut hvilke en ønsker å gå videre med for en mer detaljert analyse. Utvelgelse av scenarier kan gjøres ut fra hvilke scenarioer som kan gi størst negative konsekvenser, hvilke som umiddelbart anses som mest sannsynlig eller etter andre kriterier som risikoeier har definert.

2.4.1.7 Sannsynlighet, usikkerhet og kunnskapsstyrke

Resultatet av risikoanalysen vil påvirkes av kunnskapsgrunnlaget og denne kunnskapen kan være sterk eller svak.

Tabell 2 Bakgrunnskunnskap, motivert av (Aven, 2015, ss. 58-59) (Aven, 2017, s. 35)

	Svak kunnskap	**Sterk kunnskap**
Forutsetninger	Sterke forenklinger	Svært rimelige
Data/informasjon	Ikke-eksisterende, upålitelig eller irrelevant	Store mengder pålitelig og relevant
Eksperter	Stor uenighet	Bred enighet
Fenomener og modeller	Dårlig forstått, eksisterer ikke eller kjent for dårlige prediksjoner	Godt forstått, kjent for prediksjoner med nødvendig nøyaktighet

Som Aven (2015, ss. 58-59) (2017, s. 35) beskriver det, se Tabell 2, vil kunnskapsgrunnlaget påvirkes av flere aspekter som forutsetningene som ligger til grunn for analysen og hvor riktige eller gode disse forutsetningene er, godheten av ekspertvurderinger og om det er

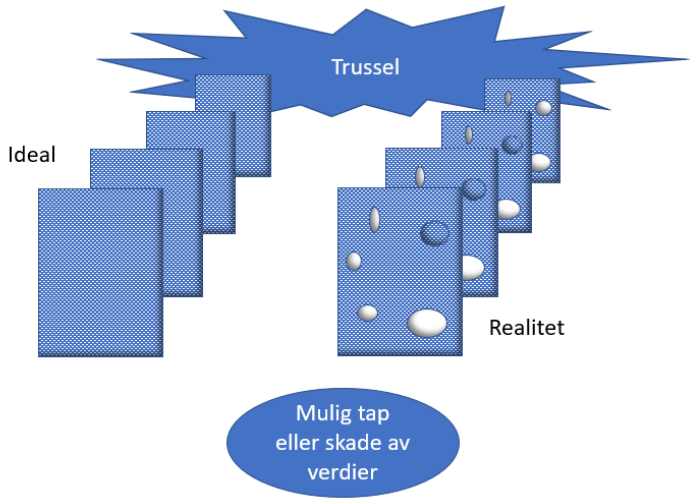
enighet mellom ekspertene, tilgjengelige data, forståelse av de involverte fenomener samt modellenes godhet.

Kunnskapsgrunnlaget en har tilgang til i prosessen beskrives som usikkerhet og uttrykkes gjennom sannsynlighetsvurderingen. Det vil være grad av usikkerhet i forhold til om trusselen eksisterer og om en trussels intensjon og kapasitet, om hendelsen inntreffer, barrierenes sårbarheter og effekt i forhold til den aktuelle trusselen, og i forhold til konsekvenser og følgehendelser (med potensielt nye konsekvenser).

2.4.1.8 Forsvar i dybden

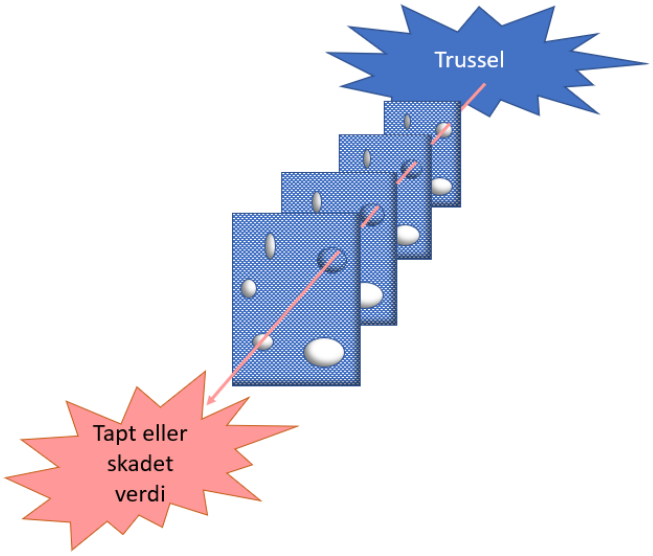
Smith og Brooks (2013, ss. 107-109) presenterer forsvar i dybden som et prinsipp som har vært benyttet innen militære operasjoner gjennom århundrer. Hensikten med flere lag av fysiske sikkerhetstiltak har vært å forsinke en fiendes framrykking mot et mål inntil nye tropper eller våpen er på plass til å pågripe eller nedkjempe fienden. Gjennom erfaring er det funnet ut at flere barrierer gir bedre effekt enn en enkelt, sterk barriere. Prinsippet om forsvar i dybden er videreført i dagens teori om sikring av verdier og tiltakene er gjerne en miks av organisatoriske, menneskelige og fysiske barrierer

Som et eksempel kan sikkerhetsgradert informasjon i en virksomhet beskyttes av inngjerdet område, dører med låssystem, datamaskiner med passord og tilgangskontroll og krav til sikkerhetsklarering og autorisasjon, før en person gis bruker til systemet, samt regler for bruk av systemet som må etterleves. Barrierene skal hindre et potensielt tap eller skade på informasjonen.



Figur 5 – Forsvar i dybden (Reason, 1997, s. 9; oversatt)

James Reason (1997) påpeker sveitserhull-effekten som en utfordring med forsvar i dybden prinsippet. Ideelt sett skal hver barriere oppfylle sin funksjon for å sikre aktuell verdi og hindre trusselen i å nå fram til verdien, hvilket er illustrert som «perfekte osteskiver» til venstre i Figur 5. Reason trekker imidlertid fram at det finnes sårbarheter i alle barrierer, hvilket er illustrert som hull i «osteskivene» til høyre i figuren, som i en sveitserost. Han tar også fram at sårbarhetsbildet til enhver tid er i endring og det kan ses på som at «osteskivene» til enhver tid er i bevegelse, eller at enkelte «osteskiver» fjernes eller nye legges til, og at hullene flytter seg rundt eller økes og minkes i størrelse. Sårbarhetene kan skyldes aktive feil som at en person slipper inn en person som egentlig ikke har adgang. Det kan også være latente feil som har bygd seg opp i systemet over tid som for eksempel et system med tilgangsgrupper i et datasystem som har vokst over tid og som det er mangel på oversikt over hva de gir tilgang til. Moderne systemer blir stadig mer komplekse, og dette gjelder også oppbyggingen av sikkerhetstiltak. Det blir stadig mer utfordrende å ha oversikt over alle mulige scenarioer, noe som medfører at latente sårbarheter får mulighet til å utvikle seg og ikke oppdages.



Figur 6 – Sveitserost-modellen (Reason, 1997, s. 12; oversatt)

Som et resultat av dette oppstå situasjoner hvor alle barrierer svikter og trusselen lykkes med sitt angrep, som vist i Figur 6, med påfølgende skade og tap for virksomheten (Reason, 1997, ss. 7-13).

2.4.2 Risikoevaluering

Aven (2017, s. 22) (2015, s. 15) presenterer risikoevalueringen som en del av risikovurderingen. I risikoevalueringen evalueres resultatene fra risikoanalysen. Er risikoen akseptabel på analysetidspunktet, eller er det behov for å identifisere nye tiltak som kan bidra til å redusere risikoen til et akseptabelt nivå? Usikkerhet i forhold til kunnskapsgrunnlaget vil ha betydning for evalueringen av risikoen og de forskjellige tiltakene og løsningsalternativene evalueres i forhold til den kunnskapen som er tilgjengelig.. Risikoevalueringen omfatter også forslag til hvordan risikoen kan håndteres.

2.5 Tidligere forskningsoppgaver

Av tidligere forskning i tilknytning til temaet finnes det et utvalg norske masteroppgaver:

Jon Petter Syvertsen (Syvertsen, 2007) undersøkte i sin masteroppgave *Insider Threat* innsidetrusselen i Norge. Dessverre var det lav respons fra informantene på undersøkelsen da data om dette anses som svært sensitive.

Terje Benjaminsen (Benjaminsen, 2017) gjorde i sin masteroppgave *The Norwegian Downsizing Approach in Terms of the Insider Threat - An interpretive study* en undersøkelse av hvordan norske organisasjoner forholder seg til innsidetrusselen i en nedbemanningssituasjon.

Per Ringstad (Ringstad, 2020) sin oppgave *Sikkerhetsstyringens utvikling* omhandler sikkerhetsstyringens utvikling gjennom 20 år og tar for seg hvordan risikooppfatningen knyttet til personellsikkerhet har utviklet seg disse årene og hvordan en innsidehendelse kan forklares fra et organisatorisk perspektiv.

Julie Dahl Jacobsen (Jacobsen, 2021) undersøkte i sin oppgave *Hvordan holde innsidere på utsiden?* hva som forårsaker at noen personer blir ondsinnede innsidere, deres motivasjon og hvordan denne trusselen kan forebygges.

I tillegg utarbeidet Det norske Veritas og Germanischer Lloyd (DNV GL) en rapport (DNV GL, 2019) om innsiderisiko i petroleumsnæringen på oppdrag for Petroleumstilsynet (Ptil). Denne rapporten gir en dybdebeskrivelse av fenomenet innsidetrussel, presenterer et verktøy for å måle hvor moden en virksomhet er på området, og foreslår 45 konkrete tiltak som god praksis for å håndtere innsidetrusselen.

3 DESIGN OG METODE

I dette kapitlet presenteres valg av problemstilling, forskningsdesign, valg av metode, innsamling av data og utfordringer underveis med analyse av dataene. I tillegg presenteres noen vurderinger og refleksjoner i forhold til validitet, reliabilitet og etikk.

Denne oppgaven har i stor grad bestått av dokumentstudier samt noe kvalitetssikring av data gjennom ulike fora for utveksling av erfaringer og diskusjon.

3.1 Valg av problemstilling

Fordi hele masterstudiet startet med forfatters ønske om å tilegne seg mer faglig kunnskap og kompetanse i risikoanalyse og risikovurdering, var den opprinnelige planen for masteroppgaven å gjennomføre en analyse av den reviderte NS 5814:2021 (Standard Norge, 2021) for å undersøke om etterlevelse av NS 5814:2021 kan tilføre ytterligere verdi til risikovurderingen i en risikostyringsprosess som er basert på den overordnede standarden for risikostyring, NS-ISO31000:2018 (Standard Norge, 2018). Oppgaven skulle gjennomføres ved å analysere en eksisterende prosess for risikostyring og vurdere om elementer fra NS5814:21 burde implementeres i denne prosessen.

I det forberedende arbeidet og litteraturstudiene til oppgaven ble forfatter påvirket av debatter og innlegg på NSM sin sikkerhetskonferanse 2022. Utspillet fra PST-sjef Hans Sverre Sjøvold (NSM, 2022b) i forhold til om sikkerhetsklarering også bør benyttes for personer som skal jobbe med forskning som omfatter sensitiv informasjon, trigget interessen for å gjøre en mer konkret analyse av hvordan sikkerhetsklarering som tiltak påvirker virksomheter i dag, sett i sammenheng med risikovurdering. Før en tar i bruk et eksisterende tiltak på nye områder, bør det undersøkes hvordan det fungerer i dagens situasjon. Fordi risikovurdering allerede var et tema i oppgaven, førte denne avsporingen fram til det som ble den endelige problemstillingen for oppgaven

- *Hvordan kan bruk av sikkerhetsklarering påvirke vurderingen av innsiderisiko?*

Denne endringen medførte at både forskningsdesign, metode og innsamling av data måtte korrigeres for å får fram et underlag for den nye problemstillingen med tilhørende forskningsspørsmål.

3.2 Forskningsdesign

Blaikie (2010, s. 36) hevder at det som skal oppnås med et forskningsdesign er å få maksimal kontroll på forskningsprosessen.

For å besvare problemstillingen ble det satt opp tre forskningsspørsmål som skulle bidra til å belyse den:

1. Hvordan defineres en innsider?
2. Hvordan vurdere innsiderisiko i en virksomhet?
3. Hvilken effekt har sikkerhetsklarering på vurdering av innsiderisiko?

Det ble deretter lagt en plan for utforsking av de forskjellige forskningsspørsmålene.

Strategien for å gjennomføre denne studien var å benytte internett og litteraturstudier. En styrke med dette er mengden informasjon som er tilgjengelig, noe som også blir en svakhet i forhold til å gjennomføre et strukturert utvalg og å være i stand til å begrense datamengden. Dette kan være spesielt utfordrende dersom den som skal gjennomføre studien er interessert og engasjert i tematikken, ut over det som er nødvendig eller relevant for den aktuelle oppgaven.

Noen av temaene og funnene er også diskutert med kolleger både internt i egen virksomhet og med kolleger i andre norske virksomheter, men de er helt bevisst ikke benyttet direkte som informanter eller intervjuobjekter.

3.3 Metodevalg

Det har vært benyttet kvalitativ metode i denne oppgaven, med innsamling av en mindre mengde data og fortolkning av disse dataene.

Oppgaven har i hovedsak vært gjennomført som en litteraturstudie.

Med den tidshorisonten som var til rådighet, måtte mengden data begrenses. Det kunne ellers være svært interessant å undersøke data fra andre nasjoner og organisasjoner. For eksempel i forhold til bruk av sikkerhetsklarering og hvordan samspillet mellom myndigheter og virksomheter er tenkt å fungere i andre land enn Norge. Kultur vil raskt komme opp som en av faktorene om en skal øke bredden i studien, og da blir det en helt annen oppgave og et annet omfang.

3.4 Datainnsamling

I denne oppgaven er det hovedsakelig tatt utgangspunkt i dokumentasjon fra offentlige instanser som utfører sitt arbeid på vegne av offentlige styringsorganer i de landene som har vært gjenstand for undersøkelsen. Dette er gjort som et bevisst valg, da sikkerhetsklarering er et anerkjent virkemiddel på tvers av land, og som også benyttes for å få tilgang til informasjon som eies av allianser som for eksempel NATO. Det er i størst mulig grad benyttet litteratur som ligger åpent tilgjengelig på internett, da det har vært et ønske om å ta utgangspunkt i åpne kilder. Samtidig er det i stor grad søkt å benytte nettsteder som er styrt av myndighetene i det enkelte land.

En utfordring med å bruke internett som kilde er den uendelige mengden data som finnes der. Det er derfor gjort en jobb med å kryssjekke deler av informasjonen.

For den norske litteraturen, som lover og forskrifter og NSM sine dokumenter, så er dette kjente nettsteder som Lovdata og NSM, og også underlag som forfatter benytter i daglig arbeid.

Innsider

Utgangspunktet for studiet av begrepet innsider var dokumentasjon fra Norge, USA og Storbritannia. Ved uklarheter ble det søkt etter flere ressurser for å bekrefte eller avkrefte hendelsesløpet og utviklingen av definisjonen på en innsider. Det er grunnen til at det for USA er benyttet flere forskjellige kilder (CMMC, U.S, DoD, Carnegie Mellom University), da funnene avviker fra det som ble funnet i Norge og Storbritannia. Da det viste seg at både Norge og Storbritannia refererte til Australia i sine dokumenter, ble litteratursøket utvidet til å omfatte Australia.

Risikovurdering av innsidere

I starten av studien var det ukjent for forfatter at det fantes egen metodikk med støtte i skjemaer spesialtilpasset for vurdering av innsiderisiko. Dette ble oppdaget gjennom det brede litteratursøket og studiene av forskjellige definisjoner for innsidere.

For å svare ut forskningsspørsmålet om vurdering av innsiderisikovurdering i en virksomhet, ble det valgt å studere metoden fra CPNI (CPNI, 2013b) i Storbritannia og analysere denne opp imot de norske veilederne fra NSM, samt teori.

Noe som gjorde denne analysen svært interessant var CPNI sin modell som framstår som generell og allmenngyldig for enhver virksomhet, mens NSM sin veiledere ført og fremst er tilpasset virksomheter som er underlagt sikkerhetsloven.

Sikkerhetsklarering

For å vurdere det siste forskningsspørsmålet, og problemstillingen, ble det tatt utgangspunkt i det norske forskrifter og veiledere som støtter opp om sikkerhetsloven, samt barriereteori.

3.5 Dataanalysens utfordringer

Data samlet inn over tid er utfordrende når det stadig tilkommer nye data, som f.eks. den nye veilederen fra CPNI som kom underveis i oppgaveskrivingen. Samtidig viser dette at fagområdet er i utvikling, og at flere ser utfordringer i forhold til dagens praksis innenfor fagfeltet.

Utfordrende når en ikke gjenfinner data i oppdatert/nyere dokumentasjon.

Å sette seg inn i og lære ny kunnskap kan være utfordrende, men samtidig enkelt da det bare skal fylles opp med noe nytt. Å tilegne seg kunnskap som bryter med/går på tvers av kunnskap og oppfatning en allerede sitter inne med krever noe annet, da det som eksisterer må brytes ned, for så å kunne fylles opp igjen med fornyet og utvidet forståelse.

Svært bred oppgave, mange aspekter som må vurderes og ses opp imot hverandre. Dette kan medføre at analysen blir for overfladisk, i stedet for å gå dypere inn i enkelte deler av oppgaven.

Tid ble en påvirkende faktor, både i forhold til oppgavens bredde, men også grunnet bytte av oppgave underveis.

Forfatter var kjent med at det fantes forskjellige perspektiver i forhold til begrepet innsider, men var likevel ikke forberedt på hvor mange varianter, eller nyanser som finnes. Forfatter

opplevde også i diskusjoner at det var både sterke meninger og følelser involvert, og at det legges forskjellig betydning i flere av adjektivene som benyttes for å beskrive type innsider.

En stor utfordring at oppgaven ikke ble planlagt godt nok i forhold til å sette avgrensninger og holde seg til disse. Det er en svært stor mengde informasjon som er tilgjengelig.

3.6 Validitet (intern og ekstern) og reliabilitet

Validitet er en måling på om de konklusjoner som trekkes ut fra funn og drøfting vil være anvendelige og kunne anerkjennes.

Intern validitet

Noen av temaene er diskutert med kolleger og vil være aktuelle for andre som har sitt virke innenfor samme fagområde.

En utfordring kan være begrepet innsider som i denne studien er benyttet på en annen måte enn i det daglige språk i Norge, hvor innsider ofte benyttes om en som bevisst og ondskapsfullt gjennomfører handlinger, som for eksempel spionasje. Til tross for at valg av innhold i begreper er basert på funn og drøfting, kan det likevel være til hinder for forståelse og aksept.

Ekstern validitet

I denne studien er det sett på det norske regimet for sikkerhetsklarering. Hvorvidt dette er direkte overførbar kunnskap til andre områder som for eksempel andre nasjoner og deres sikkerhetsklareringsregimer, vil være avhengig av om de har et tilsvarende regime med en myndighet som sikkerhetsklarering og at virksomheten må ta ansvaret for autorisasjon og oppfølging.

Samtidig er funnene i studien sett opp mot teori om barrierer og forsvar i dybden (Reason, 1997). I dette tilfellet er det forskjellig ansvarlige for hver av barrierene og det gjøres funn på at å legge mye tillit i første barriere kan få en uheldig effekt ved at de påfølgende barrierene er svekket ved å utvise for stor tillit til den første barrieren. Dette perspektivet kan være overførbart også til andre områder som benytter flere forskjellige barrierer for beskyttelse.

Reliabilitet

Reliabilitet handler om studien kan gjennomføre en gang til, med de samme resultatene.

I forhold til reliabilitet i dataene er det for det meste benyttet litteratursøk og skriftlige kilder i denne oppgaven. Data som er hentet fra litteraturen vil være reproduserbare.

I drøftingen vil perspektiver og erfaringer gjennom flere år ligge til grunn for momenter som er tatt med i studien. Selv om de er drøftet opp imot empiri og teori, kan en annen forsker ha annen erfaring og kan komme fram til et annet resultat. Det er ingen garanti for at alle perspektiver er ivaretatt i denne studien, og en annen forsker vil kunne komme inn med nye vinklinger.

3.7 Etiske refleksjoner

Opprinnelig valgt tema for oppgaven, analyse av den reviderte NS 5814:2021 (Standard Norge, 2021), var et ønske fra forfatter om en oppgave som i tillegg til å gi læring kunne gjennomføres med objektivitet til temaet.

Forfatter har hatt arbeid innen personellsikkerhet i en virksomhet som har sikkerhetsklarert personell og flere autorisasjonsansvarlige.

Det kan være en styrke å ha bakgrunnskunnskap om temaet som skal studeres, men samtidig kan det medføre at en leter etter funn som støtter opp om egne teorier og meninger, og at andre funn og observasjoner overses.

4 EMPIRI

I dette kapitlet følger en presentasjon av empiriske data funnet gjennom litteraturstudier.

4.1 Innsider – Innsidetrussel – Innsiderisiko

«Insider er en som hører til et samfunn, en organisasjon, en gruppe eller lignende, og som derfor har adgang til spesielle og ofte hemmelige opplysninger og kunnskap som folk utenfor ikke har» står det i Store norske leksikon («Insider», 2020). Fra finansnæringen er kjøp og salg av børsnoterte aksjer basert på innsideinformasjon kjent under betegnelsen innsidehandel og forbudt ved lov. Innsideren benytter i dette tilfelle informasjon som forventes å medføre endring i aksjekursen til å kjøpe eller selge aksjer for å oppnå egen vinning.

4.1.1 USA

Cybersecurity Maturity Model Certification (CMMC) (U.S. DoD, 2022) er et omfattende rammeverk og sertifiseringsprogram utviklet av USAs forsvarsdepartement. Krav om sertifisering vil bli stilt til leverandører til det amerikanske forsvar, inkludert leverandører utenfor USA. Hensikten med CMMC er å forbedre beskyttelsen av sensitiv ugradert informasjon i forsvarsindustrien mot stadig flere og mer komplekse cyber-angrep og konteksten er USAs verdier.

CMMC (U.S. DoD, 2021, s. 15) definerer en innsider som «Enhver person med autorisert tilgang til en hvilken som helst organisasjon eller ressurser fra USAs myndigheter for å inkludere personell, fasiliteter, informasjon, utstyr, nettverk eller systemer» (U.S. DoD, 2021, s. 15; oversatt), mens innsidetrussel er «trusselen om at en innsider vil bruke sin autoriserte tilgang, bevisst eller ubevisst, for å skade organisasjonens eller USAs sikkerhet. Denne trusselen kan omfatte skade på USA gjennom spionasje, terrorisme, uautorisert avsløring, eller gjennom tap eller forringelse av avdelingers ressurser eller kapasiteter » (U.S. DoD, 2021, s. 15; oversatt).

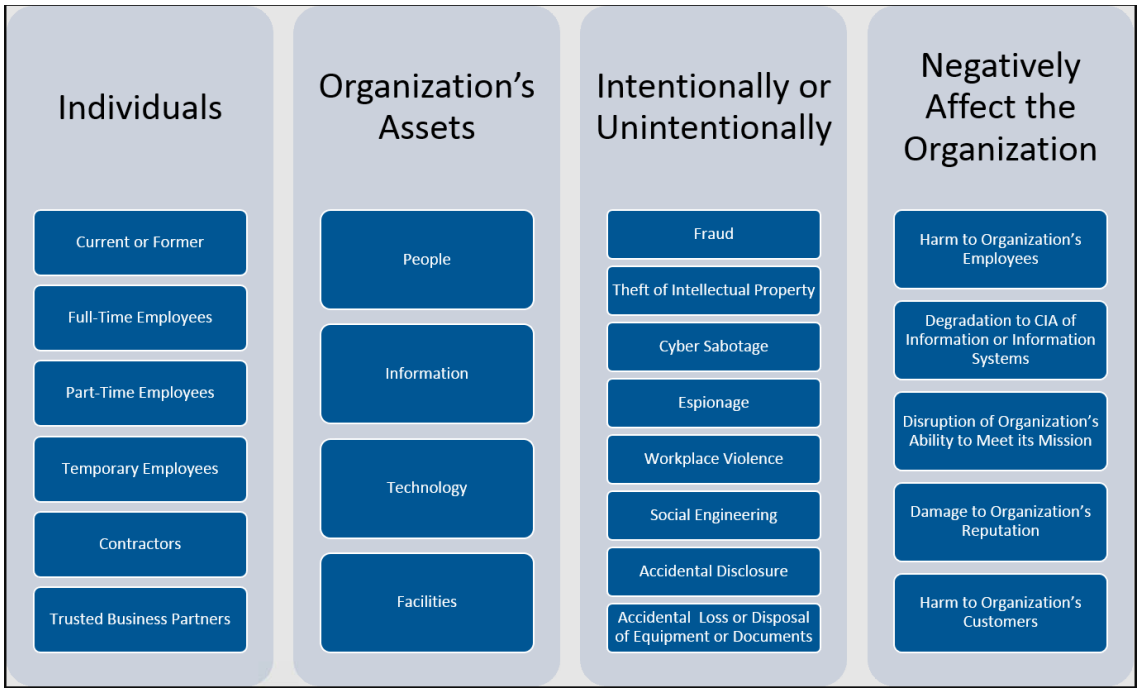
Cybersecurity and Infrastructure Security Agency (CISA) (U.S. Government, u.å.) har en mer generell tilnærming og definerer en innsider som «enhver person som har eller har hatt autorisert tilgang til eller kunnskap om en organisasjons ressurser, inkludert personell, fasiliteter, informasjon, utstyr, nettverk og systemer» (U.S. Government, u.å.; oversatt), og innsidetrussel som «potensialet for en innsider til å bruke sin autoriserte tilgang eller

forståelse av en organisasjon for å skade den organisasjonen. Denne skaden kan omfatte ondsinnede, selvtilfredse eller utilsiktede handlinger som negativt påvirker integriteten, konfidensialiteten og tilgjengeligheten til organisasjonen, dens data, personell eller fasiliteter» (U.S. Government, u.å.; oversatt). CISA deler det de kaller innsideradferd inn i spionasje, terrorisme, uautorisert utlevering av informasjon, korrupsjon, sabotasje, vold på arbeidsplassen og tilsiktet eller utilsiktet tap eller forringelse av avdelingsressurser eller kapabiliteter.

I en grunnleggende studie utført av CERT Insider Threat team ved Carnegie Mellon University (Carnegie Mellon University, 2013, s. 2) om utilsiktede innsidetrusler, ble utilsiktet innsidetrussel definert som «en nåværende eller tidligere ansatt, kontraktør eller forretningspartner som har eller hadde autorisert tilgang til en organisasjons nettverk, system eller data, *og som gjennom handling eller passivitet uten ondsinnet hensikt forårsaker skade eller øker sannsynligheten vesentlig for at fremtidig alvorlig skade på* konfidensialiteten, integriteten eller tilgjengeligheten til organisasjonens informasjon eller informasjonssystemer» (Carnegie Mellon University, 2013, s. 2; oversatt). De utilsiktede hendelsene ble delt inn i de fire kategoriene utilsiktet avsløring av sensitiv informasjon, ondsinnet hacking fra tredjepart, feil eller utilsiktet avhending av fysiske verdier som papirdokumenter, og mistet eller frastjålet utstyr med lagringsenhet som telefon eller minnepenn. Denne studien konkluderte med at det er forskjell på utilsiktet og tilsiktet innsidetrussel, både i forhold til motivasjon, trusselindikatorer, og andre faktorer som må forstås bedre for å utvikle gode tiltak for å forebygge og redusere risikoen. Faktorene omfatter blant annet menneskelige/kognitive faktorer som menneskelige feil, tretthet eller søvnighet, subjektiv mental arbeidsbelastning, situasjonsbevissthet og tankevandring, samt psykososiale og sosiokulturelle faktorer som risikotoleranse, kulturelle faktorer, kjønn, humør, alderseffekter med variasjoner over tid, og påvirkning av narkotika og hormoner (Carnegie Mellon University, 2013).

Med utgangspunkt i definisjon av utilsiktet innsidetrussel og CERT (Costa, 2017) sin definisjon av ondsinnet innsidetrussel «en nåværende eller tidligere ansatt, kontraktør eller forretningspartner som har eller hadde autorisert tilgang til en organisasjons nettverk, system eller data *og med vilje har overskredet eller misbrukt denne tilgangen på en måte som negativt påvirket* konfidensialitet, integritet eller tilgjengeligheten av organisasjonens informasjon eller informasjonssystemer» (Costa, 2017; oversatt) publiserte Software Engineering Institute (SEI) ved Carnegie Mellom i 2017 en oppdatert definisjon på

innsidetrussel: «**potensialet** for en person som har eller hadde autorisert tilgang til en organisasjons kritiske eiendeler til å bruke denne tilgangen, enten ondsinnet eller utilsiktet, til å handle på en måte som kan påvirke organisasjonen negativt» (Costa, 2017; oversatt). Denne generelle og enkle definisjonen er tiltenkt å møte behov og krav fra enhver organisasjon samtidig som den ivaretar framtidige endringer i forhold til hvilke trusselaktører som vurderes som innsidetrussel og hvilke som vurderes å være en innsider. Dette står i kontrast til de definisjoner som lister forskjellig type trusselaktører, hva de har tilgang til og hvilken skade de kan påføre en organisasjon. SEI har i definisjonen bevisst skilt *trusselen* fra *aktøren* og definisjonen skal ivareta både ondsinnede tilsiktede og ikke-ondsinnede (utilsiktede) handlinger. Imidlertid vil det i praktisk bruk være behov for mer detaljert beskrivelse for å sikre at omfanget av truslene og konsekvensene av dem blir forstått. SEI har derfor utviklet et diagram som kan bidra til dette, og som kan tilpasses den enkelte organisasjon, se Figur 7.



Figur 7 – Innsidetrusselen med potensielle konsekvenser (Costa, 2017)

4.1.2 NATO

En studie om deteksjon av innsidetrusler (Kont et al., 2015) som ble gjennomført i regi av NATO beskriver innsideren som en som kan være medlem av en organisasjon, en medarbeider (innleid, forretningspartner eller gjest), alle med autorisasjon til å utføre visse aktiviteter, alle som er autentisert av systemet (inkludert uautoriserte brukere som bruker gyldig legitimasjon), eller en uvillig eller tvunget medskyldig til en ekstern aktør. En person

som har sluttet å være medarbeider eller medlem av en bestemt organisasjon kan fortsatt betraktes som en innsider dersom vedkommendes autentisering ikke har blitt fullstendig opphevet eller personen (mis)bruker tidligere ervervet kunnskap. Definisjonen av en innsider kan derfor deles i tre kategorier, personer som har kunnskap, tilgang og/eller tillit (Kont et al., 2015, s. 12). Studien tar utgangspunkt i fem profiler for innsidertrussel som en base for å analysere problemet som denne trusselen utgjør. Innsidertrusselprofilene er *sabotasje* som vanligvis er motivert av hevn og har som mål å ødelegge i størst mulig grad, *tyveri* og *svindel* som oftest motiveres av grådighet og gjerne foregår i det skjulte, *spionasje* som har kjennetegn fra flere profiler, men mest lik adferd som sabotasje (Kont et al., 2015, s. 22). I tillegg kommer den utilsiktede innsideren som allerede er beskrevet i denne oppgavens kap. 4.1.1.

4.1.3 Storbritannia

Det britiske Centre for the Protection of National Infrastructure (CPNI) som er den nasjonale tekniske myndighet for forebyggende fysisk og personellsikkerhet for den britiske regjering, definerer innsider som «en person som utnytter, eller har til hensikt å utnytte, sin legitime tilgang til en organisasjons eiendeler for uautoriserte formål» (CPNI, 2013a, s. 4; oversatt). CPNI (2013a, s. 9) kategoriserer insidere etter tre typer adferd. Den første kategorien er den *bevisste innsideren* som søker seg til en stilling med bevisst intensjon om å misbruke de tilgangene som posisjonen stillingen gir. Den *frivillige eller selvinitierte* er en som personlig bestemmer seg for å misbruke sine tilganger, men som ikke hadde disse hensiktene før ansettelse i organisasjonen. Den *utnyttede eller rekrutterte* innsideren hadde heller ingen bevisst intensjon om å utnytte tilgangene før ansettelse, men blir på et tidspunkt i ansettelsesforholdet utnyttet eller rekruttert av en tredjepart til å gjøre det. Utlevering av sensitiv informasjon til uautoriserte, prosesskorrupsjon, tilrettelegging for tredjeparts tilgang til en organisasjons eiendeler, fysisk sabotasje og elektronisk eller IT-sabotasje er identifisert som de fem hovedtypene for innsideaktivitet (CPNI, 2013a, s. 4). I studien ble hovedmotivasjonene for å bli en innsider identifisert som økonomisk gevinst, ideologi, ønske om anerkjennelse, lojalitet til venner/familie/land og hevn (CPNI, 2013a, s. 9). CPNI definerer ikke begrepet innsidetrussel spesifikt, men i veilederen for forebyggende rollebasert risikovurdering (CPNI, 2022b, s. 1) defineres trussel som den intensjon og kapasitet en fiendtlig aktør har til å gjennomføre en handling, som eksempelvis et terrorangrep.

4.1.4 Australia

Den australske regjering har utgitt en håndbok i personellsikkerhet, *Managing the Insider Threat to Your Business. A personnel security handbook* (Australian Government, 2014). Håndboka refererer til studien fra CPNI (2013a), men har gjort noen tilpasninger til definisjonene. Innsidere beskrives i den australske håndboka (Australian Government, 2014) som «pålitelige innsidere er potensielle, nåværende eller tidligere ansatte eller kontraktører som har legitim tilgang til informasjon, teknikker, teknologi, eiendeler eller lokaler» (s. 2; oversatt) og innsidetrusselen som «trusselen forårsaket av **uautorisert** tilgang, bruk eller avsløring av privilegert informasjon, teknikker, teknologi, eiendeler eller lokaler av en person med legitime eller indirekte tilgang, som kan forårsake skade» (s. 2; oversatt). Pålitelige innsidere som utgjør en trussel deles i to hovedkategorier, utilsiktet og ondsinnet. Den *utilsiktede* innsideren beskrives som en som utfører handlinger som fører til tap av eller skade på verdier uten selv å forstå konsekvensen av handlingene sine. De ondsinnede innsiderne deles i underkategoriene selvmotiverte og rekrutterte. Den *selvmotiverte* utfører bevisst og med vilje handlinger som er personlig initiert, uten påvirkning fra en tredjepart. Mens den *rekrutterte* innsideren utfører bevisst og med vilje handlinger på vegne av en tredjepart som bevisst utnytter innsiderens potensielle, nåværende eller tidigere tilganger.

Den australske regjering har også en håndbok fra 2010, *The Insider Threat to Business. A personnel security handbook* (Australian Government, 2010), som omhandler samme tema, men hvor innsider defineres som «en nåværende eller tidligere arbeidstaker i en organisasjon eller som har legitim tilgang til organisasjonens ressurser og **bruker eller forsøker å bruke** denne tilgangen til å forårsake skade» (Australian Government, 2010, s. 2; oversatt). Her kategoriserer innsidere i de som bevisst søker en stilling for å forårsake skade, de som skader etter å ha blitt ansatt uten at dette var intensjonen før ansettelse, og de som blir utnyttet av andre til å gjøre skade etter at de er ansatt og kan være enten en passiv, uvitende eller uvillig innsider. Innsidetrusselen defineres i denne håndboka som «en eller flere personer med tilgang og/eller innsidekunnskap om en virksomhet eller organisasjon eller en virksomhet som vil tillate dem å utnytte sårbarhetene til enhetens sikkerhet, systemer, tjenester, produkter eller fasiliteter med hensikt om å forårsake skade» (Australian Government, 2010, s. 2; oversatt).

4.1.5 Norge

I Norge kom det i 2017 en veileder (PST et al., 2017) som har til hensikt å til øke bevisstheten om innsidetrusselen, samt å sette både offentlige og private virksomheter bedre i stand til å etablere gode rutiner både før, under og ved avvikling av ansettelses- og innleieforhold. Veilederen ble etablert i et samarbeid mellom PST, NSM, Politiet og Næringslivets sikkerhetsråd (PST et al., 2017).

Denne veilederen refererer til den Australske regjerings håndbok i personellsikkerhet (Australian Government, 2014), men har omarbeidet definisjonene. Veilederen (PST et al., 2017) beskriver en innsider som «*en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt autorisert tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som* ***misbruker*** *denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap*» (s. 4). Veilederen deler innsidere i tre kategorier. Den første kategorien er infiltratøren som er plassert av en tredjepart, den andre er den selvmotiverte som utfører handlinger på eget initiativ og ikke er i befatning med en tredjepart, og den tredje er den rekrutterte som jobber på vegne av en tredjepart og er rekruttert etter at innsideren har fått tilgang til verdier. Uten å inkludere den i innsiderkategoriene, omtaler denne veilederen i tillegg en fjerde kategori som omfatter både de som er manipulert eller forledet av en tredjepart og de som ikke selv forstår konsekvensene av sine handlinger (PST et al., 2017, s. 5). Veilederen har ingen klar beskrivelse av innsidetrussel, men har definert trusselaktør som «en aktør som ønsker å utføre en handling eller påvirke andre på en måte som er i strid med norske sikkerhetsinteresser eller en bestemt virksomhets interesser» (PST et al., 2017, s. 18).

Årlig utarbeider PST og Etterretningstjenesten hver sin trusselvurdering som de siste årene har blitt lagt fram og presentert offentlig i et samarbeid med NSM. NSM legger samtidig fram sin nasjonale risikovurdering som har fokus på hvordan trusselaktører kan utnytte sårbarheter i samfunnet og virksomheter, og hvilken risiko dette medfører. Rapporten fra NSM har også fokus på hvordan sårbarhetene bør reduseres (NSM, 2022d, s. 4).

PST setter i sin trusselvurdering for 2022 (PST, 2022, ss. 9-10) fokus på hva som påvirker og får personer til å utføre handlinger som fører til negative konsekvenser. Handlingene kan være i form av informasjonslekkasje grunnet statlig etterretningsvirksomhet, og volds-, sabotasje eller terrorhandlinger grunnet radikalisering, ideologi eller antistatlige overbevisninger. Begrepet innsider defineres ikke i denne rapporten og benyttes heller ikke.

Men som eksempel belyses trussel fra statlige etterretningsvirksomhet som rekrutterer personer for å få tilgang til informasjon. Personer som er av interesse for etterretningsvirksomhet kan være personer som selv har tilgang til sensitiv informasjon eller personer som har denne tilgangen gjennom sitt nettverk av familie, kollegaer eller andre bekjente.

Etterretningstjenesten har i Fokus 2022 (Etterretningstjenesten, 2022) fokus på internasjonale truslers påvirkning på norske interesser. Et av områdene som framheves er etterretningstrusselen fra Russland og Kina. Norge er et attraktive mål fordi vi er langt framme både innen næringsliv og teknologiutvikling og forskning. Påvirkning av og informasjonsinnhenting fra enkeltpersoner er blant virkemidlene som benyttes, men heller ikke denne rapporten definerer hva som legges i begrepet innsider.

NSM påpeker innsiderisikoen i sin risikorapport for 2022 (NSM, 2022d, ss. 29-30), men henviser til Temarapporten om Innsiderisiko (NSM, 2019d) for detaljer om temaet.

NSM har en egen Temarapport om innsiderisiko (NSM, 2019d) for å øke kunnskapen og motstandsdyktigheten gjennom gode forebyggende tiltak hos både offentlige og private virksomheter. I rapporten beskriver NSM innsideren som «en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som **misbruker** denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap» (NSM, 2019d, s. 9). Innsideren kan være personer som kan påvirke, som har framtidig potensial, som kan skaffe seg tilgang, som har direkte tilgang eller som kan utnyttes for eksempel ved manipulasjon. Innsiderisikoen belyses ved å se på innsiderens intensjon, kapabilitet og mulighet.

I rapporten (NSM, 2019d, ss. 8-13) deles innsidere inn i de ubevisste, uten intensjon, og de bevisste, som har intensjon. En ubevisst innsider kan med sine tilganger til en virksomhets verdier påføre virksomheten skade eller tap, uten vilje eller intensjon om å gjøre det. Mangelfull kjennskap til sikkerhetsregler og rutiner, uoppmerksomhet eller lignende kan være årsaken til at en person kompromitterer informasjon eller forårsaker annen skade. Personen kan også bli utnyttet eller manipulert på annen måte av en tredjepart til å begå handlinger med skade eller tap som konsekvens for virksomheten, eksempelvis avsløre sensitiv informasjon. Den bevisste innsideren beskrives som en innsider med intensjon om å begå en handling i strid med en virksomhets interesser, men som ikke alltid er kjent med alle

konsekvenser handlingen medfører. Den bevisste innsideren kategoriseres i den *selvmotiverte*, som ikke er påvirket av noen tredjepart, *infiltratøren* som søker seg bevisst til en virksomhet med intensjon om å kunne utnytte sin posisjon, gjerne rekruttert av en tredjepart, eller i den *rekrutterte* som rekrutteres av en tredjepart gjennom press eller annen påvirkning etter å ha kommet i en posisjon som gir tilgang til en virksomhets verdier, men som ikke på forhånd hadde noen intensjon om å bli en bevisst innsider.

NSMs Grunnprinsipper for personellsikkerhet (2021) beskriver ikke eksplisitt begrepet innsider, men deler innsidere i ubevisst og bevisst, hvor den bevisste enten er selvmotivert eller påvirket av en ekstern aktør (NSM, 2021, s. 4). I tillegg defineres innsidevirksomhet som «tilfeller der en nåværende eller tidligere medarbeider misbruker sin tilgang eller kunnskap for å utføre handlinger som påfører virksomheten skade eller tap» hvor medarbeider omfatter «faste, midlertidige og innleide medarbeidere» (NSM, 2021, s. 4).

4.2 Risikovurdering

Blant annet PST og NSM har trukket fram innsiderisikoen som en betydelig risiko, med svært høyt skadepotensial. Sikkerhetstiltak som er etablert med hensikt å stoppe eksterne aktører kan miste sin effekt om trusselen kommer fra en som befinner seg på innsiden, og som har tilgang til verdiene. (Meld. St. 5 (2020-2021), s. 77). For å ha et forsvarlig sikkerhetsnivå og kontroll på virksomhetens verdier må risikoen knyttet til de viktigste verdiene kontinuerlig vurderes og håndteres (NSM, 2019c, s. 5).

4.2.1 Storbritannia - Veileder for risikovurdering

CPNI kom i juli 2022 med en veileder (CPNI, 2022b) for rollebasert, forebyggende risikovurdering. Målet med den rollebaserte risikovurderingen er å forstå den potensielle innsiderisikoen som eksisterer i organisasjonen, basert på hvilken tilgang til verdiene de enkelte rollene i organisasjonen har, vurdering av eksisterende sikkerhetstiltak som beskytter verdiene og hvilke konsekvenser uønskede innsidehandlinger kan føre til. I tillegg må forslag til nye eller endrede risikoreduserende tiltak prioriteres og planlegges. I veilederen er trussel definert som en fiendtlig aktørs intensjon og kapasitet til å iverksette handlinger mot en organisasjon, eksempelvis ved å skaffe seg informasjon digitalt eller å utføre et terrorangrep. Risikoen defineres som muligheten for at en slik handling iverksettes og konsekvensen av

handlingen. Innsider er definert som en som utnytter eller har til hensikt å utnytte sin legitime tilgang til en organisasjons eiendeler til uautoriserte formål. Innsideren kan være en heltids- eller deltidsansatt, en innleid eller en forretningspartner (CPNI, 2022b, s. 1). Innsidedefinisjonen er i overensstemmelse med CPNIs tidigere definisjon, innsider er den bevisste, ondsinnede personen på innsiden, definert som «en person som utnytter, eller har til hensikt å utnytte, sin legitime tilgang til en organisasjons eiendeler for uautoriserte formål» (CPNI, 2013a, s. 4; oversatt).

Som en forutsetning for risikovurderingen må organisasjonen ha gjennomført en kartlegging og klassifisering av sine eiendeler og systemer (verdier), for å prioritere beskyttelse av de verdiene som er viktigst for virksomhetens verdiskapning og operasjonelle drift . I tillegg må virksomheten gjøre seg kjent med, og vurdere, hvilke trusler som anses å være de mest truende for virksomheten, både med hensyn til intensjon og kapasitet.

Risikovurderingen startes med å sette sammen ett tverrfaglig team som kjenner organisasjonen og har god kunnskap om de eiendeler og systemer som anses å være mest kritiske. Hensikten er å gå gjennom scenarier for potensielle uønsket innsideaktivitet rettet mot organisasjonens kritiske verdier, det vil si vurdere muligheten for at en handling kan gjennomføres, av hvilke roller i organisasjonen, og kartlegge konsekvensene en slik handling kan føre til. Den rollebaserte risikovurderingen må gjennomføres så detaljert at det er mulig å komme fram til risikoreduserende tiltak (barrierer), tiltak som reduserer både muligheten for at handlingen inntreffer og virkningen av innsideaktiviteten. I en stor organisasjon kan det være nødvendig at den rollebaserte vurderingen gjennomføres også på flere nivåer i organisasjonen for å dekke alle områder. Veilederen (CPNI, 2022b) foreslår derfor å ta utgangspunkt i noen hovedtyper for innsiderisiko for at organisasjonen skal følge samme prosess for risikovurderingen dersom den skal gjennomføres i flere deler av organisasjonen. Samtidig må ikke hovedtypene begrense vurderingen, det er viktig også å ta med annen relevant uønsket innsideaktivitet i vurderingen. De fem hovedtypene CPNI foreslår er:

1. Uautorisert deling av sensitiv informasjon med en tredjepart – bevisst, for eksempel ved å dele tekniske tegninger med en konkurrent, eller ubevisst, for eksempel ved en feil å sende en epost med sensitiv informasjon til feil mottaker
2. Prosesskorrupsjon – for eksempel av en økonomisk prosess for å muliggjøre svindel
3. Tilrettelegging for tredjeparts tilgang til verdier – for eksempel ved å slippe uautorisert inn på område som krever autorisasjon

4. Fysisk sabotasje – for eksempel ødelegge maskiner i produksjonslokalene
5. IT eller elektronisk sabotasje – for eksempel laste ned eller installere skadelig programvare som ødelegger data på serverne

Ved vurdering av mulighet for innsideaktivitet må eksisterende forebyggende barrierer tas med i betraktning, om de er hensiktsmessige og tilstrekkelige. Det samme gjelder i forhold til eksisterende barrierer som er ment å redusere effekten av en hendelse, har de forventet effekt og er de hensiktsmessige i forhold til å redusere konsekvensen for den *aktuelle* hendelsen.

For hver av risikoene som identifiseres kartlegges det hvilke roller som har tilgang og mulighet til å gjennomføre handlingen.

CPNI (2022a) (2022b) foreslår bruk av en standard 5 x 5 mulighet-konsekvens matrise for å visualisere de rollebaserte risikoene. Etter å ha innført risikoreduserende tiltak må risikovurderingen gjennomgås på nytt for å se hvordan endringene har påvirket risikobildet, og ved behov må underlaget oppdateres.

CPNI har også en veileder for personellsikkerhetsrisikovurdering fra 2013 (CPNI, 2013b).

Denne veilederen (CPNI, 2013b, s. 5) bryter sannsynlighet for at en innsidehendelse vil finne sted ned i de tre faktorene 1) en *innsiders* intensjon eller motivasjon til å utføre handlingen, 2) i hvilken grad innsideren har ferdigheter, kunnskaper og ressurser til å lykkes i forsøket, og til sist 3) muligheten innsideren har til å gjennomføre handlingen, gjennom tilgang til verdiene kombinert med sårbarheten i beskyttelsestiltakene for verdiene. Det bør også vurderes hvor realistisk det er at akkurat denne organisasjonen er utsatt for type trussel som vurderes, for eksempel om lignende hendelser har skjedd tidligere, hvordan sikkerhetstilstanden og -kulturen er i organisasjonen og evnen de ansatte har til å gjennomføre den type handling (CPNI, 2013b, ss. 9-10).

I veilederen fra 2013 (CPNI, 2013b, ss. 4-18) gjennomføres de forskjellige stegene i risikovurderingen på forskjellige nivåer i organisasjonen.

- **Organisasjonsnivå** – identifisere spekteret av innsidetrusler som organisasjonen står overfor, eksempelvis fysiske angrep og uautorisert deling av sensitiv informasjon, og deretter prioritere truslene i forhold til sannsynlighet og forventet effekt.

- **Gruppenivå** – identifisere hvilke grupper av ansatte som har best tilgang på de prioriterte verdiene og av den grunn størst mulighet for å kunne gjennomføre truslene identifisert på organisasjonsnivå. Evnen til å gjennomføre trusselen må også vurderes, eksempelvis teknisk kunnskap. Derimot er motivasjon ikke en del av risikovurderingen og det er viktig å holde utenfor antagelser om eksempelvis at trusselen om tyveri er mer sannsynlig i en gruppe ansatte med lavere lønn. Å ta inn slike antagelser kan føre til unøyaktigheter i risikovurderingen.
- **Rollebasert (individ)** – ressurskrevende vurdering som krever nøkkelperson som har god kunnskap om rollen og tilgangen den gir.

Når vurdering på *gruppenivå* er gjennomført, vurderes tilstrekkeligheten av eksisterende sikkerhetstiltak i forhold til å redusere risikoen for de enkelte gruppene. Ved behov, identifiseres eventuelt nye sikkerhetstiltak, eller tilpasning av de eksisterende for bedre å imøtegå truslene. Det settes også opp et forslag til plan for innføring av endringer og nye sikkerhetstiltak.

Den *rollebaserte* vurderingen er ressurskrevende og gjennomføres derfor gjerne kun for høyrisikoroller som krever egne detaljerte risikovurderinger. Denne vurderingen kan være nyttig for å få inngående kunnskap om hvor mye tilgang den enkelte rolle har. Det er viktig å legge merke til at en rollebasert risikovurdering benyttes til å vurdere rollen, ikke personen som innehar rollen eller en stilling.

På samme måte som for andre risikovurderinger er det viktig at informasjonen som kommer fram, beslutningene som tas og logikken bak beslutningene, dokumenteres, og at dataene beskyttes. Beskyttelse av dokumentasjonen er spesielt viktig ved gjennomføring av rollebaserte risikovurderinger da den vil inneholde detaljert informasjon om sårbarheter i organisasjonen.

4.2.2 Norge - Sikkerhetslovens krav til risikovurdering

I likhet med andre lover fastsetter sikkerhetsloven (2018) rettigheter og plikter som kan håndheves ved en norsk domstol. Utfyllende bestemmelser, som er bindende på samme måte som loven, fastsettes i forskrifter. For virksomheter som er omfattet av sikkerhetsloven er det virksomhetsikkerhetsforskriften (2018) som er mest aktuell. I tillegg gis det føringer for tolkning og anvendelse av lov og forskrift i form av veiledere. For sikkerhetsloven er det NSM som gir veiledning.

Sikkerhetsloven har som formål å bidra til å trygge Norges nasjonale sikkerhetsinteresser og at sikkerhetstruende virksomhet forebygges, avdekkes og motvirkes (Sikkerhetsloven, 2018, ss. § 1-1 punkt a-b). Loven stiller eksplisitt krav til at «Virksomheten skal gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet» (Sikkerhetsloven, 2018, ss. § 4-3 første ledd første punktum). Med sikkerhetstruende virksomhet menes tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. De handlingene som *direkte* kan skade omfatter blant annet sabotasje- og terroraksjoner der målet med handlingene er å ramme viktige samfunnsfunksjoner. Med tilsiktede handlinger som *indirekte* kan skade, menes handlinger der konsekvenser som følger av handlingene kan skade sikkerhetsinteressene, men hvor dette ikke hvor dette ikke var intensjonen eller målet med handlingen.

Sikkerhetsloven (2018, ss. § 4-2) setter krav til at risikovurdering skal gjennomføres og være grunnlag for det forebyggende sikkerhetsarbeidet i virksomheter som er underlagt loven. Virksomhetsikkerhetsforskriften (2018, s. § 12) beskriver hvordan vurdering av risiko skal gjennomføres. Risikovurderingen skal omfatte verdier, identifisering av trusler mot verdiene, sannsynlighet for hendelser, avdekking av sårbarheter, konsekvenser og avhengighet til andre virksomheter. Det anbefales at risikovurderinger gjennomføres etter anerkjente standarder som NS 5814, NS 583x-serien eller ISO31000-serien (NSM, 2019c, s. 7). NSM anbefaler i sin veileder for sikkerhetsstyring (NSM, 2019c, ss. 5-6) at det benyttes scenarioer for relevante uønskede hendelser og at det avdekkes *sårbarheter* i forhold til menneskelige forhold som påvirkning av personell i roller med betydning for sikkerhet i virksomheten, eksempelvis gjennom sosial manipulasjon.

Veilederen ((NSM, 2019c, ss. 7-8) anbefaler å gjøre en konkretisering av mulige aktører bak hendelsen, med vurdering av tilhørighet til virksomheten. Tilhørighet kategoriseres som

- eget personell med tilgang,
- eget personell uten tilgang og
- eksternt personell.

Aktørene bør også vurderes med hensyn til kapasitet (eller evne) og intensjon (eller vilje). Intensjonen kategoriseres som

- ubevisst, uønsket handling

- bevisst, opportunistisk handling og
- handling med hensikt og plan.

Sikkerhetsloven (2018) setter krav til at virksomheter skal etablere sikkerhetstiltak for å redusere risikoen knyttet til sikkerhetstruende virksomhet. Dette er utdypet av NSM (2019c, ss. 20-22) som grunnsikringstiltak (sikkerhetstiltak i normalsituasjon), påbyggingstiltak (tiltak som iverksettes ved forhøyet trussel) og tiltak for skadebegrensning og gjenoppretting. Tiltakene kan være fysiske, elektroniske, menneskelige eller organisatoriske og følger prinsipper om

- minimalisme
- minste privilegium
- sikring i dybden
- motstandsdyktighet
- balansert styrke.

4.2.3 NSM Grunnprinsipper for personellsikkerhet

NSM har utarbeidet grunnprinsipper for personellsikkerhet (NSM, 2021, ss. 4-5), et sett med anbefalte tiltak for å motvirke innsidetrusselen. Grunnprinsippene beskriver bare i liten grad hvordan tiltak bør gjøres da fokuset er på **hva** og **hvorfor,** og det er opp til den enkelte virksomhet å vurdere hvilke konkrete tiltak som er aktuelle for seg.

Grunnprinsippene (NSM, 2021) anbefaler at det gjennomføres stillings- og oppdragsspesifikke risikovurderinger for å kartlegge hvilke stillinger og oppdrag som kan gi «betydelig innblikk i sentrale deler av virksomheten, eller som av andre grunner kan gjøre medarbeidere særlig utsatt for rekrutteringsforsøk eller andre trusler» (NSM, 2021, s. 6). Som en del av denne risikovurderingen anbefales en vurdering av konsekvensene ved innsidevirksomhet i de konkrete stillingene eller oppdragene og om det bør innføres tiltak som mer omfattende bakgrunnsundersøkelse og sikkerhetsopplæring for medarbeidere i utsatte stillinger (NSM, 2021, s. 6).

I forbindelse med rekruttering anbefales bakgrunnsundersøkelser av søkerne for å avdekke sårbarheter ved personen som kan påvirke virksomhetens risikobilde ved en ansettelse (NSM, 2021, s. 6). Underveis i ansettelsesforholdet anbefales sårbarhetsoppfølging av medarbeiderne underveis i ansettelsesforholdet for oppfølging og implementasjon av tiltak

for å redusere risiko, og for identifisering av nye sårbarheter «som vil kunne lede til ubevisst innsidevirksomhet og/eller utnyttes av en trusselaktør» (NSM, 2021, ss. 9-12). Nye sårbarheter kan eksempelvis oppstå som følge av manglende sikkerhetsmessig bevissthet, misnøye på arbeidsplassen eller andre endringer i medarbeiderens liv.

4.2.4 Veileder – Sikkerhet ved ansettelsesforhold

PST, NSM, Politiet og NSR sin Veileder om Sikkerhet ved ansettelsesforhold (PST et al., 2017) er ment som et hjelpemiddel til både offentlige og private virksomheter, men er tydelig på at den «ikke skal benyttes i tilfeller der sikkerhetsloven stiller krav til sikkerhetstiltak overfor ansatt personell» (PST et al., 2017, s. 4).

I veilederen oppfordres det til at sikkerhetsarbeidet settes i system, både for å få oversikt over og kunne opprettholde en tilfredsstillende sikkerhetstilstand (PST et al., 2017, s. 6). Den oppfordrer til at verdiene i virksomheten bør kartlegges, spesielt utsatte stillinger og oppgaver identifiseres og rutiner for bakgrunnssjekk for de utsatt oppgavene eller stillingene etableres (PST et al., 2017, s. 7). Bakgrunnssjekken kan avdekke om opplysningene en jobbkandidat oppgir er korrekte og den kan avdekke eventuelle sårbarheter ved personen som eksempelvis en økonomisk situasjon som er ute av kontroll.

4.3 Personellsikkerhet

Personellsikkerhet handler om å forebygge, avdekke og motvirke handlinger som kan true sikkerheten og som begås av personer med tilgang til verdiene en organisasjon ønsker å beskytte. Personellsikkerhet skal bidra til å sikre at personell som har tilgang til sensitiv informasjon og andre verdier, har den nødvendige lojalitet, pålitelighet og tillit i et sikkerhetsmessig perspektiv og skal sørge for at den menneskelige faktor i sikkerhetsarbeidet bidrar til å styrke sikkerheten, ikke svekke den. Dette omfatter blant annet å håndtere menneskelige sårbarheter (Meld. St. 5 (2020-2021), s. 77) (NOU 2016: 19, 2016, s. 192).

Sikkerhetsloven regulerer dette ved å sette krav til sikkerhetsklarering og tilhørende autorisasjon for å få tilgang til sikkerhetsgradert informasjon.

4.3.1 Sikkerhetsklarering

NSM gir i sin veileder for personellsikkerhet (NSM, 2019b) veiledning i forhold til sikkerhetsklarering, både for de organisasjoner som har behov for sikkerhetsklarert personell og for klareringsmyndigheten.

Fra sikkerhetsloven (2018) stilles kravet om at personer som skal få tilgang til sikkerhetsgradert informasjon på nivå KONFIDENSIELT og høyere må ha gyldig sikkerhetsklarering og autorisasjon (Sikkerhetsloven, 2018, ss. § 8-1).

NSM (2019a) detaljerer dette ved å forklare at sikkerhetsklarering er en avgjørelse fattet av en *klareringsmyndighet* om en persons antatte skikkethet for å behandle sikkerhetsgradert informasjon, mens autorisasjon er en godkjenning gitt av personens *autorisasjonsansvarlig* slik at personen skal få tilgang til sikkerhetsgradert informasjon og adgang til skjermingsverdige objekter og infrastruktur i virksomheten. Hensikten med sikkerhetsklarering og autorisasjon er å beskytte virksomheter mot personer som på eget initiativ, eller fordi personen fristes, forledes, presses eller trues til å begå handlinger som truer sikkerheten og setter nasjonale sikkerhetsinteresser i fare

Avgjørelse om en person skal få sikkerhetsklarering fattes av en klareringsmyndighet. «En person kan bare klareres dersom det ikke finnes rimelig grunn til å tvile på om personen er sikkerhetsmessig skikket» (Sikkerhetsloven, 2018, ss. § 8-4) og det skal «legges vekt på forhold som er relevante for personens pålitelighet, lojalitet og dømmekraft i forbindelse med behandling av gradert informasjon og tilgang til skjermingsverdige objekter og infrastruktur» (Sikkerhetsloven, 2018, ss. § 8-4).

Personkontroll beskrives av NSM (2019b, ss. 13-14) som noe som skal gjennomføres av alle som skal klareres. Vurderingsgrunnlaget for personkontrollen omfatter opplysninger personen selv oppgir enten skriftlig eller gjennom en sikkerhetssamtale med klareringsmyndigheten, samt opplysninger fra relevante registre. Det kan også gjennomføres en personkontroll av nærstående personer. I sikkerhetsloven (2018, ss. § 8-4) og klareringsforskriften (2018, s. § 8) finnes det oversikt over hvilke opplysninger klareringsmyndigheten kan tillegge vekt i sin vurdering, samt hvilke registre NSM kan innhente og videreformidle opplysninger fra. Verifikasjon av informasjonen kan eksempelvis gjøres med innhenting av opplysninger far registre, innhenting av uttalelser ved bruk av epost og referansesamtaler (NSM, 2019b, s. 53).

Klareringsmyndigheten kan gi klarering som anmodet, gi klarering på et lavere nivå enn anmodet, det kan settes vilkår som reduserer risikoen ved å gi personen klarering, eller avgjørelsen kan være at klarering ikke innvilges (Virksomhetsikkerhetsforskriften, 2018, s. § 21).

Som (NSM, 2019b, s. 62) forklarer er det virksomheten som har behov for sikkerhetsklarert personell som igangsetter klareringsprosessen og som framsender underlag fra personen som skal klareres sammen med dokumentert begrunnelse på behov. En sikkerhetsklarering har en varighet på inntil fem år, men kan gis for kortere perioder, og seks måneder før en sikkerhetsklarering utløper er det virksomheten som vurderer om det fortsatt er et behov og iverksetter en ny søknad om klarering.

Ved negativ avgjørelse på søknad om klarering settes det som oftest en karantenetid, hvor maksimal lengde er fem år, og personen får i denne perioden status INGEN KLARERING. Etter karantenetidens utløp kan det igjen søkes om sikkerhetsklarering. Søknaden vil bli behandlet som en ny søknad, hvor utfall ikke er gitt selv om karantenetiden er utløpt (NSM, 2019b, s. 59).

Klareringsmyndigheten har mulighet for å tilbakekalle, nedsette eller suspendere en sikkerhetsklarering som tidligere er innvilget. Dette gjøres på bakgrunn av nye opplysninger som klareringsmyndigheten har mottatt. Suspensjon er en midlertidig avgjørelse mens klareringsmyndigheten jobber med å opplyse saken for å kunne gjøre en helhetlig vurdering (NSM, 2019b, s. 19).

4.3.2 Autorisasjon

Autorisasjon er i praksis et spørsmål om en persons autorisasjonsansvarlig har den nødvendige tillit til at personen som skal autoriseres er i stand til å håndtere sikkerhetsgradert informasjon (NSM, 2011, s. 3). Før autorisasjon kan gis skal det gjennomføres en autorisasjonssamtale.

Fra virksomhetsikkerhetsforskriften (2018) settes kravene til autorisasjonssamtalen. Autorisasjonsansvarlig skal gjennom autorisasjonssamtalen «

a) forsikre seg om at den som skal autoriseres, kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser og forstår sin rolle i sikkerhetsarbeidet til virksomheten

b) kontrollere at opplysningene den som skal autoriseres, gir, er tilstrekkelige og oppdaterte
c) drøfte eventuelle risikofaktorer ved personen som er relevante for personellsikkerheten
d) drøfte tiltak som kan redusere risikofaktorer ved personen, eller som kan oppfylle vilkår som klareringsmyndigheten har gitt for klareringen» (Virksomhetsikkerhetsforskriften, 2018, s. § 68 andre ledd).

Veilederen (NSM, 2019b, s. 21) beskriver videre at nye opplysninger som framkommer og som kan påvirke en persons *sikkerhetsmessige skikkethet* er det den autorisasjonsansvarlige som skal vurdere om autorisasjon skal opprettholdes, tilbakekalles, nedsettes eller suspenderes. Eksempel på dette kan være at en person får en ny partner med statsborgerskap fra et land som Norge ikke har sikkerhetsmessig samarbeid med, eller at det oppstår utfordringer med psykisk helse eller økonomi. Autorisasjonsansvarlig kan også sette en persons autorisasjon ned, det vil si at personen kun vil få tilgang til informasjon på et lavere graderingsnivå enn nivået som sikkerhetsklareringen er gitt eller ikke tilgang gradert informasjon.

Det er leder av organisasjonen som er autorisasjonsansvarlig, men myndigheten til å autorisere kan ved behov delegeres (NSM, 2019b, s. 20). NSM (2011) anbefaler at muligheten anvendes med forsiktighet, men ser det kan være nødvendig der en organisasjon har et stort behov for autorisasjon.

4.3.3 Varslingsplikt

Sikkerhetsloven (2018) pålegger en person med sikkerhetsklarering og autorisasjon en plikt til å varsle om endringer og forhold som kan være av betydning for sikkerhetsmessig skikkethet (§ 8-11).

Autorisasjonsansvarlig skal vurdere om opplysningene potensielt vil kunne ha en påvirkning på personens pålitelighet, lojalitet og dømmekraft, og om det er behov for en ny autorisasjonssamtale samt vurdering av autorisasjon (Virksomhetsikkerhetsforskriften, 2018, s. § 68). Klareringsmyndigheten skal informeres dersom det framkommer opplysninger som fører til en ny vurdering av en persons autorisasjon, også selv om autorisasjonen opprettholdes.

5 DRØFTING / DISKUSJON

I dette kapitlet drøftes empirien fra litteraturstudiene i lys av tidligere presentert teori for å komme fram til svar på problemstillingen

Hvordan kan bruk av sikkerhetsklarering påvirke vurderingen av innsiderisiko?

Det er etablert tre forskningsspørsmål for å belyse problemstillingen, og disse vil bli drøftet i kapitlene som følger.

5.1 Definere en innsider

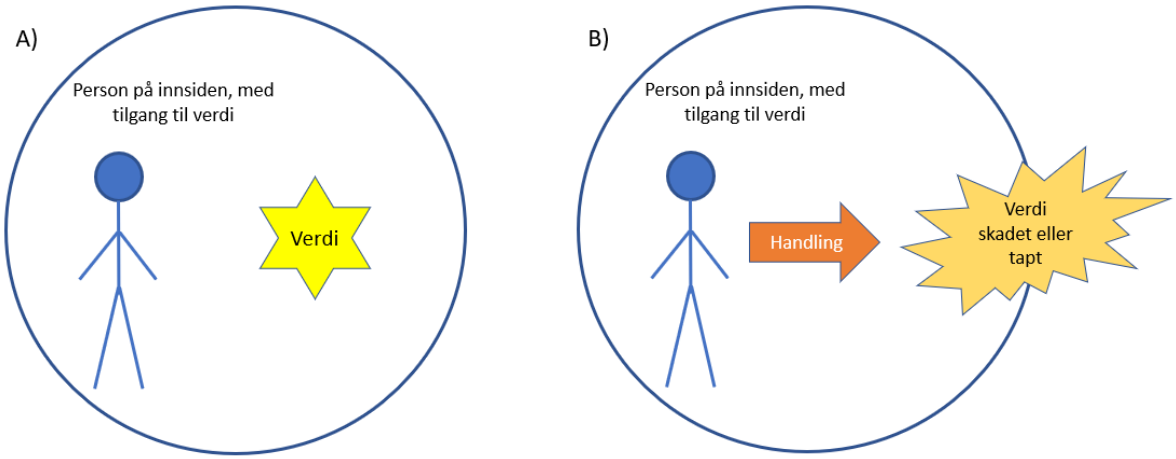
For å kunne si noe om hvordan sikkerhetsklarering kan påvirke vurdering av innsiderisiko, må det være tydelig hva som inngår i begrepet innsider. Empirien viser at det ikke er entydig hva forskjellige miljøer legger i begrepet og at det også er forskjeller mellom de landene som er undersøkt, USA, Storbritannia, Australia og Norge.

For å svare på oppgavens problemstilling «*Hvordan kan bruk av sikkerhetsklarering påvirke vurderingen av innsiderisiko?*» er første forskningsspørsmål:

1) Hvordan defineres en innsider?

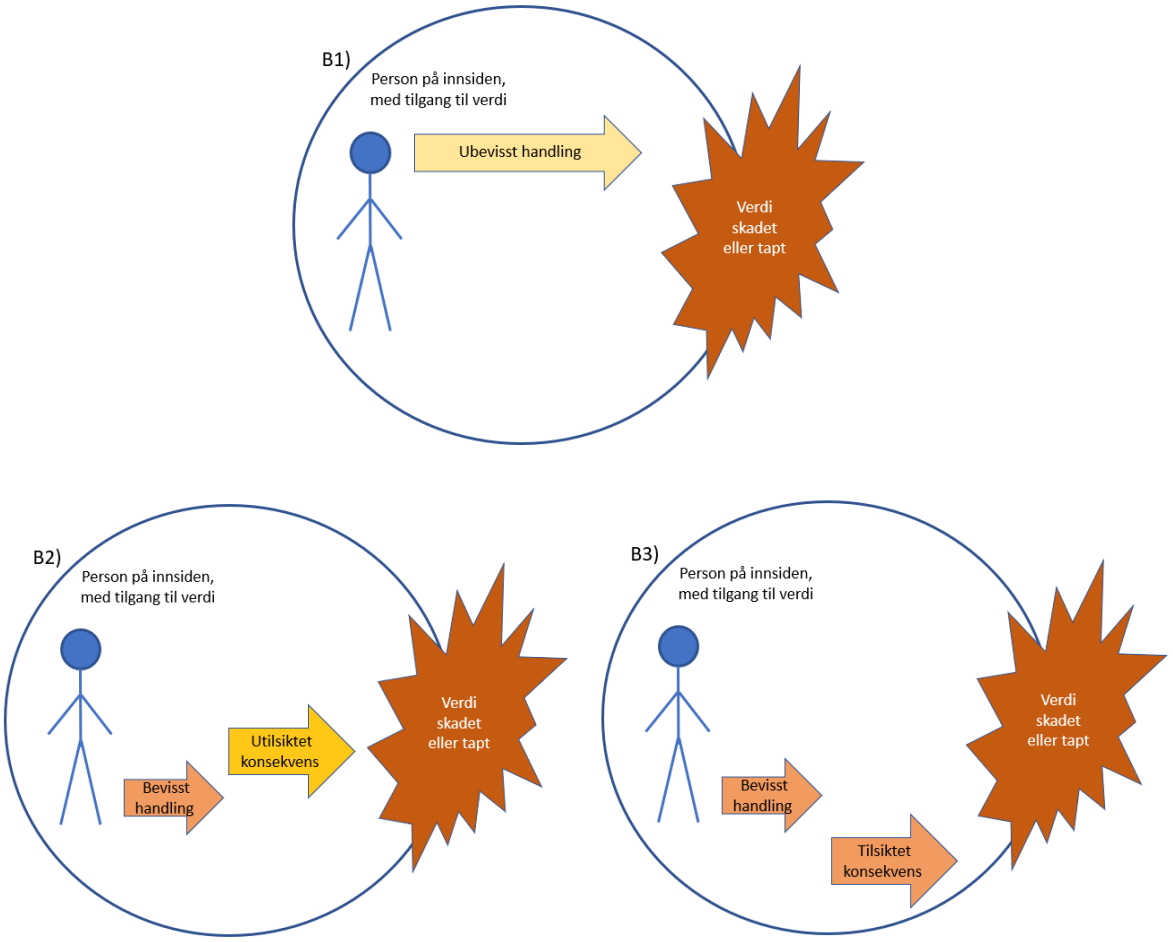
5.1.1 Perspektiver på innsider

Perspektivene på hva som er en innsider varierer mellom A) en innsider er enhver person som har eller har hatt tilgang til en organisasjons verdier, eksempelvis en nåværende eller tidligere ansatt, innleid eller en partner, og B) en innsider er en person med tilgang til en virksomhets verdier og som *utfører en handling* som leder til negativ konsekvens for virksomheten gjennom skade eller tap av verdi, se Figur 8. Perspektiv B legger til grunn at det *kun* er personer som utfører handlinger hvor verdi skades eller tapes som hører inn under betegnelsen innsider. Perspektiv B kan derfor anses som en delmengde av perspektiv A som omfatter alle personer med tilgang eller med tidligere tilgang.



Figur 8 – Perspektiv på innsider

Men utgangspunkt i perspektiv B er det i tillegg forskjellige fortolkninger av hva som definerer en innsider, sett i forhold til handlingen som utføres og konsekvensen av denne handlingen, illustrert i Figur 9.

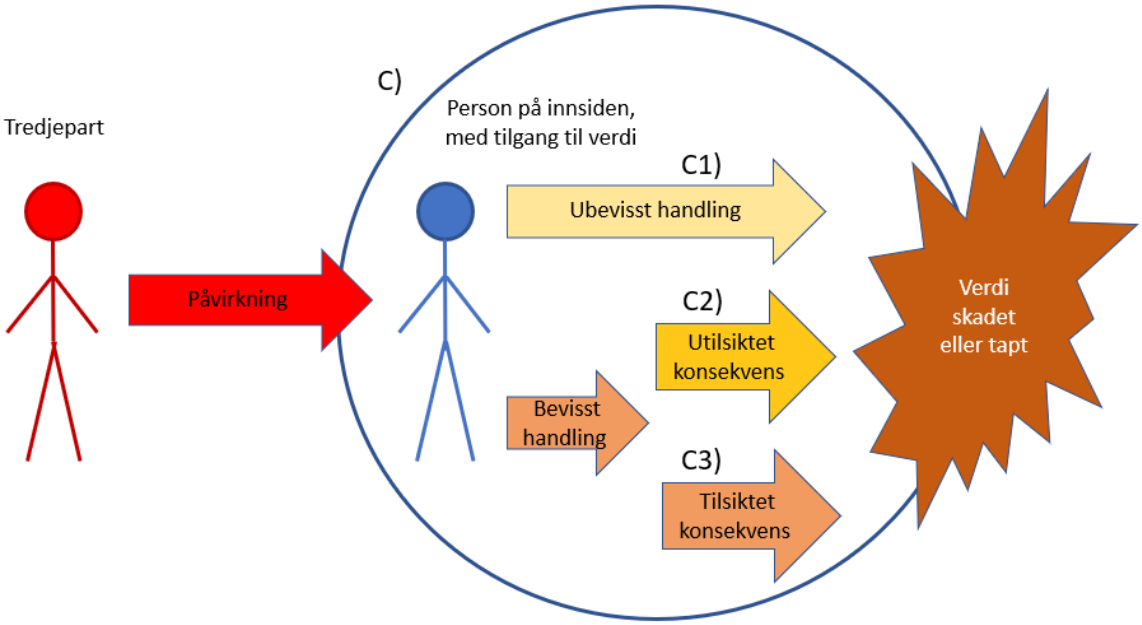


Figur 9 – Person på innsiden utfører handling som fører til skade eller tap

En uønsket hendelse kan skyldes en person som utfører en handling uten bevissthet og intensjon om å skade virksomheten (B1), ofte omtalt som en ubevisst innsider. Dette kan være en ansatt som i et øyeblikk av uoppmerksomhet klikker på en lenke som forårsaker at skadevare lastes ned på serveren, eller det kan være en ansatt som ved en feil legger ved en fil med sensitivt innhold som vedlegg i en epost til en konkurrent som ikke skulle hatt tilgang til denne informasjonen.

Det motsatte av den ubevisste er den ansatte som *bevisst* utfører en handling (B2 og B3). Variant B2 er en person som utfører en handling med de beste intensjoner, men hvor handlingen likevel fører til tap eller skade for virksomheten. Dette kan eksempelvis være en ansatt som foretar en opprydding på serverne og som sletter viktige data det ikke finnes kopier av. Variant B3 er den ansatte som helt bevisst og med viten og vilje utfører handlinger som vil skade virksomheten. Dette kan være lekkasje av informasjon til en konkurrent eller en fremmed etterretningstjeneste, eller det kan være sabotasje av viktige maskiner i produksjonen som forsinker kundeleveranser.

Som en ekstra faktor til perspektiv B, som isolert sett tar for seg selvmotiverte handlinger av en person på innsiden, kan personen på innsiden påvirkes av en tredjepart. Dette er illustrert som C (C1, C2 og C3) i Figur 10.



Figur 10 – Tredjepart påvirker person på innsiden til å utføre handling som fører til skade eller tap

En tredjepart er en aktør som bruker personen på innsiden som et verktøy for å lykkes med å oppnå egne mål. Tredjepart kan være alt fra en vinningskriminell som er ute etter PC-utstyr eller å svindle virksomheten til å utbetale penger, til en representant for en statlig etterretningstjeneste eller en terrorist. Tredjepart utnytter sårbarheter eller overbevisninger hos personen på innsiden og får denne personen til å utføre ønskede ubevisste handlinger (C1), bevisste handlinger, men uten at personen forstår konsekvensene (C2) eller bevisste handlinger med tilsiktede konsekvenser (C3).

I tillegg til faktorene som er belyst i perspektiv B og C kommer *hendelsesforløpet*, for personer som begår tilsiktede handlinger (B3 og C3). En person kan ha intensjon og motivasjon til å begå en handling, for deretter å posisjonere seg for å få tilgang til de aktuelle verdiene. Dette kan eksempelvis gjøres ved å søke seg til en spesifikk stilling i en virksomhet. Alternativt utløses motivasjonen til å handle som en utro tjener mens en person befinner seg i en stilling som gir muligheter og tilgang, uten at dette var et insitament for å gå inn i stillingen. Eksempelvis kan en ansatt som opplever å bli forbigått i en forfremmelse, eller ikke føler seg respektert eller sett av sjefen, føle seg misfornøyd og få et ønske om å hevne seg på virksomheten.

Når det gjelder hendelsesforløp og tredjepart er etterretningstjenester et eksempel på en tredjepart som jobber langsiktig, gjerne over flere år, og knytter til seg personer som de kan benytte på et senere tidspunkt. En person som jobber for en etterretningstjeneste kan «plasseres på innsiden» ved å søke seg til en stilling i en virksomhet for å tilgang til informasjon, for deretter å kopiere og utlevere dem til tredjeparten. Denne personen omtales gjerne som en infiltratør. På den annen side kan en person som allerede er i en posisjon med tilgang til viktige verdier rekrutteres av en tredjepart som kjenner, eller gjør seg kjent med, og utnytter personens sårbarheter. Tredjepart kan benytte seg av personens tillit, kommer med fristelser, eller framprovoserer frykt for å få personen på innsiden til å samarbeide.

5.1.2 Innsider – Innsidetrussel

For å tydeligere hva som legges i innsider-begrepet brukes beskrivende ord som for eksempel betrodd, bevisst, passiv, selvinitiert, rekruttert, ondsinnet, frivillig, ubevisst, infiltrert, utnyttet og selvmotivert. Men det som går igjen for alle definisjonene er at en innsider er en person som *befinner seg i en posisjon med tilgang til en virksomhets verdier* (perspektiv A). For en person som har tilgang til verdier vil det være mulighet for å utføre handlinger som kan

påvirke disse verdiene på en måte som fører til positive eller negative konsekvenser. Handlinger som gir negative konsekvenser er det som omtales som uønskede hendelser.

Det største spennet i fortolkningene av begrepet innsider ligger mellom perspektiv A, *enhver med autorisert tilgang*, som amerikanske myndigheter legger til grunn i sin definisjon, og perspektiv B3/C3 som britiske CPNI (2013a) benytter «en person som utnytter, eller har til hensikt å utnytte, sin legitime tilgang til en organisasjons eiendel for uautoriserte formål» (CPNI, 2013a, s. 4; oversatt) . CPNI (2013a, s. 9) inkluderer både personer som tar eget initiativ og de som er rekruttert av en tredjepart i sin bruk av innsiderbegrepet. Dette omfatter både hendelsesforløpet hvor personen søker seg til en stilling for å utnytte de tilgangene stillingen gir og de som bestemmer seg for å gjøre det uten at det var hensikten da de gikk inn i stillingen.

I en diskusjon om avgrensning av security som eget fagfelt, separert fra safety, setter Sissel H. Jore (2019) lys på hva som skiller security fra safety. Hun trekker fram at det er de *ondsinnede*, tilsiktede og bevisste handlingene som kjennetegner security truslene og hevder at det er fundamentale forskjeller på risikoen de ondsinnede, bevisste truslene representerer, kontra safety trusler som ubevisste handlinger er et eksempel på. Forskjellene gjør seg også gjeldene i forhold til hvilke tiltak som må iverksettes for å redusere de forskjellige risikoene. CPNI (2013a) har med sin definisjon av innsidere fokus på trusselen fra de personer som utøver, eller har til hensikt å utøve, bevisste handlinger for å utnytte tilgangene de har. Dette er det samme som å være bevisst, ondsinnet, og harmoniserer med det som Jore (2019) hevder kjennetegner security trusler. Sikkerhetstiltakene for forebygging av security truslene må tilpasses en tenkende trusselaktør som er ute etter å utnytte sårbarheter, og som tilpasser seg endringer i omgivelsene, som endring av eksisterende sikkerhetstiltak eller etablering av nye.

Ser vi på empirien fra Norge (NSM, 2019d, ss. 8-13) (NSM, 2021, s. 4) og Australia (Australian Government, 2010, s. 2) kategoriseres også en person som ubevisst, uten vilje eller intensjon (se B1 i Figur 9), utfører handling som påfører organisasjonen skade, enten på egenhånd eller påvirket av en tredjepart, som en innsider. Utfordringene med den utvidede definisjonen av innsider-begrepet er at det kreves andre sikkerhetstiltak for å forebygge truslene fra den ubevisste innsideren enn den bevisste ondsinnede innsideren. På den annen side kan det være hensiktsmessig å se på sikkerhetstiltak for forebygging av utilsiktede og

tilsiktede hendelser under ett, for å unngå konflikt mellom tiltakene og for å finne fram til optimale og kostnadseffektive løsninger (NOU 2016: 19, 2016, s. 14).

Ser vi på USA går det fram at det amerikanske sertifiseringsrammeverket CMMC (U.S. DoD, 2021) legger perspektiv A til grunn for betegnelsen innsider og at de ser på perspektiv B, den aktive handlingen, som innside*trusselen* «trusselen om at en innsider vil bruke sin autoriserte tilgang, bevisst eller ubevisst, for å skade organisasjonens eller USAs sikkerhet» (U.S. Department of Defense, 2021, s. 15; oversatt). Smith og Brooks (2013, s. 64) belyser trussel som fenomen og definerer det som faktorene *intensjon x kapasitet*. Intensjonen er *begjæret* i kombinasjon med *forventningen* om å lykkes, mens kapasiteten er *ressursene* i kombinasjon med *kunnskapen* som bidrar til at handlingene kan gjennomføres (se Figur 3). Å si at en person har tilgang til verdier (se A i Figur 8) sier noe om personens kapasitet i forhold til kunnskap om å få tak i verdien og påvirke den, men hvilke ressurser personen rår over og om det er noen intensjon om å begå en handling framgår ikke. Denne beskrivelsen er derfor mangelfull i forhold til å kvantifisere en trussel, men den belyser at det er en persons tilgang til verdier som ikke er tilgjengelig for alle og enhver som skiller en innsider fra de som er utenfor og ikke har den samme tilgangen.

Men om vi bruker innsidertrussel som begrep, skal vi da si at alle personer som befinner seg på innsiden (med tilgang til verdier), ikke bare er innsidere, men at de også er en trussel mot virksomheten? I realiteten kan alle med tilgang til verdier komme til å utføre handlinger som vil skade organisasjonen som eier verdien, enten bevisst, med eller uten intensjon om å skade, eller ubevisst som ved et uhell. For å være fleksibel nok til å ivareta alle muligheter for type innsidere og samtidig skille trusselen fra aktøren (personen) har SEI (Costa, 2017) etablert definisjonen «innsidetrussel er potensialet for en person som har eller hadde autorisert tilgang til en organisasjons kritiske eiendeler til å bruke denne tilgangen, enten ondsinnet eller utilsiktet, til å handle på en måte som kan påvirke organisasjonen negativt» (Costa, 2017; oversatt). For en organisasjon som skal gjøre en vurdering av innsidetrusselen kan organisasjonen selv fastsette hvilke individer og handlinger som er de mest aktuelle, eller som .2det skal fokuseres på, samt hvilke verdier som skal ivaretas og konsekvensene om de utsettes for uønskede handlinger (se Figur 7). Denne definisjonen kan derfor benyttes både av de som vil fokusere på security truslene, de ondsinnede, bevisste innsiderne, og for de som vil gjøre en helhetlig vurdering og inkludere alle type handlinger, uavhengig av om årsaken er en bevisst, forsettlig handling, eller en ubevisst handling.

Dette leder til at følgende definisjoner vil benyttes videre i drøftingen, med mindre annet spesifiseres:

- **Innsider** - enhver person som har eller har hatt tilgang til en organisasjons verdier, eksempelvis en nåværende eller tidligere ansatt, innleid eller en partner.
- **Innsidetrussel** – «potensialet for en person som har eller hadde autorisert tilgang til en organisasjons kritiske eiendeler til å bruke denne tilgangen, enten ondsinnet eller utilsiktet, til å handle på en måte som kan påvirke organisasjonen negativt» (Costa, 2017; oversatt).

5.2 Vurdering av innsiderisiko

«Mennesker er en organisasjons største ressurs, men i noen tilfeller kan de også utgjøre en innsiderisiko» (CPNI, 2021).

For å svare på oppgavens problemstilling «*Hvordan kan bruk av sikkerhetsklarering påvirke vurderingen av innsiderisiko?*» er det etablert et forskningsspørsmål nummer to:

> 2) Hvordan vurdere innsiderisiko i en virksomhet?

Med bakgrunn i at risiko er definert som ««usikkerhet knyttet til om en *uønsket hendelse* vil inntreffe og hvilke *konsekvenser* den kan få» (Midtgaard, 2021) og innsidetrusselen som «potensialet for en person som har eller hadde autorisert tilgang til en organisasjons kritiske eiendeler til å bruke tilgangen sin, enten ondsinnet eller utilsiktet, til å handle på en måte som kan påvirke organisasjonen negativt» (Costa, 2017; oversatt), kan innsiderisiko ses på som *usikkerhet* knyttet til om en person som har eller hadde autorisert tilgang til en organisasjons kritiske eiendeler bruker denne tilgangen, enten *ondsinnet eller utilsiktet*, til å *handle* på en måte som kan påvirke organisasjonen negativt og hvilke *konsekvenser* handlingen kan få.

Innsiderisikoen, eller *sannsynligheten* for en innsidehendelse, kvantifiseres ved å se på innsiderens intensjon, kapabilitet og mulighet (NSM, 2019d, s. 9). I dette perspektivet er det innside*trusselen* som står i sentrum for vurderingen, potensialet en innsider har til å misbruke tilgangen til virksomhetens eiendeler, enten ondsinnet eller utilsiktet. Dette potensialet er i første rekke avhengig av hvilken tilgang personen har til verdier (eiendeler og systemer) og hvor alvorlig det vil være for virksomheten dersom verdiene utsettes for skade eller tap. Det er ikke verken personens stilling eller betydning i forhold til en leveranse som er det

avgjørende. På den annen side kan også en person i en topplederstilling ha tilganger som kan være ødeleggende for virksomheten dersom denne personen har ondsinnede hensikter, eller en viktig produksjonsarbeider kan ved en forglemmelse (ubevisst) innføre en kritiske feil i et produkt ved å utelate et steg i sammenstillingsprosessen.

En forutsetning for å vurdere innsiderisiko er en oversikt over virksomhetens viktigste verdier. Dersom en slik oversikt ikke foreligger må verdiene kartlegges og de verdiene som er kritiske for at virksomheten skal være operativ og leveransedyktig må identifiseres (CPNI, u.å.) (NSM et al., 2015, s. 7). Denne anbefalingen fra empirien støttes av Njå et al. (2020, s. 258) som anbefaler å gjennomføre en systematisk verdikartlegging med vurdering av konsekvenser for virksomheten dersom verdiene ødelegges, kompromitteres eller endres.

Med utgangspunktet *enhver person med tilgang til verdier har potensial til å utføre handlinger som gir negativ effekt for organisasjonen*, legges grunnlaget for en analyse av den potensielle trusselen hver enkelt persons handlinger utgjør. For å vurdere risikoen må aktuelle scenarioer, sannsynligheten (mulighet, intensjon og kapasitet) for at den enkelte person utfører handlingene, og konsekvenser av hendelsene identifiseres. Det samlede resultatet fra hver av disse analysene vil til sammen danne et bilde av virksomhetens innsiderisiko. Empiriske data fra NSM (2021) og PST et al. (2017) understøtter dette ved sin vektlegging på å identifisere, følge opp og håndtere av den enkelte persons sårbarheter og endring i adferd. Den største ulempen med framgangsmåten er at den vil være svært ressurskrevende. Og med hensyn til alle faktorer som kan motivere noen til å bli en innsider, som for eksempel misnøye med arbeidsgiver, økonomi, ønske om hevn, søken etter spenning, samt faktorer som kan utløse uønskede hendelser som for dårlige sikkerhetsrutiner, manglende personlig sikkerhetsmessig dømmekraft, eller manglende opplæring, så vil trusselen som den enkelte person utgjør være i kontinuerlig endring.

Organisasjonsnivå

En alternativ framgangsmåte er å starte prosessen med å etablere et overordnet innsiderisikobilde på organisasjonsnivå med fokus på truslene som tiltrekkes av virksomhetens verdier, som ble funnet i veileder fra CPNI (2013b). Truslene identifiseres og det gjøres en vurdering i forhold til sannsynlighet og konsekvens (se skjematikk i Tabell 3 i vedlegg). For å oppnå en helhetlig vurdering av trusselen må forskjellige varianter av innsidehandlinger beskrevet tidligere i oppgaven tas med i betraktningen, se Figur 9 (ubevisst

handling (B1), bevisst handling med utilsiktet konsekvens (B2) og bevisst handling med tilsiktet konsekvens (B3)). Som et alternativ er det mulig å begrense analysen til for eksempel kun å ta for seg de bevisste handlingene med tilsiktet negativ konsekvens (security hendelser) for å belyse risikoen knyttet til den bevisste, ondsinnede personen på innsiden (B3).

CPNI (2022b) har identifisert fem hovedtyper innsideaktivitet, eller trusler, som utgangspunkt for vurdering av innsiderisiko, uautorisert deling av informasjon, prosesskorrupsjon, tilrettelegging for tredjepart, fysisk sabotasje og IT eller elektronisk sabotasje. På samme måte har studie om deteksjon og analyse av innsidetrusler gjennomført av NATO (Kont et al., 2015, s. 22) valgt å gruppere innsidere i forhold til type aktiviteter, sabotasje, tyveri, svindel, spionasje og utilsiktede hendelser. Forhåndsdefinerte innsideaktiviteter kan sikre bredden i vurderingen dersom det gjennomføres flere analyser hvor forskjellige personer deltar i hver av analysene, og det sikrer samtidig at alle analyser minimum vurderer de aktivitetene som er definert. Ulempen med predefinerte aktiviteter er at de kan virke begrensende for analysen i en slik grad at virksomhetens verdier og trusselbilde ikke blir godt nok ivaretatt. Som et alternativ kan innsidetruslene og innsideaktivitetene som er aktuelle for virksomheten identifiseres og vurderes på organisasjonsnivå, noe som anbefales i CPNIs veileder (CPNI, 2013b). En slik framgangsmåte stiller større krav til kompetanse hos de som deltar i analysen på organisasjonsnivå, og er derfor best egnet for virksomheter som har en viss modenhet på området. Samtidig kan dette være en god metode for å sikre at virksomhetens egenart ivaretas. Alternativt kan en gjøre begge deler. Enten starte med listen over forhåndsdefinerte hendelser som utgangspunkt og i tillegg gjøre en identifisering av andre aktuelle hendelser for egen organisasjon, eller gjøre en idémyldring for å komme fram til aktuelle hendelser og deretter sjekke mot lista om det er noe som er uteglemt og bør tas inn i vurderingen.

Innenfor det valgte omfanget for analysen, vil resultatet gi et overordnet bilde som synliggjør virksomhetens mest kritiske innsiderisikoer, basert på sannsynlighet og konsekvens. En rangering av de identifiserte og analyserte truslene gir føring for hvilke innsidetrusler som bør analyseres i mer detalj (CPNI, 2013b, ss. 11-14).

Gruppenivå

Etter en vurdering av trusler på organisasjonsnivå anbefaler empirien fra CPNI (CPNI, 2013b, s. 15) en identifisering av hvilken gruppering av personer eller roller som er i stand til

å gjennomføre innsidetruslene eller -aktivitetene, prioritert etter hvilke trusler som er høyest rangert. På dette nivået anbefaler CPNI (2013b) (2022b) at konkrete roller og stillinger identifiseres. SEI (Costa, 2017) kategoriserer personer i nåværende eller tidligere ansatte, fulltids- og deltidsansatte, innleide og pålitelige forretningspartnere i sitt diagram, se Figur 7, noe som er en grovere inndeling enn å identifisere de enkelte roller. NSM (2019c, s. 7) deler aktørene inn etter tilhørighet. Det skilles mellom eget personell med tilgang, eget personell uten tilgang og eksternt personell.

Grovinndelingen som NSM (2019c, s. 7) beskriver omfatter alle type aktører og er ikke spesielt innrettet mot innsiderisiko. For en vurdering hvor omfanget er begrenset til den potensielle trusselen fra personer som er på innsiden, og hvor det med dette menes «personer som har eller har hatt autorisert tilgang», vil alle aktører som vurderes havne i kategorien «eget personell». Denne inndelingen egner seg derfor ikke som en gruppeinndeling for vurdering av innsiderisiko.

SEI og CPNI har forskjellige betraktninger omkring hva en innsider er. CPNI (2013a, s. 9) ser på innsideren som en person som ondsinnet og bevisst har en intensjon om å misbruke sine tilganger, enten selvinitiert eller under påvirkning av en tredjepart (B3 i Figur 9 og C3 i Figur 10). SEI (Costa, 2017) sin forståelse av innsider omfatter alle personer med tilgang, og innsidetrusselen som potensialet for at innsideren kan utføre handlinger (bevisst eller ubevisst) som fører til negative konsekvenser. Med utgangspunkt i SEI sin omfattende definisjon for innsidere kan det være hensiktsmessig å benytte en grovere inndeling enn roller for å vurdere innsiderisikoen, men for at det skal være formålstjenlig forutsetter dette at grupperingen enten har samme intensjon, kapasitet eller mulighet. En grov inndeling av personer kan føre til større usikkerhet i resultatet, men på den annen side kan en veldig detaljert analyse bli uoversiktlig og uhåndterlig, spesielt i en stor virksomhet med mange roller og stillinger involvert. Hvor detaljert en skal gjennomføre analysen med tanke på gruppering av personer, kan også avhenge av hvor stor virksomheten er, hvilke ressurser (kunnskap, tid) en har til rådighet, samt trusselens alvorlighetsgrad. Det kan være krevende å identifisere alle som har tilgang til de enkelte verdiene, og tilganger går ikke alltid fram av en rolle- eller stillingsbetegnelse. Dette setter krav til at de som deltar i vurderingene er godt kjent med rollene for at oversikten skal bli så komplett som mulig.

I tillegg til å identifisere roller, eller grupper av roller, må det gjennomføres en fornyet vurdering av sannsynligheten eller muligheten for at hendelsen vil inntreffe, basert på den

mer detaljerte kunnskapen. Sannsynlighet kan brytes ned i faktorene intensjon og kapasitet som utgjør trusselen, og i tillegg kommer muligheten som er en kombinasjon av *tilgang* til verdien og *sårbarheten* i barrierene, eller sikkerhetstiltakene, som er iverksatt for å beskytte verdiene. Gjennom analyse av eksisterende sikkerhetstiltak og deres sårbarheter overfor den spesifiserte trusselen kan det komme fram forslag om endringer eller iverksettelse av nye tiltak for å øke sikkerhetsnivået for den aktuelle verdien (se Tabell 5 i vedlegg for eksempel på skjema som kan benyttes). Resultatet blir en oppdatert oversikt over de roller eller grupper av roller som er forbundet med størst innsiderisiko for virksomheten.

Individuelt nivå

Empirien fra CPNI (2013b, s. 18) anbefaler at det *ved behov* gjennomføres egne individuelle risikovurderinger for høyrisikoroller, i tillegg til vurderingene på det organisatorisk nivå og gruppenivå. Høyrisikoroller er de rollene som har størst skadepotensial dersom de innehas av en person som begår innsidehandlinger. En individuell risikovurdering er nyttig for å få dybdekompetanse om alle tilganger og hvilket skadepotensial en høyrisikorolle har. Resultatet kan gi føringer for ekstra sikkerhetstiltak som bør iverksettes, som eksempelvis årlig gjennomgang av sikkerhetsrutiner eller fornyet bakgrunnssjekk hvert annet år for personer som innehar rollen. For øvrig er det viktig å merke seg at det er rollen som vurderes (analyseobjektet), *ikke* personen som innehar den (CPNI, 2013b, s. 18).

I stedet for en ressurskrevende full analyse av alle roller for å etablere risikobildet, som var det første alternativet, gjennomføres denne analysen og vurderingen kun for de roller hvor skadepotensialet vurderes å være størst. Iverksettelse av ekstra sikkerhetstiltak, som kan omfatte tiltak som oppleves som inngripende overfor den enkelte person, kan da begrenses til områder hvor risikoen er størst og tiltakene har mest effekt.

Risikoevaluering

Gjennom analysejobben på nivåene organisasjon, gruppe og individ, kan VTS-modellen fra NS 5832:2014 (Standard Norge, 2014) benyttes i vurderingen for å presentere et bilde på verdiene som er analyseobjektet, truslene som tiltrekkes av dem og verdienes sårbarheter i forhold til truslene (Njå et al., 2020, s. 259). VTS-modellen framstår visuelt enkel med sine tre faktorer og trekantform. På den annen side har denne modellen noen svakheter som

sløyfemodellen (Hellesøy, 2021) er sterkere på da denne ivaretar bedre faktorer som sannsynlighet, barrierer og usikkerhet, se Figur 4. Bruk av sløyfemodellen, eventuelt i kombinasjon med VTS-modellen, for å illustrere risikoen bidrar til et helhetlig og forståelig bilde av risikoen både for de som er involvert i analyse og vurderinger, og for presentasjon. Alle forutsetninger, vurderinger og tilhørende usikkerhet dokumenteres for at det senere skal være mulig å hente opp analyse og vurdering, for å oppdatere den med fornyet kunnskap eller endrede data.

Gjennom analysen er forslag til nye sikkerhetstiltak, eller forbedring av eksisterende tiltak, identifisert. Neste steg er å evaluer risikonivået opp mot sikkerhetsmål for innsiderisiko og å beslutte om restrisikoen kan aksepteres eller om det skal iverksettes implementasjon av nye eller endrede tiltak som er foreslått.

Innsider under påvirkning av tredjepart

I empirien fra CPNI (2013b), både på organisatorisk, gruppe- og individuelt nivå, er det trusselen personen på innsiden utgjør og denne personens handlinger i kombinasjon med handlingenes skadepotensial, som er det sentrale. Dette tilsvarer perspektiv B, se Figur 9.

Perspektiv C tar inn en tredjepart som bruker personen på innsiden som et verktøy for å oppnå egne mål, se Figur 10. Ifølge NOU 2016: 19 (s. 66) er det i de fleste tilfeller menneskelige sårbarheter som utnyttes, som manglende kunnskap, manglende motivasjon til å følge sikkerhetsbestemmelser eller evnen til å la seg friste eller lure gjennom sosial manipulasjon. Innsideren kan for eksempel lures til å gi fra seg passord eller fortelle om sikkerhetsrutiner som åpner veien inn i virksomheten for tredjepart (C1 i Figur 10). Ved bruk av fristelser eller press kan tredjepart få en innsider til å utføre handlinger for seg, i noen tilfeller uten at innsideren forstår konsekvensen av handlingene selv (C2 i Figur 10), men også handlinger hvor innsideren er bevisst både handlingen og de tilsiktede konsekvensene som ved sabotasje og deling av informasjon med noen som ikke er autorisert for informasjonen (C3 i Figur 10). Når innsiderisikoen skal vurderes er det fortsatt innsideren og innsiderens handlinger som utgjør trusselen, men faktoren intensjon, både i forhold til forventning om å lykkes og motivasjon for handlingen, vil være påvirket av at personen handler under innflytelse eller påvirkning av en tredjepart, se Figur 3 (Smith & Brooks, 2013, s. 65). Empirien fra NSM (2021, s. 6) anbefaler at det gjøres en kartlegging av hvilke stillinger eller roller som gjør personer i virksomheten spesielt utsatt for rekruttering eller

annen påvirkning av tredjepart. Dette kan for eksempel være roller som jobber med teknologi som fremmed etterretning er interessert i å få tilgang til eller det kan være roller som medfører mye reisevirksomhet til et land hvor det er kjent at nordmenn på reise kan bli utsatt for rekrutteringsforsøk (PST, 2022, ss. 9-12).

En organisasjons verdier beskyttes av barrierer eller sikkerhetstiltak som kan være fysiske, teknologiske, organisatoriske eller menneskelige. Personen på innsiden kan ses på som en av disse *barrierene* som beskytter verdier gjennom sin kunnskap om trusler, sin årvåkenhet og sin etterlevelse av sikkerhetsregler og -rutiner. Empirien viser at NSM (2019c, s. 7) anbefaler bruk av scenarioer nettopp for å avdekke sårbarheter i menneskelige forhold som påvirkning av personer i roller som har betydning for sikkerhet i virksomheten. En ekstern trusselaktør, tredjepart, som utnytter en person på innsiden «snur virkningen» av den menneskelige barrieren fra å være et sikkerhetstiltak til å bli en åpning for eller en forsterkning av det tredjepart ønsker å oppnå. Dette gjøres for eksempel gjennom phishing-angrep hvor en ansatt klikker på en lenke og det er denne personen som iverksetter nedlasting av ondsinnet programvare. Denne handlingen kan ha vært bevisst fra den som trykker på lenken, i et samarbeid med tredjepart, enten med gode eller onde intensjoner i forhold til konsekvensene, eller det kan være en ubevisst handling.

Med betraktningen om at innsiderisiko kan ses på som *usikkerhet knyttet til om en person som har eller hadde autorisert tilgang til en organisasjons kritiske eiendeler bruker denne tilgangen, enten ondsinnet eller utilsiktet, til å handle på en måte som kan påvirke organisasjonen negativt og hvilke konsekvenser handlingen kan få*, vil det likevel fortsatt være innsideren som er faktoren *trussel* i vurderingen av innsiderisiko. Flere lag sikkerhetstiltak etter prinsippet om forsvar i dybden, gjerne i en kombinasjon av organisatoriske, menneskelige og fysiske barrierer, skal forhindre at en enkelt persons handlinger får store skadefølger (Smith & Brooks, 2013, ss. 107-109). Både de forebyggende og konsekvensreduserende sikkerhetstiltakene, og sårbarheter i dem, vil være en del av risikovurderingen som vist i teorien bak sløyfemodellen (Hellesøy, 2021) og i empirien for risikovurdering på gruppenivå (CPNI, 2013b, s. 17).

Rolle eller person som analyseobjekt

Gjennom funn i CPNI (2013b, s. 18) sin veileder framgår *rollene* som analyseobjektet ved vurdering av innsiderisiko i virksomheten, ikke personene som innehar rollene. Empirien

redegjør for at det er viktig å holde seg nøytral i forhold til hvem som innehar rollen for å styre klar av unøyaktigheter i analysen. Eksempelvis bør det unngås å legge inn antagelser som at de som har en lavere betalt jobb har større sannsynlighet for å begå innsidehandling for personlig gevinst enn de som har bedre betalte stillinger og at de som er leid inn som konsulenter oftere lekker informasjon enn fast ansatte (CPNI, 2013b, s. 15). En kartlegging av høyrisikoroller, som er beskrevet tidligere i oppgaven, gir en oversikt over hvilke roller som har størst skadepotensial for virksomheten (CPNI, 2013b, s. 18).

Empirien fra NSM (2021) setter på sin side fokus på hvordan innsideaktivitet kan forebygges og avdekkes ved å identifisere og følge opp sårbarheter ved *den enkelte person*, fra ansettelse, gjennom ansettelsesforholdet og i avslutningen av ansettelsesforholdet. Disse funnene bekreftes i veilederen Sikkerhet ved ansettelsesforhold (PST et al., 2017) og Grunnprinsippene for personellsikkerhet (NSM, 2021).

CPNI (2013b) og NSM (PST et al., 2017) (NSM, 2021) sine metoder for vurdering av innsiderisiko kan oppfattes som dels motstridende, med fokus på henholdsvis *roller* og *personer som innehar rollene*. Men dette kan også betraktes som komplementære vinklinger.

I vurderingen av innsiderisiko på gruppe- og rollenivå legges det fra CPNI (2013b) vekt på hvilke sikkerhetstiltak, eller barrierer, virksomheten har iverksatt og satt i system for å forebygge innsiderisiko, som for eksempel bakgrunnssjekk før personer ansettes eller går over i ny rolle eller stilling, virksomhetens sikkerhetskultur, endring av tilganger ved endring i tjenstlig behov, med mere. Sikkerhetstiltakene med tilhørende sårbarheter er en del av kunnskapsgrunnlaget som vil påvirke vurdering av sannsynlighet for uønskede hendelser forårsaket av innsidere.

Settes dette i sammenheng med et system for rapportering og oppfølging av sikkerhetsobservasjoner og sikkerhetshendelser samt personene som er involvert i disse, kan både hendelser og den enkelte persons sårbarheter identifiseres og følges opp. En oversikt over hvilke roller som har størst skadepotensial i kombinasjon med en oversikt over de roller som har størst risiko for å bli påvirket av tredjepart, sammen med kunnskap om en enkeltpersons sårbarheter gir et godt grunnlag for å vurdere innsiderisikoen ved å tilordne, eller beholde, personen i en spesifikk rolle. Det muliggjør vurdering av om en enkeltpersons sårbarheter er forenlig med risikoen for uønskede innsidehandlinger, bevisst eller ubevisst, i den rollen personen innehar eller skal tildeles. Eventuelt om risikoen kan reduseres til et akseptabelt nivå ved å tilpasse eksisterende eller innføre ekstra sikkerhetstiltak. For å holde

risikoen på et akseptabelt nivå vil det det være lavere toleranse for en persons sårbarheter i en rolle med stort skadepotensial, enn i en rolle som ikke har mulighet for å påføre skade i samme grad. På den annen side kan rollen ha stor sannsynlighet til å bli påvirket av en tredjepart, som er med på å øke sannsynligheten for at risikoen for en uønsket innsidehendelse materialiseres.

5.2.1 Oppsummering

Innsiderisiko kan defineres som *usikkerhet* knyttet til om en person som har eller hadde autorisert tilgang til en organisasjons kritiske eiendeler bruker denne tilgangen, enten *ondsinnet eller utilsiktet*, til å *handle* på en måte som kan påvirke organisasjonen negativt og hvilke *konsekvenser* handlingen kan få.

I lys av teori for risikovurdering, samt empiriske data fra Storbritannia og Norge, starter vurdering av innsiderisiko med en identifisering, kartlegging og rangering av virksomhetens viktigste verdier. Den potensielle trusselen fra innsidere mot verdiene identifiseres, samt konsekvensene av en uønsket innsidehandling. Innsiderens motivasjon og intensjon kan være påvirket av en ekstern trusselaktør som presser, frister eller manipulerer innsideren, men trusselen ved vurdering av innsiderisiko er *det potensialet som en person på innsiden har til å skade virksomheten, enten bevisst eller ubevisst*, uavhengig av om det er selvinitiert eller under påvirkning av en tredjepart og uavhengig av hva som er intensjonen eller motivasjonen. Når truslene er identifisert, analyseres hvilke roller, eller grupper av roller, som har mulighet for å gjennomføre innsidetruslene som er høyest rangert, og det gjøres en vurdering av eksisterende sikkerhetstiltak og deres sårbarheter. Ut fra dette identifiseres forslag til endringer for å redusere risikoen ytterligere. Høyrisikoroller er de *rollene som har størst skadepotensial for virksomheten om de bekles av en person som begår uønskede innsidehandlinger*. For høyrisikorollene kan det gjennomføres en mer detaljert og grundig kartlegging og vurdering av tilganger og sikkerhetstiltakenes effektivitet, for å komme fram til mer effektive og treffsikre tiltak i forhold til å redusere risikoen for disse rollene til et akseptabelt nivå.

Ved vurdering av innsiderisiko for virksomheten vil den enkelte persons sårbarheter ikke inngå i virksomhetens innsiderisikovurdering da det er rollen, ikke personen som bekler rollen, som er analyseobjektet. Enkeltpersoners sårbarheter identifiseres og følges opp med nødvendige tiltak for å redusere risikoen til et akseptabelt nivå for rollen som skal bekles, og

gjennom dette redusere den faktiske risikoen for uønskede innsidehendelser i virksomheten. I ytterste konsekvens kan tiltaket kan være at personen ikke ansettes, eller får fortsette, i rollen, da sårbarheter og andre risikofaktorer ved personen, sett i opp imot alvorlighetsgraden for innsiderisikoen i rollen, ikke gir et forsvarlig sikkerhetsnivå.

5.3 Sikkerhetsklareringens effekt på vurdering av innsiderisiko

«Formålet med personellsikkerhet er å sikre at personell som skal ha tilgang til verdier har den nødvendige påliteligheten og lojaliteten slik at man kan ha begrunnet tillit til at personen er sikkerhetsmessig skikket» (Prop. 153 L, 2016-2017, s. 114). Personellsikkerhet er tiltak og aktiviteter for å forebygge, avdekke og motvirke handlinger som påfører organisasjonen tap eller skade, og som utføres av en person med tilgang til organisasjonens verdier. Sikkerhetsloven (2018) med forskrifter sammen med veiledende dokumenter fra NSM beskriver flere konkrete personellsikkerhetstiltak for å beskytte verdier som er omfattet av sikkerhetsloven. Tiltakene kan deles inn kategoriene sikkerhetsklarering, autorisasjon og sikkerhetsmessig ledelse og kontroll (NSM, 2019b, s. 5).

Som NSM (2019b, s. 6) tydeliggjør er gyldig sikkerhetsklarering et krav sikkerhetsloven pålegger for personer som skal ha tilgang til sikkerhetsgradert informasjon på nivå KONFIDENSIELT og høyere, og det samme kravet gjelder for personer som enkelt kan skaffe seg denne tilgangen eller som kan få utilsiktet tilgang gjennom sitt arbeid. Personer som skal ha tilgang til informasjonen må i tillegg autoriseres. Sikkerhetsklarering og autorisasjon er det som Aven (2017, s. 16) beskriver som sikkerhetstiltak av type sannsynlighetsreduserende barrierer, eller barrierer som skal forhindre en uønsket hendelse. På samme måte er også sikkerhetsmessig ledelse og kontroll personellsikkerhetstiltak, men i denne kategorien kan tiltakene som NSM (2021, s. 3) være både sannsynlighetsreduserende tiltak som for eksempel bakgrunnssjekk og rekrutteringsprosesser og det kan være skadeforebyggende tiltak som å følge opp medarbeidere under håndtering av en pågående hendelse.

For å svare på oppgavens problemstilling «*Hvordan kan bruk av sikkerhetsklarering påvirke vurderingen av innsiderisiko?*» er det etablert et siste forskningsspørsmål:

3) Hvilken effekt kan sikkerhetsklarering ha på vurdering av innsiderisiko?

Som forklart ovenfor er sikkerhetsklarering ett av flere personellsikkerhetstiltak eller barrierer iverksatt for beskyttelse av sikkerhetsgradert informasjon. Sikkerhetsklarering gjennomføres av en klareringsmyndighet som etter å ha gjennomført personkontroll av en person gjør en helhetlig vurdering og tar en avgjørelse i forhold til om sikkerhetsklarering kan innvilges. Som tallene fra EOS-utvalget (2022) viser var det 652 personer totalt, eller i underkant av 2,4% av de som fikk avgjort sin søknad om klarering i 2021 som fikk negativt svar på søknaden sin. Tallet omfatter både de som ikke ble klarert, de som fikk lavere nivå enn det ble anmodet om og de som fikk klarering med vilkår. Men det som ikke framgår av rapporten er hvilket utvalg av befolkningen som søker om klarering eller hvilken utvelgelsesprosess som finner sted i forkant.

Det er hver av organisasjonene som har behov for sikkerhetsklarert personell som tar beslutningene om hvem det skal søkes sikkerhetsklarering for og som av den grunn får sende inn en søknad til klareringsmyndigheten (NSM, 2011, s. 7).

Før iverksettelse av sikkerhetsklarering

Fordi sikkerhetsklarering er et krav for å få tilgang til sikkerhetsgradert informasjon opplyses det gjerne om i stillingsutlysningen hvor det er aktuelt. Dette kan oppfattes som en barriere som hindrer enkelte å søke stillingen, enten fordi de antar at de ikke vil få en sikkerhetsklarering for eksempel på grunn av straffehistorikk eller et utenlandsk statsborgerskap, eller det oppleves som for inngripende å underlegge seg det regimet med åpenhet som sikkerhetsloven krever gjennom personkontroll, autorisasjonssamtaler og varslingsplikt (2018, ss. §§ 8-9 og 8-11). For andre kan utlysningen ha motsatt effekt da det anses som ekstra attraktivt og spennende å få jobbe med noe som kun et utvalg får tilgang til. Som Njå et al. (2020, s. 258) beskriver det vil en slik annonsering også være en eksponering av både organisasjonen og stillingen som håndterer nasjonale verdier og som derfor kan virke tiltrekkende på en aktør som av egen motivasjon, (se B3 i Figur 9) eller under påvirkning av en tredjepart (se C3 i Figur 10), har som mål å påvirke, skade eller stjele disse verdiene.

PST et al. (2017) tar til orde for at det er viktig å tenke på sikkerhetsaspektet i tillegg til å finne den beste kandidaten i rekrutteringsprosessen og trekker frem blant annet bakgrunnssjekk og intervju som virkemiddel. Organisasjonen bør tilpasse

rekrutteringsprosessens omfang til den enkelte stilling eller rolle, og det kan være forskjellig prosess for eksterne og interne (internt bytte) kandidater. Gjennom prosessen kan det avdekkes faktorer som diskvalifiserer kandidaten som for eksempel manglende faglige kvalifikasjoner og personlige kvaliteter som ikke passer inn i stillingen, men også manglende sikkerhetsmessig dømmekraft eller faktorer som skaper usikkerhet i forhold til risiko for en negativ klareringsavgjørelse, kommer inn i vurderingen. Hvor risikovillig en organisasjon er i en ansettelse kan bero på både kunnskap og forståelse for innsiderisikoen og kunnskap om risikoen ved å søke om sikkerhetsklarering (se Tabell 2), samt at det vil være en helhetsvurdering som omfatter mer enn sikkerhetsaspektet.

Utvalget som søker om sikkerhetsklarering vil være de personene som kommer gjennom den enkelte organisasjons rekrutteringsprosess for en stilling eller rolle som krever sikkerhetsklarering.

Sikkerhetsklarering

Jamfør sikkerhetsloven (2018, ss. § 8-4) er det klareringsmyndigheten som fatter en avgjørelse om sikkerhetsklarering kan innvilges etter gjennomført personkontroll av personen. Vurderingen som gjøres skal vektlegge relevante forhold for en persons pålitelighet, lojalitet og dømmekraft i forhold til behandling av sikkerhetsgradert informasjon og tilgang til skjermingsverdige objekter og infrastruktur. Sikkerhetsloven viser til hvilke opplysninger klareringsmyndigheten kan legge vekt på i sin risikovurdering. Men som poengtert i NOU 2016:19 så påpekte en arbeidsgruppe i forbindelse med forslaget til ny sikkerhetslov problemet med at dagens klareringer må gis på et mer generelt grunnlag for å kunne brukes i flere virksomheter i forhold til om en klarering ble gitt for en bestemt stilling (NOU 2016: 19, 2016, s. 197). Klareringsmyndigheten vil av den grunn muligens ta høyde for en hypotetisk mulighet for at en person kan utløse høy risiko i en framtidig stilling innenfor klareringsperioden. Dette kan føre til en negativ klareringsavgjørelse selv om sannsynligheten for at risikoen utløses er lav (NOU 2016: 19, 2016, s. 197). Eksempel på en slik situasjon kan for eksempel være en person med familiære eller økonomiske bindinger til et land som kan sette personen under press. På den annen side kan klareringsmyndigheten redusere risikoen ved å sette vilkår som avgrenser bruk av klareringen til en bestemt organisasjon eller stilling (NSM, 2019b, s. 17). En avgjørelse om sikkerhetsklarering vil

uansett basere seg på en forventning om at personen vil være å stole på for fremtiden i kombinasjon med risikovillighet (NSM, 2011, s. 3).

Autorisasjon

Sikkerhetsloven (2018) pålegger at personer som skal ha tilgang til sikkerhetsgradert informasjon skal autoriseres og at det skal gjennomføres en autorisasjonssamtale før autorisasjonen gis. Autorisasjonsansvarlig skal vurdere om personen er sikkerhetsmessig skikket til å håndtere sikkerhetsgradert informasjon, som vil si vurdere innsidetrusselen eller risikoen for om personen kan komme til å utføre en handling som kan føre til skade eller tap for virksomheten. Dette kan være en ubevisst handling, en bevisst handling med utilsiktet konsekvens eller en bevisst handling med tilsiktet konsekvens (se kap. 5.1.1 og 5.1.2). Autorisasjonsansvarlig som skal gjennomføre samtalen har tilgang til personens egenopplysninger i søknaden om sikkerhetsklarering (NSM, 2011, s. 7). I tillegg må autorisasjonsansvarlig ha kunnskap om virksomhetens trussel- og risikobilde samt det som er aktuelt for rollen personen skal ha og informasjonen (verdiene) det skal autoriseres for tilgang til. Autorisasjonsansvarlig skal gjennom autorisasjonssamtalen identifisere og vurdere om det er aspekter eller risikofaktorer ved personen som kan påvirke personens sikkerhetsmessige skikkethet, og om dette er forenlig med rollen personen skal ha, vurdert opp mot rollens risikoprofil (NSM, 2011).

Virksomhetens leder er autorisasjonsansvarlig, men myndigheten kan delegeres dersom behovet for autorisasjon er stort (NSM, 2011, s. 13). I en virksomhet av litt størrelse og spredning over flere lokasjoner, som for eksempel forsvaret, vil flere ansatte få delegert autorisasjonsmyndighet. Det foreligger ikke noen lovfestede eller formelle krav til bakgrunn eller kompetanse for å ha autorisasjonsmyndighet, så det er opp til den enkelte virksomhet hvordan autorisasjonsansvarlig gjøres i stand til å utøve sin myndighet. Det foreligger ingen kjente data om den enkelte autorisasjonsansvarliges kunnskap og kompetanse eller kvalitet på utførelse av autorisasjonssamtaler.

For en person med sikkerhetsklarering har klareringsmyndigheten allerede gjennomført en vurdering av personen basert på opplysninger mottatt fra personen selv, fra flere registre og eventuelt gjennom referansesamtaler (NSM, 2019b, ss. 13-14). Sikkerhetsloven (2018) åpner for at autorisasjonsansvarlig kan vurdere en person med sikkerhetsklarering som ikke sikkerhetsmessig skikket til å håndtere sikkerhetsgradert informasjon og beslutte at personen

ikke får autorisasjon eller at autorisasjon som er gitt, trekkes tilbake eller settes ned til et lavere nivå. Samtidig kan klareringsmyndigheten, etter en vurdering av opplysningene som fører til autorisasjonsansvarliges beslutning, overprøve denne beslutningen og opprettholde sikkerhetsklareringen. Virksomheten må da omgjøre sin beslutning om autorisasjon på lavere nivå eller ingen autorisasjon (Virksomhetsikkerhetsforskriften, 2018, s. § 74).

Fordi klareringsmyndigheten er en autoritet kan det være utfordrende å skulle gå imot en beslutning de har fattet. Klareringsmyndigheten har tilgang til et bredt spekter av data som faktagrunnlag for sine vurderinger og det er de som besitter den utøvende fagkompetansen på vurdering av innsiderisiko på myndighetsnivå, samt at det er de som har fullmakt til å utstede sikkerhetsklareringer. I tillegg til at klareringsmyndigheten er ekspertene er det norske samfunn basert på en høy grad av tillit, både til hverandre og til statsmakten. Av dette følger naturlig en høy grad av tillit til klareringsmyndigheten, og til deres beslutninger, samtidig som bruk av utøvende myndigheters ressurser for å øke sikkerheten er tillitsskapende (Engen, et al., 2016, s. 49). For en autorisasjonsansvarlig, ofte med betydelig lavere fagkompetanse og uten tilgang til de data klareringsmyndigheten har, vil klareringsmyndighetens beslutning kunne veie tungt i en vurdering.

Samtidig kan det bli en for enkel løsning å støtte seg til klareringsmyndighetens beslutning, og at en person har en sikkerhetsklarering. I Norge følger sikkerhetsklareringen personen på tvers av stillinger, roller og virksomheter. Trussel- og risikobildet varierer, spesielt fra virksomhet til virksomhet, og autorisasjonen må ta høyde for dette. En klarering gis for å kunne brukes i flere virksomheter (NOU 2016: 19, 2016, s. 197), men det er autorisasjonsansvarlig som avgjør om personen kan få tilgang til de verdiene den enkelte virksomhet forvalter.

En annen problemstilling kan være personer som har en klareringssøknad til behandling hos klareringsmyndigheten, men hvor avgjørelse ikke er fattet på det tidspunkt som personen har behov for sin autorisasjon. Ifølge EOS-utvalget (2022) er gjennomsnittlig behandlingstid på tvers av klareringsmyndighet og avgjørelse (negativ eller positiv) 44 dager. I disse tallene er det et spenn fra gjennomsnittlig saksbehandlingstid på 38 dager for positive avgjørelser behandlet av FSA til gjennomsnittlig 277 dager for negative avgjørelser behandlet av NSM. For tilgang til gradert informasjon på nivå KONFIDENSIELT er det et absolutt krav til sikkerhetsklarering så på det nivået er det ingen problemstilling. Men for autorisasjon til lavere graderingsnivå og vurdering av personen generelt, kan lang saksbehandlingstid øke

autorisasjonsansvarliges usikkerhet i forhold til om personen vil få sikkerhetsklarering og vurderes skikket for tilgang til sikkerhetsgradert informasjon av klareringsmyndigheten. Dette forsterkes av tallene som indikerer at det er søknader med negativt utfall som krever lengst behandlingstid (EOS-utvalget, 2022).

Autorisasjonsansvarlig er ansatt i virksomheten som har behovet for at personen kan jobbe med gradert informasjon, og dette behovet kan bidra til å økt risikoaksept på bekostning av sikkerhet. Ved at avgjørelsen om klarering tas av en utenforstående klareringsmyndighet, vil det være større sannsynlighet for at de opptrer nøytralt og ikke lar seg påvirke til å sette behovet ressursen foran nødvendigheten å sikre at «klareringssaken er så godt opplyst som mulig» (Sikkerhetsloven, 2018, ss. § 8-4).

Aven (2015) trekker fram kunnskapsgrunnlaget og styrken på kunnskapen som faktorer som påvirker usikkerheten i risikovurderingen. I saker hvor autorisasjonsansvarlig skal autorisere til laveste nivå (BEGRENSET), og det ikke foreligger en klarering, er vurderingen i større grad avhengig av autorisasjonsansvarliges kunnskap og forståelse for fenomenet innsiderisiko og -trusler, og hvilke datagrunnlag og informasjon som er tilgjengelig, enn i saker hvor det foreligger en sikkerhetsklarering. Klareringsmyndigheten gjennomfører en grundig bakgrunnssjekk for de som gjennomgår en klareringsprosess. For de som ikke har en sikkerhetsklarering vil det kun være virksomhetens egen prosess og tiltak som gir underlag for vurderingen. På den annen side kan også klareringsmyndighetens ekspertise tillegges for stor vekt i vurderingen av innsiderisiko for en sikkerhetsklarert person, avhengig av autorisasjonsansvarliges kunnskap og forståelse for fenomenet innsiderisiko.

Sikkerhetsmessig ledelse og kontroll

Ledelse og kontroll er ifølge NSM (NSM, 2019b, s. 5) den tredje kategorien under personellsikkerhetstiltak, og sikkerhetsloven (2018) pålegger eksplisitt personer som er sikkerhetsklarert og autorisert en varslingsplikt om forhold som kan ha betydning for sikkerhetsmessig skikkethet (§ 8-11). Personen som er autorisert kan også be om en autorisasjonssamtale ved behov og på samme måte kan autorisasjonsansvarlig gjennomføre en autorisasjonssamtale når vedkommende finner grunn til det (Virksomhetsikkerhetsforskriften, 2018, s. § 68). Sett i forhold til sikkerhetsklareringens påvirkning på vurdering av innsiderisiko er dette en direkte effekt, hvor både den enkelte

person og autorisasjonsansvarlig pålegges varsling og oppfølging av potensielle risikofaktorer og sårbarheter.

For personer som har gode intensjoner, et ønske om å beholde jobben og en avhengighet til sikkerhetsklarering for å beholde den, vil varslingsplikten fungere som en mulighet til å ta opp saker som personen selv opplever som relevant i forhold til sin sikkerhetsmessige skikkethet. Et godt tillitsforhold legger til rette for at personer som kan komme i, eller som befinner seg i, en presset eller ubehagelig situasjon, kan ta opp dette med autorisasjonsansvarlig og redusere risikoen ved å være åpen og eventuelt få hjelp til å håndtere situasjonen for å redusere ytterligere skade eller tap. Dette gjelder også i tilfeller hvor personer har utført en handling, og først i ettertid forstår konsekvensene av handlingen (se B2 i Figur 9). Om det er en god kultur for å ta opp saken øker det sannsynligheten for at skaden kan reduseres. I tillegg forventes det at den autoriserte informerer om forhold som er endringer av opplysninger sendt til klareringsmyndigheten ved søknad om klarering (NSM, 2011, s. 15). Autorisasjonsansvarlig er samtidig pålagt å realitetsbehandle opplysningene ved å vurdere om opplysningene fører til økt risiko, eller om det bør iverksettes noen ekstra tiltak (NSM, 2011, s. 12).

For en person som kommer inn i en rolle med et bevisst ønske om å utnytte de tilgangene rollen gir, har ikke varslingsplikten like stor effekt, da det ikke vil være åpenhet som har fokus. Men i en virksomhet med en kultur for å si ifra og følge opp, kan det være andre som reagerer på unormal adferd og uregelmessigheter, og som kan benytte tillitsforholdet til sin autorisasjonsansvarlig for å ta opp saken. Når motivasjonsfaktorer til å begå uønskede handlinger blant annet kan skyldes misnøye med arbeidsgiver, personlige eller arbeidsrelaterte problemer og hevn, kan det være mulig å fange opp slike endringer gjennom årvåkenhet (PSTet al., 2017, s. 5). På den annen side må det unngås at enhver endring ved en person leder til at personen mistenkes for å planlegge eller utøve uønskede handlinger og at vedkommende behandles som en trusselaktør.

Gjennom det som er diskutert går det fram at «autorisasjon er en prosess som følger en sikkerhetsklarert person i hele den perioden vedkommende har tilgang til sikkerhetsgradert informasjon og blir således [også] en del av begrepet sikkerhetsmessig ledelse og kontroll» (NSM, 2011, s. 3). Det går tydelig fram at autorisasjonsansvarlig har en viktig rolle i forhold til vurdering av innsiderisikoen når det gjelder oppfølging av den enkelte person.

Forsvar i dybden

Smith og Brooks (Smith & Brooks, 2013, ss. 107-109) beskriver prinsippet forsvar i dybden som benyttes for beskyttelse av verdier. Beskyttelsen består ofte av en kombinasjon av både fysiske, menneskelige og organisatoriske barrierer. Sikkerhetstiltakene sikkerhetsklarering, autorisasjon og sikkerhetsmessig ledelse og kontroll som pålegges gjennom sikkerhetsloven (2018) for å beskytte sikkerhetsgradert informasjon, er ett eksempel på bruk av flere barrierer.

Erfaring har vist at flere barrierer har bedre effekt enn en enkelt, sterk barriere, men James Reason (1997) hevder at bruk av flere barrierer kan føre til det han omtaler som en sveitserost-effekt, hvor sårbarheter i de forskjellige barrierene under uheldige omstendigheter kan opptre samtidig, og en uønsket hendelse utløses (se Figur 6). Et eksempel på dette kan være en person som har et forhold til en statsborger fra et land med aktiv statlig etterretningstjeneste. Personen unnlater bevisst å opplyse om forholdet i sin søknad om sikkerhetsklarering, klareringsmyndigheten innvilger sikkerhetsklarering og første barriere passeres. Autorisasjonsansvarlig forholder seg til beslutningen fra klareringsmyndigheten og stiller ikke mange spørsmål under autorisasjonssamtalen. Det kan også være bevisst tilbakeholdelse av opplysninger fra personen under denne samtalen. Den aktuelle trusselen mot virksomheten, i form av fremmed etterretning som påvirker egne borgere og nærstående til spionasje for å få tak i sikkerhetsgradert teknisk informasjon, tas ikke opp som tema under samtalen da det ikke framgår at personen som autoriseres verken har statsborgerskap fra et annet land eller noen nære forbindelser. Personen autoriseres for tilgang til sikkerhetsgradert informasjon, og andre barriere er passert. Kollega som er bosatt i personens nabolag har registrert det nære forholdet til den utenlandske forbindelsen, men tar det ikke opp med arbeidsgiver da det antas å være sjekket ut siden personen har fått både sikkerhetsklarering og autorisasjon, og kollegaen har heller ikke fått noen informasjon om at dette er en svært aktuell trussel mot virksomheten og fagområdet som denne personen jobber med. I verste tilfelle befinner den aktuelle personen seg under press, eller har latt seg friste, og deler derfor gradert informasjon med en fremmed stat.

Sett fra den fremmede etterretningstjenesten, eller tredjepart, sitt ståsted så er forholdet til statsborgeren fra dette landet en sårbarhet som eksponerer personen som har tilgang til den sikkerhetsgraderte informasjonen, verdiene, som tredjepart er interessert i (Smith & Brooks, 2013, ss. 67-68).

I dette eksemplet hadde både autorisasjonsansvarlig og kollega stor tillit til klareringsmyndigheten og deres beslutning, i kombinasjon med manglende kunnskap om virksomhetens trusselbilde og innsiderisikoen. Autorisasjonsansvarlig var kanskje heller ikke godt nok opplært, hadde for lite kunnskap, liten erfaring eller forstod kanskje ikke viktigheten av autorisasjonsrollen. Til tross for tiltak i form av flere separate barrierer svekkes tiltakenes effekt når det meste av tillit legges til første barriere, sikkerhetsklareringen. Dette er et eksempel som bekrefter Reason (1997) sin sveitserost-teori.

Innsiderisikovurdering

Som vist i kap. 5.2 kan det ved å følge CPNI (2013b) sin metode for innsiderisikovurdering gjennomføres vurderinger på flere nivåer, betegnet som *organisasjonsnivå*, *gruppenivå* og *individnivå*. Felles for alle nivåene er at det er rollen som er analyseobjektet i vurderingene, ikke den enkelte person som bekler rollen.

For å vurdere effekten av sikkerhetsklarering i forhold til roller, vil det være virksomhetens *system* for gjennomføring og oppfølging av sikkerhetsklarering, autorisasjon, sikkerhetsmessig ledelse og kontroll som vil påvirke vurderingen. Dette er en del av risikostyringen i virksomheten, og som Aven (2015) påpeker, så er alle tiltak og aktiviteter som gjøres for å styre risiko en del av risikostyringen i en virksomhet (Aven, 2015, s. 13).

Hvor gode rutiner virksomheten har for å gjennomføre sikkerhetstiltak som for eksempel sikkerhetsklarering, autorisasjon og sikkerhetsmessig ledelse og kontroll, vil være grunnlaget for vurdering av den potensielle innsidetrusselen og innsiderisikoen. Systemer for oppfølging, overvåking og kontroll (se Figur 1) vil framskaffe data i forhold til om rutiner følges og også status for eksempel i forhold til om og når autorisasjonssamtaler gjennomføres i praksis. Dataene øker styrken på kunnskapsgrunnlaget om den reelle statusen i virksomheten, i motsetning til å vite at det eksisterer rutiner, men ikke noe i forhold til om de følges.

For å vurdere effekten av sikkerhetsklarering kan det skilles mellom verdier som krever sikkerhetsklarering for å få tilgang til verdien og verdier som ikke har krav til sikkerhetsklarering. For verdier som personer både med og uten sikkerhetsklarering har tilgang til, vil kunnskap om andelen sikkerhetsklarerte som har tilgang, sammen med kunnskap om hvor stor andel som følges opp gjennom en systematisk autorisasjonsprosess for autorisasjon og varslingsplikt, være et viktig kunnskapsbidrag til vurdering av trusselen.

For verdier som krever sikkerhetsklarering for tilgang vil det være oppfølgingen med autorisasjon og sikkerhetsmessig ledelse og kontroll som sikkerhetsklarering pålegger som påvirker risikoen.

5.3.1 Oppsummering

Sikkerhetsklarering er et sikkerhetstiltak rettet mot den enkelte person, hvor en klareringsmyndighet gjennomfører en omfattende screening av de som søkes sikkerhetsklarert grunnet tjenstlig behov. I virksomheten som har behovet for sikkerhetsklarert personell følges i tillegg klareringen opp med autorisasjon og sikkerhetsmessig ledelse og kontroll gjennom hele klareringens varighet.

Ifølge anbefalt metode fra CPNI (2013b) er det rollen som er analyseobjektet i vurderingen, *ikke* hvilke personer som innehar eller bekler rollene når en skal komme fram til et risikobilde for innsiderisikoen i en virksomhet. Sikkerhetsklareringens effekt på *vurdering av innsiderisiko* vil derfor være avhengig av kunnskap om rollene som har tilgang til verdiene som er gjenstand for vurdering har en sikkerhetsklarering eller ikke, hvor stor andel som har det, samt hvordan dette følges opp i virksomheten med autorisasjon og sikkerhetsmessig ledelse og kontroll. Kjennskap til rutiner og systemer for oppfølging sammen med data fra måling og kontroll vil bidra til å styrke kunnskapen om reell status i virksomheten. Dersom dataene er differensiert på roller vil det styrke kunnskapsgrunnlaget for vurdering både på organisasjons-, gruppe- og individnivå.

I forhold til risikovurdering av den enkelte person, og rollen personen skal bekle, vil en sikkerhetsklarering sammen med gode rutiner for autorisasjon, ledelse og kontroll til sammen utgjøre et sterkt verktøy for både å forebygge og begrense uønsket innsideaktivitet. På den annen side kan sikkerhetsklarering gjennomført av klareringsmyndigheten bli et påskudd for virksomheten til å utelate ytterligere tiltak. Det kan skyldes at det ikke er etablert gode nok systemer for oppfølging. Det kan også være lav grad av kunnskap og forståelse for innsidetrusselen som hver enkelt person som har tilgang til verdier representerer, samt lite kunnskap om trussel- og risikobildet for virksomheten og de enkelte rollene.

6 KONKLUSJON

Formålet med denne oppgaven har vært å øke kunnskapen om tiltaket sikkerhetsklarering som et virkemiddel for å redusere innsiderisiko. Dette er undersøkt gjennom problemstillingen «*hvordan kan bruk av sikkerhetsklarering påvirke vurderingen av innsiderisiko?*».

Oppgaven har belyst innsideren og den potensielle trusselen innsideren representerer gjennom sin tilgang til verdier. Litteraturstudiene avdekket forskjellige perspektiver og tilnærminger til begrepet innsider, på tvers av flere land. Det ble funnet enkelte fellestrekk og ut fra det kan det konkluderes med at disse fellestrekkene er *enhver person som har eller har hatt tilgang til en organisasjons verdier*, eksempelvis en nåværende eller tidligere ansatt, innleid eller en partner. Med tilgang til en verdi følger et potensial for skade eller tap av denne verdien, og av den grunn utgjør personen en trussel mot verdien, en innsidetrussel. Trusselen materialiseres gjennom en handling og innsidere kan deles inn i følgende kategorier: de som utfører en ubevisst handling, de som utfører en bevisst handling med en utilsiktet konsekvens og de som utfører en bevisst handling med tilsiktet konsekvens. Innsideren kan være selvmotivert eller påvirket av en tredjepart, men det er uansett innsiderens potensial for å påføre verdien skade eller tap som utgjør innsidetrusselen (Costa, 2017).

Gjennom studien er det i empirien funnet metode for vurdering av innsiderisiko (CPNI, 2013b) (CPNI, 2022b). Som forutsetning for risikovurderingen må det gjennomføres en identifisering, kartlegging og rangering av virksomhetens viktigste verdier. Innsiderisikoen i virksomheten vurderes ved å identifisere, analysere og rangere innsidetruslene mot de mest kritiske verdiene, samt konsekvensene dersom truslene materialiseres. Deretter gjennomføres en kartlegging av hvilke roller, eller grupper av roller, som har mulighet for å gjennomføre de høyest rangerte innsidetruslene. I tillegg må det gjennomføres en analyse av sikkerhetstiltakenes godhet i forhold til trusselen. Analysen kan avdekke behov for nye tiltak eller forbedring av eksisterende. Empirien anbefaler en detaljert og grundig gjennomgang av høyrisikorollene, de rollene som har størst skadepotensiale for virksomheten, for å identifisere mer effektive og treffsikre tiltak i forhold til å redusere risikoen for disse rollene. Konklusjonen som kan trekkes er at det er rollen som er analyseobjektet i vurderingen av innsiderisiko i virksomheten, ikke personen som bekler den. Det er virksomhetens system for gjennomføring og oppfølging av sikkerhetstiltak og sikkerhetsstyringen som gir kunnskapsgrunnlaget til risikovurderingen, og ikke tiltakene iverksatt for den enkelte person.

Sikkerhetsgradert informasjon på nivå KONFIDENSIELT og høyere, har et høyt skadepotensial, og sikkerhetsklarering gjennomført av en klareringsmyndighet benyttes derfor som tiltak for å beskytte disse verdiene. Den sikkerhetsklarerte skal i tillegg følges opp med autorisasjon og sikkerhetsmessig ledelse og kontroll i virksomheten som gir tilgang til verdiene.

Drøfting av fordeler og ulemper med dagens system for sikkerhetsklarering bidrar til å øke kunnskapen om tiltaket sikkerhetsklarering som et virkemiddel for å redusere innsiderisiko. Det er ikke alle som får en sikkerhetsklarering. og utvalget som søker om det vil være de som kommer gjennom en virksomhets rekrutteringsprosess. Sikkerhetsklarering kan medføre at virksomheten legger så stor grad av tillit til sikkerhetsklareringen at andre tiltak som autorisasjon og sikkerhetsmessig ledelse og kontroll mister noe av sin effekt. Det kan også føre til at andre tiltak verken vurderes eller iverksettes.

Det er virksomheten som kjenner sine trusler og som møter personen med sikkerhetsklarering i det daglige, og selv med sikkerhetsklarering er det fortsatt nødvendig at virksomheten gjør sine tiltak for å redusere innsiderisikoen. Denne konklusjonen stemmer overens med det Ringstad (2020), på et litt mer overordnet nivå, kom fram til i sin masteroppgave, at forebyggende sikkerhet må ses på som et delt ansvar mellom myndighetene og den enkelte virksomhet.

Å utvide bruk av sikkerhetsklarering til andre områder enn de som dekkes av dagens sikkerhetslov bør vurderes opp imot andre tiltak som å forsterke bakgrunnssjekk og innføre en variant av autorisasjonssamtaler for andre verdier i samfunnet enn de som omfattes av sikkerhetsloven i dag. Sikkerhetsklarering er et inngripende tiltak overfor det enkelte individ og ikke alle kan få en sikkerhetsklarering. Å ta i bruk dette virkemiddelet på flere og andre områder enn det som er dagens praksis, kan føre til at enkelte stenges ute fra et område de er sikkerhetsmessig skikket for. Dette skyldes at sikkerhetsklareringen må ta høyde for risikoen forbundet med flere forskjellige områder fordi den følger personen på tvers av stilling og virksomheter.

6.1 Forslag til videre forskning

Gjennom arbeidet med oppgaven har det kommet fram mange nye spørsmål og problemstillinger som kunne vært utforsket nærmere for å få bredere kunnskap, men som faller utenfor rammene av denne oppgaven.

Et tema for ny forskningsoppgave kan være:

> *Hvordan redusere innsiderisiko i virksomheter som ikke benytter seg av sikkerhetsklarering som virkemiddel?*

7 REFERANSER

Australian Government. (2010). *The Insider Threat to Business. A personnel security handbook.* Hentet fra https://www.organisationalresilience.gov.au/Documents/the-insider-threat-to-business.pdf

Australian Government. (2014). *Managing the Insider Threat To Your Business. A personnel security handbook.* Hentet fra https://www.tisn.gov.au/Documents/InsiderThreatBooklet-ManagingTheInsiderThreatToYourBusiness.pdf

Aven, T. (2015). *Risikostyring* (2. utg.). Universitetsforlaget.

Aven, T. (2017). *Risikoanalyse* (2. utg.). Universitetsforlaget.

Bakke, A. (2017). Individets rettsstilling ved sikkerhetstjenestens personkontrollundersøkelser. *Lov og Rett, 56*(10), ss. 571-589. doi:https://doi.org/10.18261/issn.1504-3061-2017-10-02

Bakke, A. (2019). Refleksjoner over sikkerhetsklarering. *Lov og Rett, 58*(2), ss. 82-93. doi:https://doi.org/10.18261/issn.1504-3061-2019-02-03

Benjaminsen, T. (2017). *The Norwegian Downsizing Approach in Terms of the Insider Threat - An interpretive study.* Hentet fra [Masteroppgave, Norges teknisk-vitenskapelige universitet]. NTNU Open: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2448947

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

Busmundrud, O., Maal, M., Kiran, J. H., & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger (FFI-rapport 2015/00923).* Forsvarets forskningsinstitutt. Hentet fra https://www.ffi.no/publikasjoner/arkiv/tilnaerminger-til-risikovurderinger-for-tilsiktede-uonskede-handlinger

Carnegie Mellon University. (2013). *Unintentional Insider Threats: A Foundational Study.* Carnegie Mellon University. doi:https://doi.org/10.1184/R1/6585575.v1

Costa, D. (2017). *CERT Definition of "Insider Threat" - Updated*. Hentet 2. Oktober, 2022 fra SEI: https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/

CPNI. (2013a). *CPNI Insider Data Collection Study. Report of Main Findings.* CPNI. Hentet 14. juni, 2022 fra https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf

CPNI. (2013b). *Personnel Security Risk Assessment. A Guide.* Hentet 2. august, 2022 fra CPNI: https://www.cpni.gov.uk/resources/personnel-security-risk-assessment-guide-4th-edition

CPNI. (2021). *Insider Risk.* Hentet 2. oktober, 2022 fra CPNI: https://www.cpni.gov.uk/insider-risk

CPNI. (2022a). *Illustrative Role-based Risk Assessment case study in a Small Medium Enterprise.* CPNI. Hentet 23. juli, 2022 fra https://www.cpni.gov.uk/resources/illustrative-role-based-risk-assessment-case-study

CPNI. (2022b). *Role-based Protective Security Risk Assessment Guidance.* Hentet 27. juli, 2022 fra CPNI: https://www.cpni.gov.uk/system/files/documents/7b/80/final-role-based-protective-security-risk-assessment-211.pdf

CPNI. (u.å.). *Protective Security Risk Management.* Hentet 31. juli, 2022 fra CPNI: https://www.cpni.gov.uk/sites/default/files/Protective_Security%20_Risk_Management_v1.2.pdf

DNV GL. (2019). *Håndtering av innsiderisiko.* Petroleumstilsynet. Hentet fra https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/prosjektrapporter-2019/hvordan-handtere-innsiderisiko/

Downey, L. (2022, 30. juni). *Speculative Risk.* Hentet fra Investopedia: https://www.investopedia.com/terms/s/speculativerisk.asp

DSB. (2019). *Risikoanalyse på samfunnsnivå - Metode og prosess ved utarbeidelsen av "Analyser av krisescenarioer (AKS)".* Hentet fra https://www.dsb.no/rapporter-og-evalueringer/risikoanalyse-pa-samfunnsniva---metode-og-prosess-ved-utarbeidelsen-av-analyser-av-krisescenarioer-aks/

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

EOS-utvalget. (2022). *Årsmelding 2021 (DOKUMENT 7:1 (2021-2022)).* EOS-utvalget. Hentet fra https://eos-utvalget.no/hjem/publikasjoner/arsmeldinger/

Etterretningstjenesten. (2022). *FOKUS 2022. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* Forsvaret. Hentet fra https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus

Forskrift om personellsikkerhet. (2001). Forskrift om personellsikkerhet. *(FOR-2001-06-29-722).* Lovdata. Hentet fra https://lovdata.no/dokument/SFO/forskrift/2001-06-29-722

Graver, H. P. (2021). Sikkerhetsklarering og rettssikkerhet. *Lov og Rett, 60*(7), ss. 393-412. doi:https://doi.org/10.18261/issn.1504-3061-2021-07-03

Hellesøy, B. T. (2021, 4. mai). *Tillegg A - Bruk av sløyfemodellen i risikovurderinger.* Standard Norge. Hentet fra https://www.standard.no/Global/PDF/Standard%20Morgen/2021Risiko/Sl%c3%b8yfemodellen%20%e2%80%93%20Helles%c3%b8y.pdf

Insider. (2020). I *Store norske leksikon.* Hentet 11. juni, 2022 fra snl.no: https://snl.no/insider

Jacobsen, J. D. (2021). *Hvordan holde innsidere på utsiden?* Hentet fra [Masteroppgave, Universitetet i Stavanger]. UiS Brage: https://hdl.handle.net/11250/2786366

Jore, S. H. (2019). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research 4*, 157-174. doi:https://doi.org/10.1007/s41125-017-0021-9

Kagan, J. (2021, 10. mai). *Pure Risk.* Hentet fra Investopedia: https://www.investopedia.com/terms/p/purerisk.asp

Klareringsforskriften. (2018). Forskrift om sikkerhetsklarering og annen klarering. *(FOR-2018-12-20-2054).* Lovdata. Hentet fra https://lovdata.no/forskrift/2018-12-20-2054

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.-M. (2015). *Insider Threat Detection Study.* NATO Cooperative Cyber Defence Centre of Excellence. Hentet fra https://ccdcoe.org/library/publications/insider-threat-detection-study/

Meld. St. 5 (2020-2021). (u.d.). *Samfunnssikkerhet i en usikker verden.* Justis- og beredskapsdepartementet. Hentet fra https://www.regjeringen.no/no/dokumenter/meld.-st.-5-20202021/id2770928/

Midtgaard, A. K. (2021, 4. mai). *NS5814 Risikovurderinger – Presentasjon av revidert utgave av NS 5814.* Standard Norge. Hentet fra

https://www.standard.no/Global/PDF/Standard%20Morgen/2021Risiko/Presentasjon%20av%20revidert%20NS%205814%20SN%20Midtgaard.pdf

Njå, O., Sommer, M., Rake, E. L., & Braut, G. S. (2020). *Samfunnssikkerhet. Analyse, styring og evaluering.* Universitetsforlaget.

NOU 2000:24. (2000). *Et sårbart samfunn.* Oslo: Justis- og politidepartementet. Hentet fra https://www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/

NOU 2006: 6. (2006). *Når sikkerheten er viktigst.* Oslo: Justis- og politidepartementet. Hentet fra https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/

NOU 2016: 19. (2016). *Samhandling for sikkerhet.* Forsvarsdepartementet. Hentet fra https://www.regjeringen.no/no/dokumenter/nou-2016-19/

NSM. (2011). *Håndbok i autorisasjon og autorisasjonssamtale.* Hentet fra https://nsm.no/getfile.php/134051-1594383721/Filer/Dokumenter/Veiledere/2011---handbok-i-autorisasjon-og-autorisasjonssamtale.pdf

NSM. (2019a, 12. mars). *Slik blir du sikkerhetsklarert*. Hentet 3. oktober, 2022 fra https://nsm.no/fagomrader/personellsikkerhet/sikkerhetsklarering/slik-blir-du-sikkerhetsklarert/

NSM. (2019b). *Veileder i personellsikkerhet.* Hentet fra https://nsm.no/getfile.php/132407-1590749199/NSM/Filer/Dokumenter/Veiledere/Veileder%20i%20personellsikkerhet.pdf

NSM. (2019c). *Veileder i sikkerhetsstyring.* Hentet fra https://nsm.no/getfile.php/132933-1591350417/NSM/Filer/Dokumenter/Veiledere/veileder-i-sikkerhetsstyring.pdf

NSM. (2019d). *Temarapport. Innsiderisiko.* Hentet fra https://nsm.no/getfile.php/133153-1591706148/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf

NSM. (2021). *Grunnprinsipper for personellsikkerhet.* Hentet fra https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/introduksjon/

NSM. (2022a). Sikkerhetskonferansen 2022 [Video]. NSM. Hentet fra https://ctnor.live/sikkerhetskonferansen-2022/

NSM. (2022b, 7. April). *Alt man ikke ser - samtale mellom tjenestesjefene NSM, PST og E-tjenesten*. ([Video]) Hentet fra YouTube: https://youtu.be/FX48YCzQBgI

NSM. (2022c, 7. April). *Dilemmaet mellom akademisk frihet og sikkerhet i akademia*. ([Video]) Hentet fra YouTube: https://youtu.be/XzSypdmEQxA

NSM. (2022d). *RISIKO 2022. Økt risiko krever økt årvåkenhet.* Oslo. Hentet fra https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

NSM. (u.å.). *NSM*. Hentet 17 september, 2022 fra nsm.no: https://nsm.no/

NSM, Politidirektoratet, & Politiets sikkerhetstjeneste. (2015). *Terrorsikring. En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger.* Hentet fra https://www.pst.no/globalassets/artikler/utgivelser/veileder-i-terrorsikring.pdf

Nyblom, E. (2021, 7. Januar). *Kronikk: Er utenlandske etterretningstjenester amatører?* Hentet fra NSM: https://nsm.no/hold-deg-oppdatert/meninger/kronikk-er-utenlandske-etterretningstjenester-amatorer

Prop. 153 L. (2016-2017). *Lov om nasjonal sikkerhet (sikkerhetsloven).* Forsvarsdepartementet. Hentet fra https://www.regjeringen.no/no/dokumenter/prop.-153-l-2016-2017/id2556988/

PST. (2022). *Nasjonal trusselvurdering 2022.* Hentet fra https://www.pst.no/globalassets/ntv/2022/nasjonal-trusselvurdering-2022-pa-norsk.pdf

PST, Nasjonal sikkerhetsmyndighet, Politiet, & Næringslivets sikkerhetsråd. (2017). *Sikkerhet ved ansettelsesforhold - før, under og ved avvikling.* Hentet fra https://www.pst.no/globalassets/artikler/utgivelser/sikkerhet_ved_ansettelsesforhold_2017_utskrift.pdf

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

Ringstad, P. (2020). *Sikkerhetsstyringens utvikling.* Hentet fra [Masteroppgave, Universitetet i Stavanger]. UiS Brage: https://hdl.handle.net/11250/2712036

Sarpebakken, B., & Steine, F. (2022, 5. April). *Rekordmange utenlandske statsborgere blant de nye doktorene i 2021*. Hentet fra Statistisk sentralbyrå: https://www.ssb.no/teknologi-og-innovasjon/forskning-og-innovasjon-i-

naeringslivet/statistikk/forskerpersonale/artikler/rekordmange-utenlandske-statsborgere-blant-de-nye-doktorene-i-2021

Sikkerhetsloven. (2018). Lov om nasjonal sikkerhet. *(LOV-2018-06-01-24)*. Lovdata. Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-01-24

Smith, C. L., & Brooks, D. J. (2013). *Security Science. The Theory and practice of security.* Elsevier.

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

Standard Norge. (2018). *NS-ISO 31000:2018. Risikostyring - Retningslinjer.*

Standard Norge. (2021). *NS 5814:2021. Krav til risikovurderinger.*

Syvertsen, J. P. (2007). *Insider Threat.* Hentet fra [Masteroppgave, Norges teknisk-vitenskapelige universitet]. NTNU Open: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/143847

U.S. DoD. (2021). *CMMC Glossary and Acronyms.* Hentet fra https://www.acq.osd.mil/cmmc/docs/Glossary_MasterV2.0_FINAL_202111217_508.pdf

U.S. DoD. (2022). *Cybersecurity Maturity Model Certification*. Hentet 15 oktober, 2022 fra Acquisition & Sustainment Office of the Under Secretary of Defence: https://www.acq.osd.mil/cmmc/index.html

U.S. Government. (u.å.). *Defining Insider Threats*. Hentet 27. juli, 2022 fra Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/defining-insider-threats

Virksomhetsikkerhetsforskriften. (2018). Forskrift om virksomheters arbeid med forebyggende sikkerhet. *(FOR-2018-12-20-2053)*. Lovdata. Hentet fra https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053

VEDLEGG A – Tabeller for vurdering av innsiderisiko

Tabeller som benyttes ved vurdering av innsiderisiko.

Tabell 3 Risikovurdering på organisasjonsnivå (CPNI, 2013b, s. 19)

Innsidetrussel (nummer og beskrivelse)	Sannsynlighet (1-5)	Antagelser (sannsynlighet)	Konsekvens (1-5)	Antagelser (konsekvens)
1				
2				

Tabell 4 Risikovurdering gruppenivå - roller (CPNI, 2013b, s. 19)

Innsidetrussel (nummer)	Risikoprioritet	Grupper (roller) med høy grad av mulighet	Begrunnelse
1			
2			

Tabell 5 Risikovurdering gruppenivå - sikkerhetstiltak (CPNI, 2013b, s. 19)

Innsidetrussel (nummer)	Gruppe (roller)	Sikkerhetstiltak			Ansvarlig	Frist
		Eksisterende	Tilstrekkelig? Hvis nei, begrunn	Nye eller forbedrede tiltak		
1						
2						