MASTEROPPGAVE

Emnekode:	Navn / kandidatnummer:
BE323E Masteroppgave	Tone Gunnes - 42

Digital sikkerhetskultur i samfunnskritiske funksjoner – en studie av hva som kjennetegner digital sikkerhetskultur innen finans-, kraft- og justissektoren

Dato: 25.05.2021 Totalt antall sider: 153

NORD universitet

www.nord.no

Abstract

The digitalization of our society is ever-increasing, and so are the vulnerabilities and threats related to it. Social engineering has become a very successful way for criminals to breach organizations' technological systems and get access to sensitive information. Multiple organizations defined as critical societal functions in Norway has fallen victim to these kinds of cyber incidents the last couple of years. Because of their importance and the crucial role they play for society and well-being of citizens, they are a valuable target for criminals. Because of this, I wanted to focus on the human factor in cyber security, and the conditions that influences the process of making users aware of cyber risks and how to act to avoid cyber incidents. Thus, I came up with the following thesis question: *What factors characterizes the cyber security culture within organizations defined as critical societal functions, seen from the view of security experts inside these organizations?*

The concept of cyber security culture is relatively new, and therefore the literature review is focused on more traditional theoretical perspectives regarding organizational accidents, high reliability organizations and security culture, accompanied with more recent research within the field of cyber security culture. The study was conducted as a descriptive multiple-case study with participants from three different sectors within the critical societal organizations. The data was collected through a qualitative method including elements from grounded theory, and I conducted a total of 9 in-depth interviews of employees that worked with security and/or cyber security inside the financial services, the power plant industry, and the law enforcement and public security services. After conducting the interviews, they were transcribed before all the data material was coded and categorized by using NVivo. This process helped me gain data material that in turn laid the foundation for the three main categories in my research paper: *cyber security*, *cyber security culture* and *barriers*. These categories are thoroughly discussed in the research paper.

This study has given valuable insight on how to create strong cyber security culture in general, and especially inside organizations considered as critical societal functions. It also provides an overview of what educational programs an organization should implement to improve their employees' cyber risk awareness. Through my discussions I have discovered correlations between existing literature and empirical findings pointing out that risk perception, awareness, attitudes, and behavior are interdependent factors that play a crucial role within cyber security. A lack of understanding and compliance when it comes to cyber

security can often be attributed to a lack of knowledge and competence related to which cyber threats the organization faces and what each employee needs to take responsibility for to prevent cyber incidents. In addition, production and protection are inherent contradictions which often leads to employees taking insecure short-cuts to be as effective as possible.

My conclusion in this study is that building a strong cyber security culture requires a continuous effort over a long period of time to reach out to employees throughout the organization. The involvement and commitment from the leaders of the organization is crucial to succeed in this work, and they must create appropriate strategies and be good role models to foster openness and safe behavior. The organization also needs a simple and effective system for reporting incidents, sharing of information and conduct educational training, so that the employees can achieve better insight and competence of cyber threats the organization faces. Involvement of the users should also be incorporated when developing secure solutions to avoid bypassing and increase their motivation to comply with the security barriers. This will all in turn contribute to the goal of becoming a teaching organization where the employees are empowered to change their behavior and conduct secure behavior online.

Sammendrag

Vi lever i et samfunn som blir mer og mer digitalisert, og med dette kommer også stadig flere trusselaktører og angrepsmetoder på banen. Det å utnytte og lure *brukerne* av systemene har vist seg å være en svært effektiv metode for å få tilgang til sensitiv informasjon, og flere viktige samfunnsfunksjoner har opplevd å bli utsatt for slike digitale angrep de siste par årene. Gjennom sin rolle i samfunnet er denne gruppen spesielt utsatt, og i denne oppgaven har jeg derfor tatt utgangspunkt i den menneskelige faktoren i digital sikkerhet, og hvilke forhold som spiller inn i arbeidet med å skape bevisste brukere som bidrar til å forhindre digitale angrep. Jeg kom derfor frem til følgende problemstilling: *«Hva kjennetegner den digitale sikkerhetskulturen i samfunnskritiske funksjoner, sett fra fagansattes perspektiv?»*.

Begrepet digital sikkerhetskultur er relativt nytt, og litteraturen på området har jeg derfor i hovedsak hentet fra tradisjonelle teorier rundt organisatoriske ulykker, høypålitelige organisasjoner og sikkerhetskultur, samtidig som jeg har supplert med nyere forskning innen digital sikkerhetskultur. Prosjektet ble gjennomført som en deskriptiv flercasestudie med deltagelse fra tre ulike sektorer innen samfunnskritiske funksjoner. Datainnsamlingen ble gjennomført ved bruk av kvalitativ metode inspirert av grounded theory, og jeg gjennomførte totalt ni dybdeintervju av ansatte som jobbet med sikkerhet og/eller digital sikkerhet innenfor finans-, kraft- og justissektoren. Intervjuene ble deretter transkribert, og videre kodet og kategorisert ved hjelp av programmet NVivo. Etter denne prosessen satt jeg igjen med et selektert datamateriale som dannet grunnlaget for mine tre hovedkategorier; *digital sikkerhet*, *digital sikkerhetskultur* og *barrierer*. Disse kategoriene har videre dannet grunnlaget for drøfting og konklusjon i oppgaven.

Denne studien har bidratt med verdifull innsikt når det kommer til hvilke faktorer som fremstår som viktige for å skape en god digital sikkerhetskultur generelt, og spesielt innen samfunnskritiske funksjoner. I tillegg har den gitt en oversikt over hvilke tiltak som fremstår som mest hensiktsmessige for å øke de ansattes digitale bevissthet. Gjennom mine analyser og drøftinger har jeg funnet direkte sammenhenger mellom de empiriske funnene og eksisterende litteratur som blant annet viser at risikoforståelse, bevissthet, holdninger og atferd påvirker hverandre gjensidig og spiller en særskilt viktig rolle innenfor arbeidet med digital sikkerhet. Mangel på forståelse for og etterlevelse av digitale sikkerhetstiltak bunner i mange tilfeller ut i manglende kunnskap og kompetanse om hvilke digitale trusler virksomheten står overfor og hvilken betydning den enkelte ansatte har for å forhindre digitale angrep. I tillegg vil den

iboende målkonflikten mellom sikkerhet og produksjon ofte føre til at ansatte tar mindre sikre snarveier for å være mest mulig effektive, på tross av både kunnskap og bevissthet om farene forbundet med det.

Min konklusjon er at det å skape en god digital sikkerhetskultur krever kontinuerlig innsats over tid for å nå ut til alle ansatte innenfor ulike deler av virksomheten. Ledelsens involvering og forpliktelse er avgjørende for å lykkes med dette arbeidet, og de må både utarbeide gode strategier og gå foran som gode rollemodeller når det gjelder åpenhet og sikker digital atferd. Videre trengs det et godt system for varsling, informasjonsdeling og opplæring, slik at de ansatte får mer kunnskap og kompetanse om den digitale risikoen de står overfor. En involvering av brukerne i utviklingen av sikre teknologiske løsninger vil også kunne føre til en bedre forståelse for tiltakene og mer motivasjon til å følge dem. Sammen vil alt dette bidra til at virksomhetene blir lærende organisasjoner som faktisk klarer å endre de ansattes digitale atferd i en positiv retning.

Forord

Denne masteroppgaven markerer avslutningen på mitt treårige deltidsstudium Master i beredskap og kriseledelse, ved Nord Universitet. Oppgaven tar for seg digital sikkerhetskultur i samfunnskritiske funksjoner og bakgrunnen for dette valget var min egen interesse for organisasjonskultur generelt og sikkerhetskultur spesielt, og et ønske om å lære mer om dette i en digital kontekst. Prosessen har vært veldig interessant og lærerik og har gitt meg en dypere innsikt i feltet digital sikkerhet, noe som forhåpentligvis også kan komme andre til gode gjennom denne oppgaven.

Jeg ønsker å rette en stor takk til min veileder, Jan-Oddvar Sørnes, for meget god veiledning og konstruktive tilbakemeldinger gjennom hele prosessen. Jeg vil også takke alle som stilte opp til intervju og dermed i aller høyeste grad bidro til gjennomføringen av oppgaven! Dere delte opplevelser, erfaringer og refleksjoner som har bidratt til mye god og interessant kunnskap om digital sikkerhet. Videre vil jeg også rette en takk til både tidligere og nåværende arbeidsgiver som har lagt til rette og gitt meg muligheten til å fullføre dette studiet.

Det har ikke alltid vært like lett å kombinere studier, fulltidsjobb og to små barn, men takket være en tålmodig og forståelsesfull samboer har jeg likevel kommet meg gjennom det – tusen takk Jan Erik.

Oslo, 25. mai 2021

Tone Gunnes

Innhold

Oversikt over tabeller og figurer

Figurer:

Tabeller:

Oversikt over vedlegg

Begrepsordliste

Samfunnskritiske funksjoner:	Funksjoner som samfunnet ikke kan klare seg uten i syv døgn eller kortere uten at det truer befolkningens sikkerhet og/eller trygghet.
DSB:	Direktoratet for samfunnssikkerhet og beredskap
PST:	Politiets sikkerhetstjeneste
NSM:	Nasjonal sikkerhetsmyndighet
Grunnleggende nasjonal funksjon:	Funksjoner hvor helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.
Sikkerhetsloven:	Lov om nasjonal sikkerhet, av 01.01.2019. Lov som bl.a. har til formål å kunne motvirke trusler mot Norges sikkerhet.
IKT	Informasjons- og kommunikasjonsteknologi
NorSIS	Norsk senter for informasjonssikring
Digdir	Digitaliseringsdirektoratet

1 Innledning

Det er gjort mye forskning på generell krisehåndtering opp mot naturkatastrofer, menneskelige intenderte handlinger og kriser innad i en organisasjon. Vi lever imidlertid i en verden som blir stadig mer digitalisert og hvor teknologiske løsninger preger mye av hverdagen, både i form av avanserte systemer i daglig drift, men også til bruk i krisesituasjoner. Norge ligger i verdenstoppen når det gjelder digitalisering og vi har i stor grad gjort oss avhengige av disse systemene, samtidig som den påfølgende sårbarheten ikke blir erkjent og håndtert i tilstrekkelig grad (Samfunnssikkerhetskonferansen, 2020). Flere store virksomheter har de siste årene blitt utsatt for alvorlige digitale angrep som har forårsaket svikt i både produksjon og omdømme, og digital sikkerhet er derfor et område som bør få mer fokus for å unngå både økonomiske tap og i verste fall tap av menneskeliv på grunn av bortfall av kritiske systemer.

Norges første nasjonale strategi for digital sikkerhet kom allerede i 2003, og har etter den tid blitt revidert fire ganger med siste utgave i 2019 (Departementene, 2019a). Den første stortingsmeldingen om IKT-sikkerhet kom imidlertid ikke før i 2017 etter at Lysneutvalget publiserte sin sårbarhetsrapport i 2015 og påpekte de sårbarhetene som følger av den raske teknologiske utviklingen og digitaliseringen her i Norge (Justis- og beredskapsdepartementet, 2017; NOU 2015:13). Årlig utgis det også fire offentlige trussel- og risikovurderinger, herunder fra Direktoratet for samfunnssikkerhet og beredskap (DSB), Politiets sikkerhetstjeneste (PST), Etterretningstjenesten og Nasjonal Sikkerhetsmyndighet (NSM), og allerede i 2012 påpekte DSB at cyberangrep var et aktuelt krisescenario. De skrev samtidig at dette var sjeldne hendelser, men understreket imidlertid at det var svært alvorlige hendelser med et stort skadepotensial, spesielt sett opp mot kritiske samfunnsfunksjoner. Det ble også understreket at «manglende sikkerhetsbevissthet hos brukere er en utfordring» (DSB, 2012, s. 74). Den gangen var det imidlertid dedikert tre sider til denne type angrep, mens det i 2019 ble satt av et tosifret antall sider som omhandler samme tema hvor det også kommer frem at frekvensen av slike angrep har endret seg til å være «kontinuerlig og utgjør en stor utfordring for samfunnet og mange virksomheter» (DSB, 2019, s. 197).

NSM påpeker i sin trusselvurdering for 2021 at aktivitetsnivået mot norske virksomheter og institusjoner var høyere i 2020 sammenlignet med tidligere år, og de ser ingen tegn til at dette avtar (NSM, 2021, s. 7). De understreker også at det fremdeles er mennesker som utgjør en av de største sårbarhetene og som i ytterste konsekvens legger til

rette for et vellykket datainnbrudd (NSM, 2021, s. 37). PST påpeker den samme trenden og sier at den digitale trusselen fra statlige aktører er alvorlig, og at ingenting tyder på at den blir redusert (PST, 2021). Sammen med den nasjonale strategien for digital sikkerhet fra 2019 (Departementene, 2019a) ble det også utgitt en tiltaksoversikt for å bedre den digitale sikkerheten i Norge (Departementene, 2019b). Blant de sentrale tiltakene som trekkes frem er blant annet innføringen av den nye Sikkerhetsloven, hvor det er fastsatt krav om sikring av alle skjermingsverdige informasjonssystemer for virksomheter som regnes som en grunnleggende nasjonal funksjon (Departementene, 2019b, s. 2; Sikkerhetsloven, 2019). Videre legger de frem tiltak for digital sikkerhetskompetanse, hvor det nevnes bevisstgjørende tiltak og bedret digital sikkerhetskultur (Departementene, 2019b, s. 26). Av tiltakene som nevnes for å øke virksomheters egenevne til å beskytte seg mot uønskede digitale hendelser er det blant annet tiltak rettet mot ledelse, risikostyring og sikkerhetskultur. Her understreker de videre at ansattes kunnskaper og holdninger er vesentlig for at virksomheter kan operere sikkert, og at ledelsen må kommunisere mål og prioriteringer for digital sikkerhet tydelig og effektivt, og fremstå som gode rollemodeller. I tillegg står det at samtlige ansatte og ledere bør følge en tilpasset opplæring, kompetansebygging og bevisstgjøring om sikkerhet. Det anbefales videre at virksomheten kartlegger sin egen sikkerhetskultur og avdekker et eventuelt gap mellom nåværende nivå og ønsket tilstand (Departementene, 2019b, s. 33-34).

NSM nevner også arbeid med økt sikkerhetsbevissthet og god sikkerhetskultur som et av de anbefalte tiltakene for bedre IKT-sikkerhet i deres trusselvurdering fra 2021 (NSM, 2021, s. 43), og dette viser at fokuset på de menneskelige og organisatoriske delene av digital sikkerhet får stadig mer oppmerksomhet. Likevel er det relativt lite forskning på dette området sammenlignet med de mer tradisjonelle krisehendelsene, og med bakgrunn i dette så jeg derfor behovet for å undersøke dette nærmere. Jeg har stor interesse for organisasjonskultur generelt, og med min egen bakgrunn fra en nødetat kombinert med flere års studier innenfor krisehåndtering og beredskap, har jeg også utviklet en interesse for sikkerhetskultur spesielt. Med denne erfaringen har jeg gjort meg noen antakelser om at digital sikkerhet for mange oppleves som skumlere og mer fjernt enn de tradisjonelle sikkerhetshendelsene, og jeg ønsket derfor å se på sikkerhetskultur i en digital kontekst.

1.1 Aktualisering

Mange påpeker at det er *menneskene som bruker* systemene som er den største utfordringen når det kommer til digital sikkerhet, og at det kreves bevisstgjøring av samtlige ansatte for å forhindre digitale kriser og uønskede cyberhendelser (Bergsjø, Windvik & Øverlier, 2020; Nätt & Heide, 2015, NorSIS, 2020). «Ledelsen i mange norske selskaper (…) overlater til IT-avdelingen å «styre med sikkerheten», uten å tenke nok over at styret selv har ansvar for å bygge opp en bedriftskultur som tar sikkerhet på alvor.» (Telenor, u.å.). Digital sikkerhet blir altså ofte ansett for å være noe som tilhører IT-avdelingen, og som i liten grad angår resten av virksomheten. Slike holdninger gir grunn til å anta at lite fokus på digital sikkerhet også fører til at organisasjonen ikke prioriterer å ha verken de beste teknologiske løsningene for å håndtere sårbarhetene, eller en god strategi for opplæring og bevisstgjøring av de ansatte. Det er derfor sannsynlig at mange vil rammes av digitale kriser dersom man ikke arbeider aktivt for at organisasjonen som helhet skal bli mer robust mot denne typen hendelser.

Begrepet digital sikkerhetskultur ble beskrevet og kartlagt for første gang i Norge i 2016 da Norsk senter for informasjonssikring (NorSIS) publiserte rapporten «The Norwegian Cyber Security Culture», og har siden blitt revidert frem til siste utgave av rapporten som kom i 2020. Jeg vil gå nærmere inn på dette begrepet i teori-kapittelet, men NorSIS lister opp 8 kjerneområder som de mener er viktige når det kommer til digital sikkerhetskultur, blant annet fellesskap, tillit, risikooppfattelse, kompetanse og interesse, samt atferdsmønstre (NorSIS, 2020). Digitaliseringsdirektoratet (Digdir) gjennomførte en undersøkelse i 2018 rundt temaet sikkerhetskultur, og den viste at bare 40% av virksomhetene hadde kartlagt eller målt sikkerhetskulturen i virksomheten sin (Digdir, 2018, s. 34). De har derfor utviklet en veileder i kompetanse- og kulturutvikling innen digital sikkerhet, samt et nytt informasjonshefte om digital sikkerhetskultur som ble utgitt i februar 2021 (Digdir, u.å.; Digdir, 2021). Dette tyder på at digital sikkerhetskultur både *trenger* økt oppmerksomhet og prioritering i mange organisasjoner, men at det også har fått mer fokus av faglige, nasjonale organer.

NSM påpeker at det er når viktige samfunnsfunksjoner bli digitalisert og sårbare for digitale trusler, at vi har mest å tape (NSM, 2019, s. 5). Jeg ønsket derfor å gå dypere inn i dette og se på hvor godt forberedt de viktigste aktørene i samfunnet vårt er når det gjelder digital sikkerhet, da spesielt med tanke på de menneskelige og organisatoriske forholdene i form av en digital sikkerhetskultur. Jeg er av den oppfatning at fasen *før* en krise oppstår er den viktigste fasen, og at det er her man både legger grunnlaget for å forhindre at kriser skjer,

men også bidrar til en god håndtering dersom de likevel skulle oppstå. Det er også denne fasen som preger «hverdagen», og hvor de fleste til enhver tid befinner seg. Samtidig er det denne førkrisefasen som risikerer å bli minst prioritert, nettopp fordi forebyggende innsats er så vanskelig å måle i kroner og øre, noe som er en viktig faktor for ledelsen i ulike virksomheter.

Gjennom studiene jeg har vært gjennom har jeg fått en god innføring i ulike teorier knyttet til begrepet sikkerhetskultur og organisatoriske ulykker, og dette har både vært med på å prege min forforståelse i forkant av undersøkelsen, og også bidratt til å besvare problemstillingen. Jeg har valgt å bruke tradisjonelle teorier innen sikkerhetskultur fordi de i stor grad også vil være relevante for det digitale domenet, samtidig som jeg supplerer med forskning gjort de senere år innenfor cyber- og informasjonssikkerhet. På denne måten vil jeg vise at arbeidet med å forhindre digitale angrep og skape en god digital sikkerhetskultur ikke er mer fremmed eller vanskeligere enn arbeidet med de mer tradisjonelle krisehendelsene.

1.2 Problemstilling og forskningsspørsmål

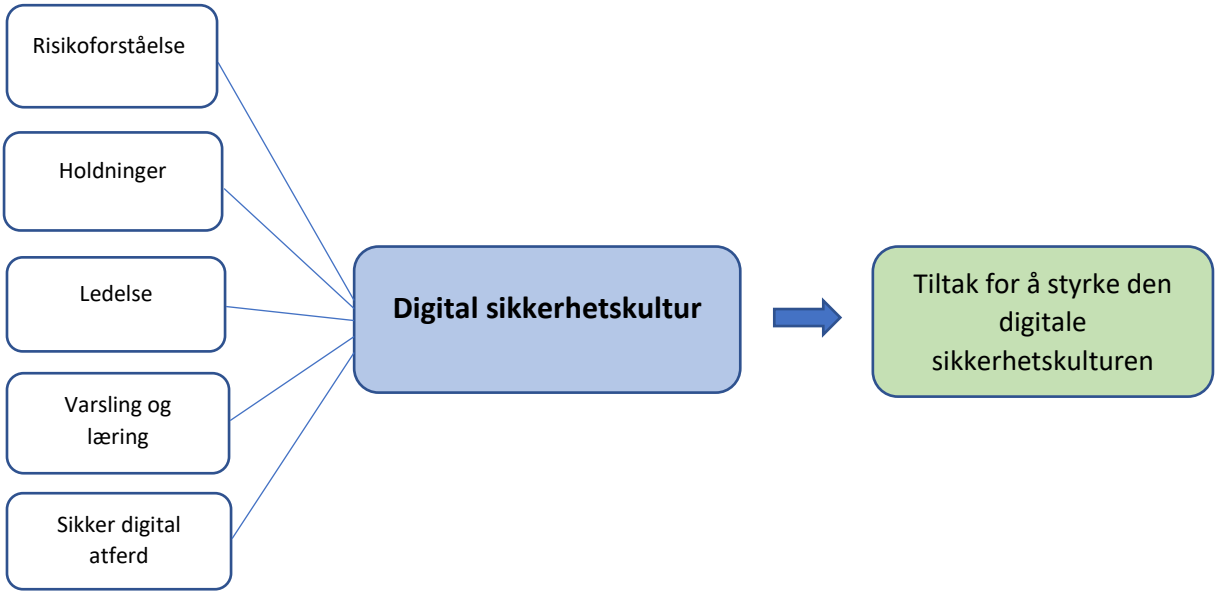
Med min interesse for sikkerhetskultur og et inntrykk av at digital sikkerhet trenger å få mer oppmerksomhet, utarbeidet jeg en problemstilling som kunne være med på å konkretisere hva digital sikkerhetskultur inneholder for derav å kunne si noe om hva som skal til for å skape en *god* digital sikkerhetskultur og bidra til å gjøre det mer håndfast for alle som jobber med dette feltet. På bakgrunn av dette kom jeg frem til følgende problemstilling:

«Hva kjennetegner den digitale sikkerhetskulturen i samfunnskritiske funksjoner, sett fra fagansattes perspektiv?»

For å besvare problemstillingen ble følgende forskningsspørsmål benyttet:

- *Hvilken digital risiko opplever virksomhetene at de står overfor?*
- *Hvilke holdninger eksisterer opp mot digital sikkerhet?*
- *Hvilken rolle spiller ledelsen i arbeidet med digital sikkerhetskultur?*
- *Hvordan ivaretar man varsling og læring i virksomheten?*
- *Hvilke utfordringer opplever de med tanke på sikker digital atferd?*
- *Hvilke forebyggende tiltak har de for å styrke den digitale sikkerhetskulturen?*

På bakgrunn av dette utviklet jeg en forskningsmodell som knytter problemstillingen og forskningsspørsmålene sammen:



Figur 1.1. Forskingsmodell

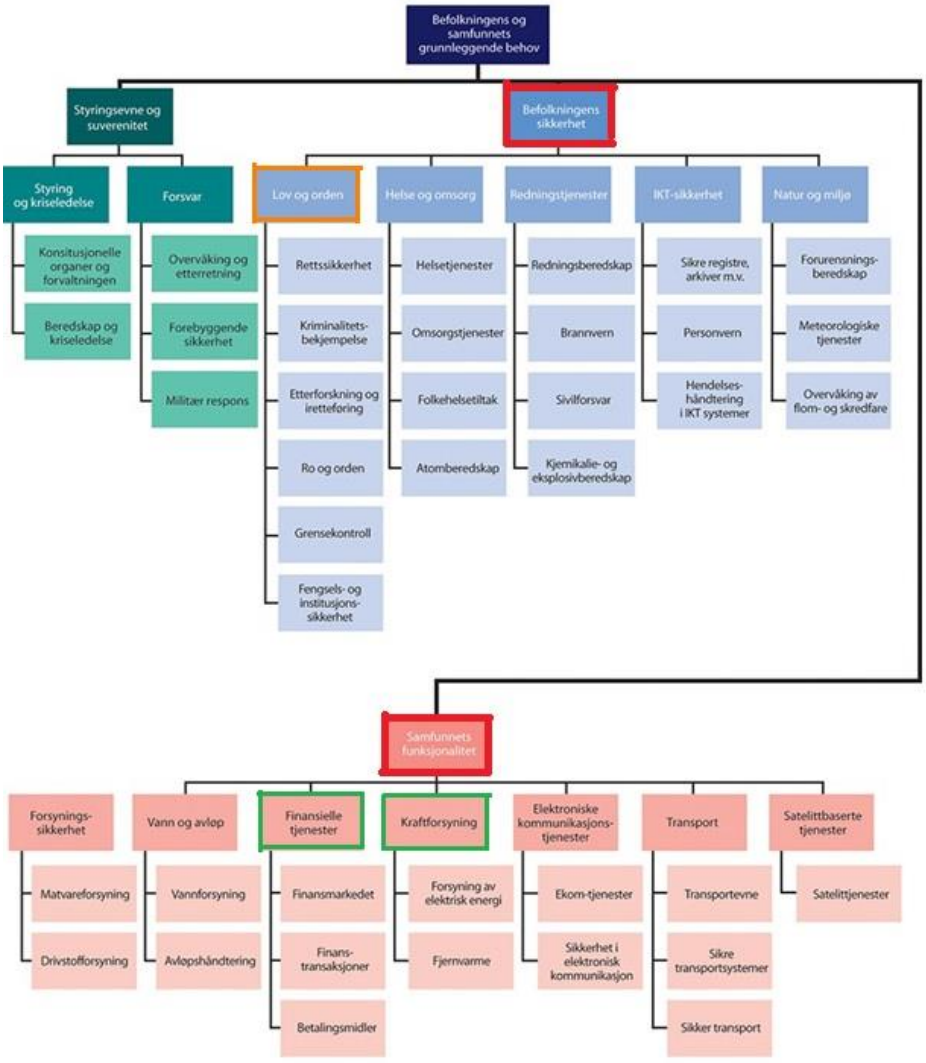
I og med at dette er en oppgave innenfor samfunnsvitenskapelige fag vil fokuset mitt være på de menneskelige og organisatoriske forholdene, og på hvilke barrierer og tiltak de ulike virksomhetene har innenfor dette for å bedre den digitale sikkerheten. Jeg vil derfor ikke gå inn på teknologiske systemer og løsninger virksomhetene har for å forhindre digitale angrep. Jeg håper med denne oppgaven å kunne bidra med suksessfaktorer knyttet til forebygging og forhindring av digitale angrep og kriser, slik at organisasjoner kan nyttiggjøre seg dette i deres arbeid med kriseledelse opp mot digital sikkerhet.

1.3 Operasjonalisering og avgrensning

1.3.1 Samfunnskritiske funksjoner

Samfunnets kritiske funksjoner er definert av Direktoratet for samfunnssikkerhet og beredskap (DSB), og de legger til grunn at dette er funksjoner som kjennetegnes av at svikt i disse funksjonene raskt kan medføre tap og skade og at det dermed er særlig viktig å unngå et avbrudd i disse (DSB, 2016, s. 26). Det er på grunnlag av dette satt en avgrensning i tid, hvor

de regner at dette er funksjoner som samfunnet ikke kan klare seg uten i syv døgn eller kortere uten at det truer befolkningens sikkerhet og/eller trygghet, og at det inntreffer hendelser som medfører behov for beredskapsressurser i løpet av denne perioden (DSB, 2016, s. 26). DSB har utarbeidet en oversikt over alle sektorene og etatene som er regnet som samfunnskritisk, som vises i figur 1.2.



Figur 1.2. Oversikt over Norges samfunnskritiske funksjoner (DSB, 2016). De deltakende sektorene i studien er uthevet.

Grunnleggende nasjonale funksjoner ble lansert som begrep i forbindelse med den nye Sikkerhetsloven som trådte i kraft 1.januar 2019, og omhandler

> «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser» (Sikkerhetsloven, 2018, § 1-5, nr. 2).

Disse definisjonene overlapper dermed hverandre i en del tilfeller, men jeg valgte å forholde meg til oversikten over kritiske samfunnsfunksjoner og rekrutterte informanter fra to av hovedkategoriene, herunder befolkningens sikkerhet og samfunnets funksjonalitet. Valget falt videre på en sektor innen «Lov og orden», en sektor innen «Finansielle tjenester» og en fra «Kraftforsyning». Samfunnskritiske funksjoner har et særegent ansvar i å ivareta befolkningens trygghet og eksistens, og jeg ville fokusere på disse nettopp fordi de har en så viktig rolle i samfunnets sikkerhetsarbeid og dermed også bør være foregangsvirksomheter for andre organisasjoner. Samtidig valgte jeg ulike sektorer fordi jeg ville se om det var forskjeller i fokuset på, og arbeidet med, digital sikkerhet selv om alle var definert som samfunnskritisk. Valget av informanter falt på ansatte med et fagansvar innen sikkerhet generelt og/eller digital sikkerhet fordi disse kunne gi et godt innblikk i den digitale sikkerhetskulturen i egen virksomhet.

1.3.2 Sikkerhet – forebygging av kriser og uønskede hendelser

Sikkerhet kan defineres som en tilstand med fravær av uønskede hendelser, frykt og fare (Norsk Standard, referert i Bergsjø et al., 2020, s. 19). Man vil aldri kunne unngå alle mulige uønskede hendelser, men sikkerhet knyttes i mange tilfeller opp mot det forebyggende arbeidet som gjøres for å redusere sannsynligheten for at de skal inntreffe. Det omfatter også den evnen et system har til å unngå skader og tap, og kan kobles både opp mot det fysiske miljøet, og til menneskelige og sosiale faktorer (Aven, Boyesen, Njå, Olsen & Sandve, 2004). På denne måten eksisterer sikkerhet som begrep på flere ulike nivå, og noe som vi kan være med å påvirke gjennom de handlinger og valg vi gjør (Aven et al., 2004).

Som en videreutvikling av begrepet sikkerhet ble begrepet *samfunnssikkerhet* første gang definert i Stortingsmelding nr. 17 (2001-2002), men har siden den gang blitt revidert og oppdatert flere ganger. I Meld. St. 10 (2016-2017) har de utvidet begrepet slik at det i større grad passer til det samfunnet vi lever i i dag, med mer teknologi og flere bevisste angrep mot viktige samfunnsfunksjoner:

> Samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av

> naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger. (Justis- og beredskapsdepartementet, 2017).

Selv om uønskede hendelser ikke nødvendigvis fører til en stor krise, vil prosessen likevel være lik da den akutte hendelsen sees i sammenheng med hva som skjer både i forkant og i etterkant av selve hendelsen. Det er en sirkulær prosess hvor den første fasen blir en inkubasjonsfase med akkumulering av latente strukturer og hvor det etableres en systemforståelse som ikke fanger opp hvordan ulykker kan utvikle seg (Engen, Kruke, Lindøe, Olsen, Olsen & Pettersen, 2016). Mitt fokus i denne oppgaven er altså på de tiltakene som blir gjort i forkant av en uønsket hendelse, hvor man bygger opp organisasjonen på en måte som gjør den mer robust til å takle de latente forholdene som i verste fall kan føre til en krise.

1.3.3 Digital sikkerhet

Det var vanskelig å skulle komme til en konklusjon om hvilket begrep jeg skulle bruke i oppgaven, da ulike organisasjoner og virksomheter også benytter seg av ulike begrep når det kommer til dette feltet. Mange bruker begrepet «IKT-sikkerhet» fordi de mener det favner bredere enn begrepet «cybersikkerhet» som ensidig fokuserer på det digitale. De fleste virksomheter har fokus på å beskytte *verdien* informasjon, uavhengig av om det er fysisk eller digitalt. IKT-sikkerhet blir dermed et mer samlende begrep for det man ønsker å jobbe for. Mitt fokus i denne oppgaven er imidlertid på det som skjer i det digitale rom, og ikke på hvilke utfordringer og tiltak virksomheter har når det kommer til å beskytte informasjonen rent fysisk, selv om dette også er en del av informasjonssikkerheten. Jeg velger derfor å bruke begrepet digital sikkerhet videre i oppgaven.

«Digital sikkerhet handler om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi. Brukes ofte synonymt med begrepene IKT-sikkerhet og cybersikkerhet.» (Departementene, 2019a). I denne oppgaven ser jeg altså på digital sikkerhet som tiltak for å forebygge og begrense uønskede hendelser når det gjelder digitale sårbarheter og angrep (Bergsjø et al., 2020). Datasikkerhet er også et begrep som faller inn under digital sikkerhet, og Nätt & Heide (2015, s. 17) beskriver datasikkerhet som din egen bevissthet om hva hackere og svindlere kan gjøre, samt hvordan du kan hindre at det skjer. Det er også bevissthet om hvordan du oppdager at noe galt har skjedd, og hvordan du kan minimere skadene. De påpeker samtidig at

mangelen på forståelse for teknologien som ligger bak hackerangrep, er den største sikkerhetsutfordringen, altså det at brukerne ikke forstår hva som faktisk er mulig å gjøre for en hacker, og hvor enkelt det kan være (Nätt & Heide, 2015, s. 25).

1.3.4 Digitale angrep

Med digitale angrep mener jeg alt av datakriminalitet og såkalt «social engineering» som begås gjennom utnyttelse av informasjonsteknologi – enten angriperen er ute etter økonomisk gevinst, hevn, status, utpressing eller liknende. Dette kan skje gjennom e-post med infiserte vedlegg, lenker til falske nettsider, koding av passord, pop-up vinduer med beskjed om at datamaskinen er låst og liknende (Nätt & Heide, 2015). Når jeg snakker om sårbarheten knyttet til digitaliseringen har jeg som tidligere nevnt fokus på de menneskelige og organisatoriske faktorene, ikke de rent teknologiske. En organisasjon er ikke sterkere enn sitt svakeste ledd, og det er ofte de ansatte i førstelinje som i stor grad må bevisstgjøres for å bevare den digitale sikkerheten i en virksomhet. Sårbarheten innen det digitale feltet øker, og denne sårbarheten viser et behov for å ta digital sikkerhet på alvor for å unngå store og grenseoverskridende kriser som følge av digitale angrep.

1.4 Oppgavens oppbygning

Oppgaven er delt inn i totalt seks kapitler. Kapittel 1 har gitt en innføring i problemstillingen og bakgrunnen for denne, samt en operasjonalisering av sentrale begrep og avgrensning for oppgaven. Kapittel 2 tar for seg de teoretiske momentene som drøftingen og analysen bygger på, og jeg har her fokus på sentral internasjonal litteratur innen begrepene organisasjonskultur, sikkerhetskultur og organisatoriske ulykker. I kapittel 3 beskriver jeg inngående om hvilket design og hvilken metode jeg har brukt for å gjennomføre studien – en deskriptiv flercasestudie med kvalitativ datainnsamling gjennom ni dybdeintervju. Resultatene fra datainnsamlingen blir presentert i kapittel 4 i form av tre hovedkategorier; digital sikkerhet, digital sikkerhetskultur og barrierer. Funnene blir vist gjennom en fremlegging av hovedfunn samt sitater fra informantene. Funnene blir videre drøftet og diskutert i kapittel 5, hvor momenter fra litteraturen blir knyttet direkte opp mot forskningsspørsmålene og de empiriske funnene for å vise sammenhenger og eventuelle avvik fra teorien. Til slutt blir konklusjon og implikasjoner presentert i kapittel 6.

2 Teoretiske momenter

Gjennom dette kapittelet vil jeg belyse deler av teorien som er relevant for problemstillingen. Noe av dette stammer fra anerkjente internasjonale klassikere innenfor teorier rundt organisatoriske ulykker og høypålitelighet, mens noe er mer spisset forskning innen sikkerhet- og beredskapsarbeid med tilknytning til Norge og mer lokale forhold. Hensikten med dette kapittelet er å gi et bakteppe og utgangspunkt for den videre drøftingen av mine konkrete funn.

2.1 Risikoforståelse og bevisstgjøring

Aven et al. (2004, s. 21) viser til den tyske sosiologen Ulrich Bech som skriver om dagens «risikosamfunn», som kjennetegnes ved samspillet mellom komplisert teknologi, komplekse organisasjoner og individuell handling i omgivelser som stadig endrer seg, samtidig som det blir mer avhengighet på tvers av både virksomheter og geografiske områder. Dette har gitt oss store gevinster når det kommer til produktivitet og effektivitet, men samtidig har det også ført med seg økt sårbarhet og større konsekvenser dersom en uønsket hendelse inntreffer (Aven et al., 2004, s. 22). Risiko er dermed noe vi må forholde oss til på alle nivå i samfunnet, og vår oppfatning og forståelse av risiko har betydning for hvordan vi til syvende og sist evner å håndtere en uønsket hendelse. Det er flere ulike tilnærminger til risiko, men jeg velger å forholde meg til begrepet risiko som «kombinasjonen av usikkerhet og konsekvens/utfall av en gitt aktivitet» (Aven et al., 2004, s. 37). Både usikkerhetsmomentet og det faktum at risiko også er knyttet opp mot en *fare*, gjør at risikovurderingen er avhengig av både *hvem* som vurderer og *hva* som vurderes.

Begrepene risikoforståelse og risikopersepsjon sier derfor noe om hvordan vi forstår, oppfatter og håndterer risiko og farer (Aven et al., 2004; Moldjord, C., Arntzen, A., Firing, K., Solberg, O.A. & Laberg, J.C., 2007). Mennesker utgjør i de fleste virksomheter den største delen av virksomhetens produksjon, enten ved at de direkte utfører arbeidet, at de styrer maskinene som utfører arbeidet eller at de overvåker systemene som styrer maskinene. Uansett vil mennesker i de aller fleste virksomheter utgjøre mye av kjernen i det som skjer i organisasjonen, og ingen kan dermed utelukke den menneskelige faktoren når det kommer til verken produksjon eller sikkerhet. Men mennesker vil alltid gjøre feil, rett og slett fordi vi er mennesker og ikke maskiner. Det vi gjør er et resultat av mange kompliserte prosesser; vi sanser, vi oppfatter, vi vurderer og vi handler. Og hva vi ser og oppfatter er igjen avhengig av

hvordan vi tolker situasjonen vi står i. Én og samme situasjon kan dermed oppfattes forskjellig fra person til person, noe som gjør verden mye mer komplisert. Bevisstgjøring er derfor avgjørende for en organisasjons sikkerhet – altså hvordan man kan *påvirke* folks forståelse og oppfatning av hvilken risiko og hvilke sårbarheter man står overfor, og dermed også oppmerksomheten den enkelte vier til sikkerhetstiltak (Aven et al., 2004). En god bevisstgjøring rundt ulike former for risiko vil også ha betydning for kriseerkjennelsen, som kan være avgjørende for hvor bra en krise vil bli håndtert. Har de ansatte en riktig forståelse av risikoen og sårbarhetene, vil de mest sannsynlig også evne å identifisere en krise på et tidligere stadium og dermed sette i verk passende tiltak (Fimreite, Lango, Lægreid & Rykkja, 2011). Både kultur og følelser spiller altså inn når folk vurderer farer og risiko, noe som gjør at risiko ikke kan sies å være en objektiv måleenhet, men et resultat av både subjektive og kulturelle faktorer (Aven et al., 2004; Moldjord et al., 2007).

2.2 Organisasjonskultur

Organisasjonskultur har blitt hevdet å være nøkkelen til suksess, etter at flere forskere og forfattere av populære bøker på starten av 1980-tallet mente at riktig bedriftskultur var det som skilte de suksessrike bedriftene fra de som ikke hadde gjort det så bra (Bang, 2011). En populær måte å definere organisasjonskultur på er å si at det er «måten vi gjør tingene på her hos oss» (Deal & Kennedy, referert i Bang, 2011). Selv om denne definisjonen av begrepet er enkel og lett å forstå, er den imidlertid veldig lite spesifikk og sier lite om hva kultur faktisk er. Bang (2011, s. 23) oppsummerer ulike definisjoner i én enkelt definisjon: «Organisasjonskultur er de sett av felles verdier, normer og virkelighetsoppfatninger som utvikler seg i en organisasjon når medlemmene samhandler med hverandre og omgivelsene». Edgar Schein (referert i Jacobsen & Thorsvik, 2013, s. 130) påpeker også at organisasjonskulturen bare opprettholdes så lenge den oppfattes som riktig, og den blir videre lært bort til nye medlemmer som den riktige måten å oppfatte, tenke og føle på. Kjernen i organisasjonskultur er altså at det er et sett med «sannheter» som medlemmene ikke stiller spørsmålstegn ved så lenge det ser ut til å fungere bra, og den vokser frem gjennom interaksjon mellom medlemmene og omgivelsene (Jacobsen & Thorsvik, 2013; Bang, 2011).

Organisasjoners kulturer skiller seg fra hverandre blant annet gjennom hvilket syn man har på menneskers handlinger, hvordan organisasjonen kommer frem til «sannhet», og hvilke antakelser man har om menneskelig natur (Jacobsen & Thorsvik, 2013). Det er heller

ikke slik at det kun finnes én kultur innad i en organisasjon, og ifølge differensieringsperspektivet skapes det subkulturer som eksisterer side om side innad i organisasjonen (Bang, 2011; Jacobsen & Thorsvik, 2013). Dette skyldes ofte organisasjonsstrukturen og hvordan man har delt inn organisasjonen i ulike avdelinger og seksjoner – med ulike delmål og arbeidsoppgaver (Jacobsen & Thorsvik, 2013). I tillegg er dette også gjerne et resultat av at ulike avdelinger representerer ulike fagmiljøer og profesjoner, og kulturelementer som er internalisert gjennom utdannelse kan veie minst like sterkt som de man prøver å bygge opp i den aktuelle organisasjonen. I tillegg vil en avdeling selektivt orientere seg mot de deler av omgivelsene som er relevante for deres arbeid, og ignorere annet. En organisasjon vil derfor alltid bestå av flere subkulturer, men det vil imidlertid ikke være et problem så lenge de ikke utgjør en motkultur som utfordrer den dominerende organisasjonskulturen eller skaper konflikter på tvers av andre subkulturer (Jacobsen & Thorsvik, 2013; Bang, 2011). Faren med subkulturer er derimot at en slik selektiv persepsjon og rasjonalisering kombinert med en systematisk skjev informasjonstilgang, ofte vil føre til at de ansatte tror at det de selv jobber med er viktigere enn andre oppgaver i organisasjonen, og derav lede til det man omtaler som «gruppetenkning». Det kan dermed bli vanskeligere å utvikle en felles organisasjonskultur (Jacobsen & Thorsvik, 2013).

Ledelse er et viktig aspekt i arbeidet med å bygge en organisasjonskultur, og en leder vil alltid påvirke de ansattes holdninger og atferd. Brukes den riktig, kan organisasjonskulturen benyttes som et styringsmiddel i form av at den angir hva som er passende atferd og det utvikles normer som de ansatte innretter seg etter (Jacobsen & Thorsvik, 2013). Ledere vil påvirke organisasjonskulturen gjennom flere kanaler, blant annet gjennom hva de retter oppmerksomhet mot, deres reaksjoner på kritiske hendelser og kriser i organisasjonen, hvordan de fordeler budsjett og ressurser, og sin egen synlige atferd (Bang, 2011, s. 80-81). Ledelsens mål og strategi gir dermed uttrykk for hva som verdsettes og anses som viktig, og dersom ledere ikke anerkjenner arbeidet med sikkerhet og de tiltakene som iverksettes, er det derfor overveiende sannsynlig at man mislykkes i å skape gode holdninger blant de andre ansatte. Det samme gjelder hvis organisasjonen har ledere som ikke tør eller vil innrømme sin egen feilbarlighet; da er det liten sannsynlighet for at de resterende ansatte står frem og sier ifra om feil eller uønskede hendelser (Kvalnes, 2010). Ledere har dermed stor påvirkningskraft når det kommer til organisasjonens holdninger og verdier, og dette blir spesielt viktig i arbeidet med å skape en god sikkerhetskultur.

2.3 Sikkerhetskultur

Sikkerhetskulturen er en del av organisasjonskulturen, og begrepet ble ifølge flere kilder først brukt i evalueringsarbeidet i etterkant av Tsjernobyl-ulykken i 1986 for å beskrive årsakene til denne katastrofale hendelsen (Laumann, 2011, s. 281; Reason, 1997, s. 194). Det fins mange til dels ulike definisjoner av begrepet, men felles for de aller fleste er at de knytter sikkerhetskultur opp mot de holdninger, antakelser, regler og handlinger som de ansatte i en organisasjon har med tanke på sikkerhet og forhold som kan anses som skadelig eller farlig (Laumann, 2011, s. 282). Dette samsvarer også med definisjonen til The Health and Safety Commission i England (referert i Reason, 1997, s. 194 og Aven et al., 2004, s. 34), hvor de beskriver sikkerhetskultur som:

> (…) produktet av individets og gruppens verdier og holdninger, av kompetanse og atferdsmønstre som viser forpliktelse og dyktighet i forhold til organisasjonens helse- og sikkerhetsprogrammer. Organisasjoner som har en positiv sikkerhetskultur er kjennetegnet ved en kommunikasjon bygget på gjensidig tillit, felles oppfatning om betydningen av sikkerhet, og med tiltro til at organisasjonens sikkerhetsmål fungerer effektivt (Aven et al., 2004, s. 34).

Sikkerhetskulturen handler altså om den kollektive forståelsen av hva som er farlig og hvordan man bidrar til å redusere farene, og organisasjonens sikkerhetskultur vil kunne virke avgjørende for om man velger snarveier og lettvinte løsninger på bekostning av målene for sikkerhet (Aven et al., 2004, s. 34).

Flere av teoriene rundt sikkerhetskultur legger vekt på ledelsens forpliktelse til arbeidet med sikkerhet, og deres holdninger generelt til kulturen i organisasjonen (Reason, 1997; Kvalnes, 2010; Weick & Sutcliffe, 2015; Turner, 1978). I likhet med byggingen av en god organisasjonskultur, vil ledere altså ha en helt sentral rolle når det kommer til det å påvirke de ansatte til å utvikle gode holdninger til sikkerhetsarbeidet og utøve en sikker atferd (Jacobsen & Thorsvik, 2013). Sikkerhetskultur er ikke noe som eksisterer på siden av alt annet i organisasjonen eller virksomheten, men det er en del av hele samspillet mellom både struktur, kultur og teknologi. For å få en god sikkerhetskultur er det derfor avgjørende at man også har en varslings- og ytringskultur hvor åpenhet og innrømmelse av feil blir verdsatt og sett på som en mulighet til forbedring. Har man en ledelse som selv ikke vil innrømme feil eller straffer ansatte som velger å stå frem, vil dette igjen føre til en fryktkultur hvor viktig

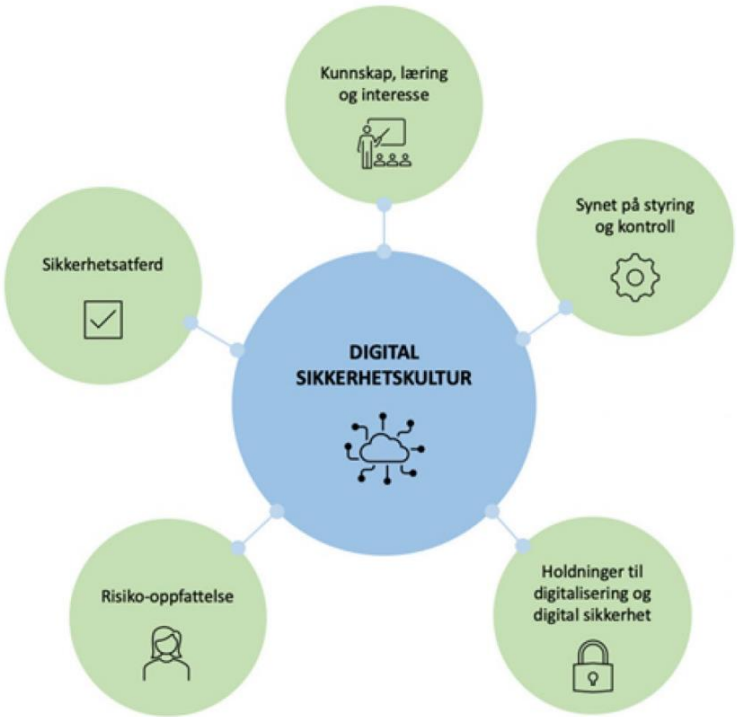
informasjon ikke kommer frem og hvor læring ikke blir en del av organisasjonslivet (Kvalnes, 2010).

Begrepet sikkerhetskultur er altså et ganske omfattende begrep, og et begrep det kan være vanskelig å få helt taket på. Det involverer mange ulike faktorer, og spenner over teori fra både organisasjonsforståelse, feilhandlinger og krisehåndtering. Reason (1997) oppsummerer på sin måte dette når han skriver: «Few phrases occur more frequently in discussions about hazardous technologies than safety culture. Few things are so sought after, and yet so little understood.» (Reason, 1997, s. 191). Sikkerhetskultur blir altså ofte brukt som forklaring på mange ulykker, men samtidig kan det være vanskelig å gå nok i dybden til å fullt ut forstå de ulike årsakene og sammenhengene. Mange har forsøkt å måle sikkerhetskulturen i en organisasjon, men dette kan også by på utfordringer da det å skulle måle holdninger og verdier kan være vanskelig. Det har likevel blitt forsøkt å foreta visse undersøkelser ved hjelp av spørreskjemaer, og flere studier som har blitt utført på bakgrunn av dette har konkludert med at sikkerhetskultur består av følgende hovedelementer: ledelse, risiko, sikkerhetsarrangement, prosedyrer, trening, kompetanse og arbeidspress (Laumann, 2011, s. 284). Dette samsvarer altså med teoriene rundt sikkerhetskultur jeg har referert til over, og viser igjen at det er et sammensatt og komplekst begrep.

2.2.1 MTO og digital sikkerhetskultur

Det er lett å tenke at det man trenger for å beskytte informasjon digitalt, er digitale løsninger og god teknologi. MTO, som står for menneske-teknologi-organisasjon, er imidlertid et begrep som har kommet i forbindelse med den raske utviklingen av teknologien, nettopp for å vise at teknologiske løsninger i seg selv ikke løser problemer eller beskytter oss mot de økte truslene all den nye teknologien fører med seg. Det kreves derimot et samspill mellom disse tre for å optimalisere både produksjon og sikkerhet i en virksomhet (Reason, 1997, s. 2; NorSIS, 2020; NSM referert i Bergsjø, Windvik & Øverlier, 2020). Schneier (referert i Nätt & Heide, 2015, s. 28) understreker viktigheten av den ikke-teknologiske delen av datasikkerhet ved å påpeke at dersom du tror at teknologi kan løse alle dine sikkerhetsutfordringer, har du verken forstått sikkerhetsutfordringene eller teknologien. Mange brukere tror de er sikre så lenge de har installert brannmurer, antivirusprogramvare og de siste oppdateringene, men faktum er at hackere og svindlere i dag fokuserer mest på å hacke *brukerne* gjennom relativt enkel teknologi og psykologi i stedet for selve systemene (Nätt & Heide, 2015).

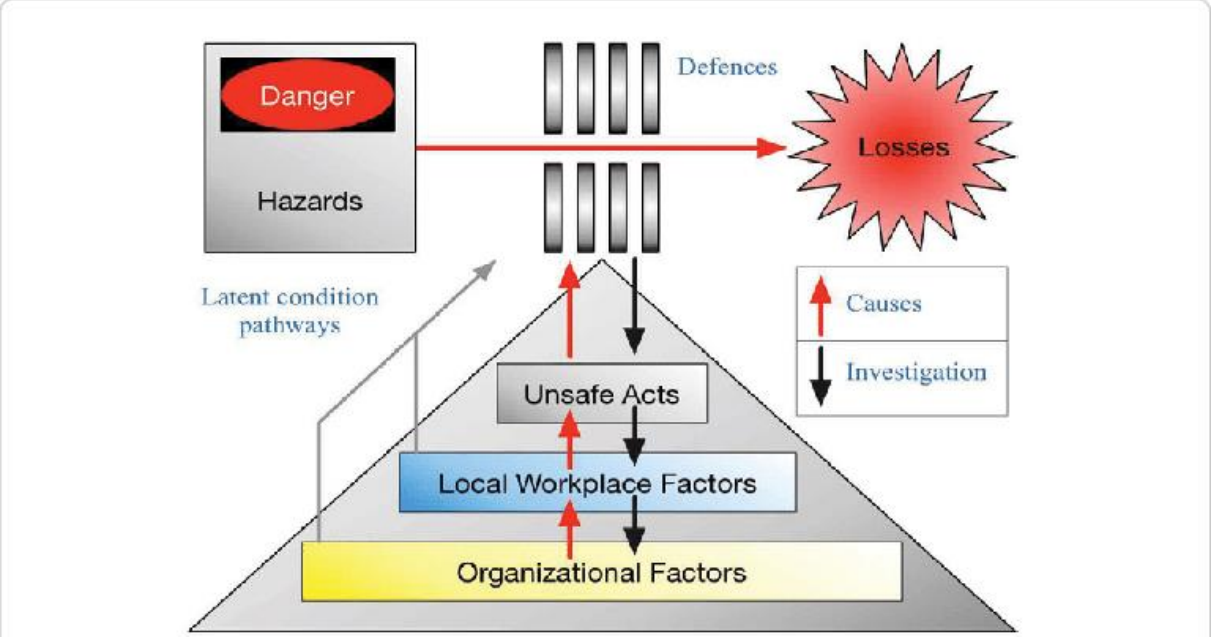
Det er altså ikke nok å ha gode teknologiske løsninger som i utgangspunktet skal fange opp trusler og angrep, når det er mennesker som bruker systemene og som til syvende og sist er de som avgjør om systemet funker eller ikke. Dette gjør at det kreves et helhetlig fokus på sikkerhet og viser at en organisasjon er nødt til å ha gode prosesser når det kommer til det å utøve god risikostyring og å utvikle en god sikkerhetskultur. Norsk senter for informasjonssikring (NorSIS) har siden 2016 gitt ut en årlig rapport hvor de har kartlagt den norske befolkningens digitale sikkerhetskultur over tid, og deres siste definisjon på digital sikkerhetskultur er følgende: «Digital sikkerhetskultur er våre felles verdier, holdninger, normer, kunnskaper og handlinger som bidrar til at vi unngår å bli rammet av digitale trusler.» (NorSIS, 2020). Bergsjø et al. (2020, s. 36) oppsummerer med å si at digital sikkerhetskultur er et sett med handlingsmønstre og et sett med ideer, normer og holdninger. Ifølge NorSIS (2020) består digital sikkerhetskultur av noen kjerneområder, herunder blant annet av holdninger til digitalisering og digital sikkerhet, tillit og risikooppfattelse, kunnskap, læring og interesse, og sikkerhetsatferd. De har også en annen modell med fem faktorer som påvirker den digitale sikkerhetskulturen, og denne vises i figur 2.1.



Figur 2.1. Fem faktorer som påvirker den digitale sikkerhetskulturen. (NorSIS, referert i Digdir, 2021).

2.4 Latente forhold som årsak til organisatoriske ulykker

Reason (1997) skriver i sin bok *Managing the Risks of Organzational Accidents* at ulykker skjer på grunn av svikt i systemet, og at menneskelige feil i hovedsak ikke skyldes individet selv, men heller forhold ved organisasjonen – et såkalt systemperspektiv. Menneskelige feilhandlinger blir dermed sett på som en konsekvens heller enn en årsak, og han påpeker derfor at det heller ikke nytter å konkludere med menneskelig svikt dersom man skal komme til bunns i årsaken til en ulykke. Han legger vekt på det han omtaler som latente forhold, hvor forhold ved organisasjonen som helhet er det som skaper ulykker. Dette er forhold som kan være til stede i mange år før de tilsynelatende overraskende kolliderer med lokale forhold ved arbeidsplassen og aktive feilhandlinger fra personell i førstelinje (Reason, 1997, s. 10). Disse latente, organisatoriske forholdene kan være strategiske beslutninger, prosedyrer og rutiner, ressursfordeling og -prioritering, kommunikasjon, trening og utstyr med mer. Hver for seg har de ikke nødvendigvis noen katastrofale effekter, men det er kombinasjonen av dem som fører til et sjeldent sammentreff av hull i de sammenhengende barrierene.



Figur 2.2. Reasons modell over organisatoriske ulykker (Reason, 1997).

For å forhindre ulykker mener derfor Reason (1997) at man er nødt til å se på de organisatoriske forholdene i en virksomhet. Når det gjelder beslutninger tatt på overordnet nivå er det ikke nødvendigvis snakk om dårlige beslutninger sett i lys av situasjonen der og da, men det faktum at ens beslutninger på et eller annet tidspunkt vil påvirke noen andre et

annet sted i systemet. Dette gjør at de latente forholdene i stor grad er basert på hva de i det øvre sjiktet av organisasjonen foretar seg, og hvor bevisste de er på de langsiktige konsekvensene av det de gjør (Reason, 1997, s. 11). Tiltakene som retter seg mot de organisatoriske forholdene er det Reason (1997, s. 8) omtaler som «myke» barrierer – en kombinasjon av tiltak innen regler og prosedyrer, trening og opplæring og med et fokus på menneskene som jobber i front. Sammen med de «harde» barrierene i form av rent tekniske tiltak, utgjør dette det totale forsvaret mot organisatoriske ulykker som skal forhindre at menneskelige feilhandlinger får et katastrofalt utfall.

2.5 Man-made disasters

Barry Turner (1978, 1997) mente at ulykker og uønskede hendelser alltid starter med små og ubetydelige beslutninger i organisasjonen. Denne teorien legger vekt på at ulykker skjer på grunn av helt vanlige og dagligdagse prosesser i en organisasjon, og at de er et resultat av samspillet mellom både sosiale, organisasjonsmessige og tekniske prosesser. Han mente at ulykker kun kunne forstås fullt ut dersom de ble plassert i den riktige sosiale konteksten de kom fra, og at kulturen var det som i bunn og grunn danner grunnlaget for en katastrofe. Han la derfor stor vekt på betydningen av organisasjonens kultur og de ansattes antakelser og oppfatninger, spesielt når det kom til risiko. Ifølge ham var nemlig det første steget i utviklingen av en katastrofe de kulturelt aksepterte oppfatningene om ulykker og hvordan de oppstår, og at disse ikke nødvendigvis stemte overens med de faktiske forholdene. Han kalte tiden frem mot en ulykke som inkubasjonstiden, hvor det viktigste momentet var at små hendelser og en kjede av skjulte feil, ikke blir forstått på en hensiktsmessig måte fordi det ikke stemmer overens med organisasjonens oppfatning om hvordan ulykker skjer. Han mente derfor at risikovurderinger er problematiske nettopp fordi risiko blir oppfattet ulikt og dermed også konstruert og tolket ulikt av ulike interessenter. De ansattes holdninger er dermed svært viktig da de kan bidra til ulykker ved å undergrave den faktiske risikoen organisasjonen står overfor.

Ifølge Turner (1978) er sikkerhetskultur det settet av antakelser og deres assosierte praksis som konstruerer oppfatninger om farer og sikkerhet. Han la også vekt på at en god sikkerhetskultur reflekterer og blir bedre av toppledelsens forpliktelse til sikkerhet, delt bekymring for farer og omsorg for deres påvirkninger, realistiske og fleksible normer og regler om farer, kontinuerlig refleksjon rundt praksis gjennom overvåkning, analyser og

tilbakemeldingssystemer, samt organisatorisk læring. Mange av utfordringene han trakk frem med ulykker og uønskede hendelser mente han skyldtes informasjons- og kommunikasjonsproblemer, blant annet gjennom manglende eller feil informasjonsformidling, for store mengder informasjon, ignorering av informasjon og informasjon som går ut til feil personer. I tillegg pekte han på at mennesket har en begrenset kapasitet til å håndtere komplekse problemer, og at vi går for det som er «godt nok», også i en organisasjon (Turner, 1978).

2.6 High Reliability Organizations (HRO)

Teorien om High Reliability Organizations er en slags motsats til de andre teoriene om ulykker. Den baserer seg nemlig på det faktum at enkelte organisasjoner har en unik evne til å *unngå* ulykker, og har derfor heller valgt å fokusere på hva som kjennetegner disse organisasjonene fremfor å se på de som opplever ulykker. Begrepet High Reliability Organizations ble utviklet av miljøet ved University of California, Berkeley på 1980-tallet, og Weick og Sutcliffe (2015) er blant de som i stor grad har vært med på å sette sitt preg på det som på norsk omtales som *høypålitelige organisasjoner*. Kjernen i deres teori er det som kalles «mindful organizing», som innebærer at de høypålitelige organisasjonene er sensitive og konstant tilpasser seg til små hint og tegn og dermed forhindrer at små uhell utvikler seg og akkumuleres med andre deler av systemet og fører til større problemer. De skaper dermed et system for persepsjoner, erfaringer og forventninger. Denne organiseringen er en konstant *meningsskapende* prosess, altså en prosess hvor man fatter hva som skjer samtidig som man handler og delvis klarer å forutsi hva som kan skje videre (Weick & Sutcliffe, 2015, s. 32).

De mener at uventede hendelser oppstår fordi vi skaper organisasjoner som konstruerer og vedtar *forventede* hendelser, og at vi dermed stort sett handler ut fra forventninger og antakelser om hvordan verden vil reagere på det vi gjør. De erkjenner at tette koblinger og kompleksitet i samspillet i systemet gjør det vanskelig å fatte hva som skjer når uventede problemer begynner å eskalere, men at denne kompleksiteten blir mer håndterbar hvis man fokuserer på prosesser som sørger for vedvarende ytelse. Dette fører til at man fanger opp problemer tidligere og når de er mindre, slik at det trengs mindre ressurser for å håndtere dem og de gjerne kan fikses helt ut før de eskalerer (Weick & Sutcliffe, 2015).

I denne teorien sammenfattes fem overordnede kognitive prinsipper som de mener gjelder for høypålitelige organisasjoner (Weick & Sutcliffe, 2015):

- Opptatt av små feil
- Motvilje mot forenkling (av årsaker)
- Sensitivitet for operasjoner
- Forpliktelse til robusthet
- Respekt for kompetanse og ekspertise

Det er disse fem prinsippene som ligger til grunn for det de kaller mindful organizing, og som sørger for en kollektiv bevissthet omkring de farene og sårbarhetene organisasjonen står overfor.

2.7 Grenseoverskridende kriser

Et digitalt angrep kan sies å være en såkalt «transboundary crisis», nettopp fordi det digitale domenet overskrider både geografiske og organisatoriske grenser. Disse krisene eller ulykkene karakteriseres ved at de skjer på tvers av ansvarsområder, undergraver funksjonen til ulike politiske sektorer og kritisk infrastruktur, og at de eskalerer hurtig (Ansell, Boin & Keller, 2010). I tillegg vil de, som enhver annen krise, kreve rask respons under stor grad av usikkerhet og stress, noe som vil bli enda mer utfordrende når kriser sprer seg på tvers av geografiske og politiske grenser (Ansell, Boin & Keller, 2010). En slik type krise kan dermed være vanskeligere både å oppdage og håndtere, og Boin (2019) påpeker at disse type hendelser har elementer i seg fra blant annet Turners (1978) teori ved at de ofte oppstår på grunn av komplekse systemer og sårbarheter i disse systemene som er vanskelige å fange opp fordi ingen egentlig har full oversikt og ulike feil bygger seg opp over tid uten at det legges merke til (Boin, 2019).

Dette viser at digitale krisehendelser kan være svært utfordrende å håndtere, noe som tydeliggjør et behov for økt fokus på dette området. Samtidig har menneskenes rolle blitt stadig viktigere fordi det meste i samfunnet blir digitalisert og man er avhengig av bevisste brukerne som bidrar i arbeidet med å forhindre digitale angrep. Det mangler imidlertid et godt teoretisk grunnlag for hvordan man bør gå frem for å skape gode holdninger og bevissthet i det digitale rommet, og mitt bidrag vil derfor være å se på hvordan tradisjonelle teorier rundt sikkerhetskultur også kan brukes for å skape en god *digital* sikkerhetskultur.

Ulike teoriers tilnærming til begrepet «sikkerhetskultur»					
	Latente forhold (Reason)	**Man-made disasters (Turner)**	**HRO (Weick & Sutcliffe)**	**Det feilbarlige menneske (Kvalnes)**	**Digital sikkerhetskultur (NorSIS/Digdir)**
Kjerneelement					
Ledelse	Forpliktelse til sikkerhet	Toppledelsens forpliktelse til sikkerhet	Forpliktelse til robusthet	Etabler kultur for feilbarlighet	Styring og kontroll
Kunnskap og kompetanse	Kompetanse, kunnskap og bevissthet		Respekt for ekspertise	Aktørkultur	Kunnskap, kompetanse, interesse
Risikoforståelse	Respekt for alt som kan bryte barrierene	Delt bekymring for farer og deres innvirkning	Motstand mot forenkling		Risikooppfattelse og holdninger til digital sikkerhet
Informasjon	Riktig informasjon	Informasjons-problemer	Sensemaking		
Læring	Læringskultur	Organisatorisk læring / kontinuerlig refleksjon	Vedvarende endring	Læringskultur	Opplæring og læring
Bevissthet		Realistiske og fleksible normer og regler for farer	Kollektiv bevissthet		Sikker atferd
Rapportering/ varsling	Rapporterings-kultur – tillit	Kommunikasjons-problemer	Opptatt av feil	Ytringskultur	Fokus på fellesskapet – stå frem ved feilhandlinger – tillit
Rettferdighet	Rettferdig kultur			Rettferdig kultur	

Tabell 2.1. Oversikt over de ulike teorienes tilnærming til begrepet «sikkerhetskultur».

3 Metodiske momenter

Vi mennesker er konstruert på en slik måte at de fleste går rundt med teorier om hvordan virkeligheten ser ut, noe som gir oss en nødvendig forutsigbarhet for å takle den kompliserte verdenen vi lever i. Gjennom slik hverdagskunnskap er det imidlertid en fare for at vi overgeneraliserer og danner oss teorier basert på selektive inntrykk og forhastede konklusjoner (Johannessen, Tufte & Christoffersen, 2016). Vitenskapelig metode handler derfor om å finne belegg for sine konklusjoner og sannsynliggjøre at antakelsene er riktige, og de viktigste kjennetegnene ved metode er systematikk, grundighet og åpenhet (Johannessen, Christoffersen & Tufte, 2011, s. 34; Johannessen et al., 2016; Jacobsen, 2015, s. 16). Samfunnsvitenskapelig metode dreier seg i sin tur om å få informasjon om den sosiale virkeligheten, og metoden gir samtidig føringer på hvordan man skal gå frem for å få denne informasjonen (Johannessen et al., 2011, s. 33; Jacobsen, 2015, s. 17 og s. 23). I tillegg sier den noe om hvordan denne informasjonen skal samles inn, analyseres og tolkes slik at den på en riktig måte forteller oss noe om de samfunnsmessige forholdene og prosessene (Johannessen et al., 2011, s. 33; Johannessen et al., 2016).

Alle forskningsprosjekt starter med en hypotese eller problemstilling, som igjen legger føringer for valg av design og metode. Min problemstilling er som følger: *«Hva kjennetegner den digitale sikkerhetskulturen i samfunnskritiske funksjoner, sett fra fagansattes perspektiv?»*

Forskningsspørsmålene mine er videre knyttet til å undersøke dette nærmere, gjennom å se på hvilken risiko virksomhetene opplever å stå overfor, hvilke holdninger de ansatte har, hvordan ledelsen påvirker kulturen og hvordan de sørger for å få bevisste ansatte. Det er flere ulike fremgangsmåter innen slike undersøkelser, og jeg vil i dette kapittelet redegjøre for de valgene jeg har tatt med tanke på design og metode, datainnsamlingsteknikk og analyse. Videre vil jeg også se på grad av validitet og pålitelighet i min egen undersøkelse, reflektere over min egen rolle som forsker og de valgene jeg har tatt, samt diskutere noe rundt etiske problemstillinger som gjør seg gjeldende i slike forskningsprosjekt.

3.1 Forskningsdesign og metode

Forskningsdesign dreier seg om å velge den beste tilnærmingen til hvordan undersøkelsen skal gjennomføres ut fra hvilken problemstilling vi har valgt (Johannessen et al., 2011, s. 77; Jacobsen, 2015, s. 21 og s. 89). Designet må altså ta utgangspunkt i hva og hvem som skal

undersøkes, hva som er formålet med undersøkelsen og hva den skal bidra med, og vi må derfor alltid spørre oss selv om det undersøkelsesopplegget vi velger er egnet til å belyse den problemstillingen vi ønsker å undersøke (Johannessen et al., 2011, s. 36; Jacobsen, 2015, s. 89). Dette er en del av den første og forberedende fasen i forskningsprosessen og forskningsdesignet man velger gir dermed føringer på hvordan de påfølgende fasene i forskningsprosessen skal gjennomføres (Johannessen et al., 2011, s. 36).

Ut fra min problemstilling ønsket jeg å gå i dybden på hvordan den digitale sikkerhetskulturen er i samfunnskritiske funksjoner. Jeg ønsket dermed å undersøke et spesifikt fenomen og få mer detaljert og nyansert informasjon om akkurat dette fenomenet slik det oppleves av de ansatte innenfor denne kategorien. Med bakgrunn i dette falt derfor valget på å gjennomføre en deskriptiv og til dels komparativ casestudie med flere caser ved at jeg undersøkte hvordan fenomenet digital sikkerhetskultur opplevdes av ansatte i tre ulike sektorer, og hvor jeg videre sammenlignet resultatene fra de ulike casene (Johannessen et al., 2016; Jacobsen, 2015; Tjora, 2012). Undersøkelsen ble til en viss grad også eksplorativ i den forstand at digital sikkerhetskultur er et relativt nytt felt hvor det ikke er gjennomført så mye tidligere forskning og det har vist seg å være et begrep med ulike fortolkninger (Johannessen et al., 2016, s. 53; Jacobsen, 2015, s. 80; Pedersen & Gaupseth, 2019). Både fordi formålet var å undersøke situasjonen her og nå, og på grunn av begrensninger i tid og omfang, ble undersøkelsen utført som en tverrsnittsundersøkelse (Johannessen et al., 2016; Jacobsen, 2015). Dette betyr at informasjonen jeg samlet inn viste tilstanden på et gitt tidspunkt, i mitt tilfelle i løpet av datainnsamlingsperioden som gikk over ca. to måneder.

Innenfor vitenskapelig metode er det i hovedsak to ulike retninger når det gjelder å samle inn data, nemlig kvantitativ og kvalitativ metode (Johannessen et al., 2016; Jacobsen, 2015). Disse kan benyttes både hver for seg og i kombinasjon, avhengig av blant annet undersøkelsens formål og tid og ressurser til rådighet. Man kan argumentere for at måling av kultur bør skje gjennom kvantitative metoder som måler utbredelse og omfang for å nå ut til flest mulig, som for eksempel en spørreundersøkelse. Dette har imidlertid vist seg å inneholde en del svakheter, blant annet på grunn av ferdigdefinerte svaralternativer og dermed mindre mulighet til å fange opp flere nyanser (Patankar og Sabin,referert i Laumann, 2011, s. 285; Bang, 2011). Jeg mente derfor at det var mest hensiktsmessig å besvare problemstillingen gjennom en kvalitativ tilnærming hvor jeg gikk for færre informanter, men samtidig gikk dypere inn i fenomenet.

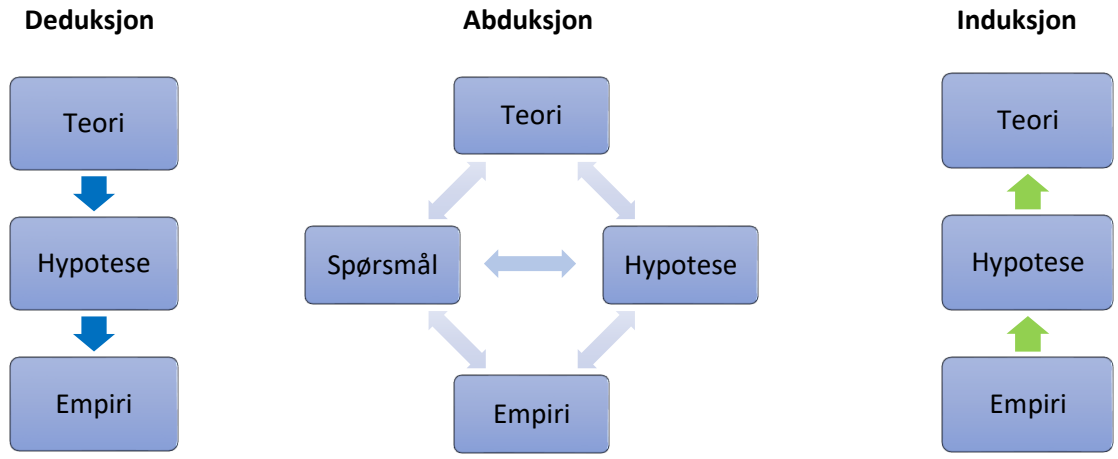
Innenfor kvalitativ metode vil det også være ulike tilnærminger når det gjelder det videre arbeidet med datainnsamling og analyse. På grunn av undersøkelsens kompleksitet vil det ofte være vanskelig å forholde seg til kun én enkelt tilnærming, og de fleste prosjekter vil derfor inneholde momenter fra flere ulike tilnærminger (Johannessen et al., 2016). Selv om jeg har valgt å studere ulike caser i min undersøkelse, benyttes disse først og fremst som rene studieobjekter fremfor å være et forskningsdesign i seg selv (Johannessen et al., 2016, s. 205). Det vil likevel være noen elementer som også kommer fra denne metoden, selv om hovedtyngden i undersøkelsen er inspirert av grounded theory. Dette valget ble gjort på bakgrunn av formålet med undersøkelsen og problemstillingens karakter, hvor jeg ønsket å undersøke hvordan virkeligheten så ut på et felt jeg ikke kjente så godt fra før og hvor målet med forskningen var å få frem en grundig beskrivelse og forståelse av fenomenet digital sikkerhetskultur (Johannessen et al., 2016, s. 181-182). Det å være inspirert av grounded theory trenger altså ikke å være ensbetydende med at man må ende opp med *produktet* grounded theory, det kan likså godt anvendes som en ren metode *uten å produsere* en ny teori (Johannessen et al., 2016, s. 182).

Det er ofte en oppfatning om at man gjennom å bruke grounded theory kun skal jobbe ut fra et empirisk perspektiv uten å ha noen som helst teoretiske antakelser før man starter datainnsamlingen. Dette er kun en sannhet med modifikasjoner da enhver forsker vil være preget av den kunnskapen og de erfaringene vedkommende sitter med fra før, og denne forforståelsen vil uansett forme datainnsamlingen på et eller annet nivå. Den sosiale virkeligheten vi lever i kan tolkes forskjellig av alle som studerer og lever i den, og derfor vil både forskeren selv og informantene ha sin egen opplevelse av det som skjer rundt en. Dette omtales gjerne som «sensitizing concepts», et begrep utviklet av den amerikanske sosiologen Blumer (1954). Det kan sies å utgjøre et slags startpunkt for kvalitative undersøkelser; enten man er det bevisst eller ikke så bringer forskeren med seg noen grunnleggende forståelser og erfaringer inn i forskningsprosessen som gjør at oppmerksomheten styres mot enkelte forhold fremfor andre (Bowen, 2006). Johannessen et al. (2016, s. 183) trekker frem det de omtaler som *teoretisk sensitivitet*, hvor både litteratur, personlige og faglige erfaringer gir en evne til å forstå og identifisere hva som er viktig og gi det en mening. Det hjelper også til med å avgrense fenomenet man ønsker å undersøke (Johannessen et al., s. 184). En forsker vil altså aldri kunne være hundre prosent objektiv verken i prosessen med å komme frem til et forskningsområde eller i datainnsamlingen og -analysen. Det viktige er derimot at man er

bevisst på dette gjennom hele forskningsprosessen og er åpen om sine erfaringer og antakelser når man legger frem resultatene.

Når jeg bestemte meg for å ha digital sikkerhet som tema for oppgaven var det på grunnlag av egne observasjoner og antakelser om at digital sikkerhet ikke alltid er så veldig høyt prioritert i ulike virksomheter, og at bevisstheten og kunnskapen rundt det til en viss grad avhenger av tilfeldigheter og interessen til enkeltpersoner. Dette ville igjen påvirke sikkerheten og hvorvidt virksomhetene lyktes i å unngå digitale krisehendelser. Etter å ha studert krisehåndtering og kriseledelse i en god del år, er jeg som tidligere nevnt også godt kjent med teorier innenfor organisatoriske ulykker, høypålitelige organisasjoner og betydningen av den menneskelige faktoren i arbeidet med sikkerhet. Disse teoriene lå derfor i bakhodet gjennom det videre arbeidet med undersøkelsen og utarbeidelsen av intervjuguiden, samtidig som feltet digital sikkerhet er noe jeg ikke kunne veldig mye om fra før og derfor måtte utforske mer.

Forskningsmetoden jeg brukte ble dermed en pragmatisk tilnærming som kombinerte både induksjon og deduksjon, en såkalt abduktiv metode som er en kontinuerlig vekselvirkning mellom teori og empiri (Jacobsen, 2015, s. 35; Tjora, 2012, s. 26). Fordelen med dette er at analysen skjer samtidig med datainnsamlingen, og at man hele tiden vurderer funnene som er gjort og utvikler nye antakelser og hypoteser som man igjen undersøker videre, helt i tråd med metoden grounded theory. Jeg hadde som sagt i utgangspunktet et sett med teorier jeg kjente til fra før, men det viste seg at jeg måtte forkaste og/eller legge til nye teorier etter hvert som jeg fikk nye data å forholde meg til. Denne prosessen passet derfor veldig bra med min fremgangsmåte da jeg var relativt åpen idet jeg startet undersøkelsen, men spisset det mer og mer underveis i prosessen.



Figur 3.1. Forskjeller mellom deduktiv, induktiv og abduktiv tilnærming. (Jacobsen, 2015, s. 35).

3.2 Datainnsamlingsteknikk og utvalg

Etter at man har utformet en problemstilling og funnet ut hvilket design og hvilken metode som passer best til undersøkelsens formål, må man se på hvordan man konkret skal samle inn dataene. Gjennom å bruke en kvalitativ datainnsamlingsmetode er hensikten altså å få fyldige beskrivelser og å komme tett innpå personer i den målgruppen vi er interessert i. Intern gyldighet er derfor veldig viktig i kvalitative undersøkelser, og valget av informanter må derfor baseres på hvem som er mest relevante og interessante ut fra formålet med undersøkelsen, og et tilfeldig utvalg er derfor lite hensiktsmessig (Johannessen et al., 2016, s. 113; Jacobsen, 2015, s. 177). I tillegg er slike kvalitative metoder både tid- og kostnadskrevende, og vi må derfor tenke nøye gjennom *hvem* vi velger ut som informanter, og *hvor mange* vi trenger, både for å sørge for å få den informasjonen vi trenger, og samtidig klare å gjennomføre det (Johannessen et al., 2016, s. 114; Jacobsen, 2015, s. 177). Kvalitative metoder samler inn og registrerer data i form av tekster, lyd og bilde, og de vanligste måtene å samle inn data på er derfor gjennom intervjuer, observasjon og gruppesamtaler (Johannessen et al., 2011, s. 37 og s. 103, Jacobsen, s. 65).

I starten av prosjektet gjennomførte jeg noen forundersøkelser i form av uformelle samtaler med kollegaer og bekjente om temaet, i tillegg til innhenting av sekundærdata gjennom aktuelle artikler, trusselvurderinger og egne erfaringer. Noen av samtalene ble gjennomført som en del av arbeidsdagen og i forbindelse med faglige diskusjoner, mens en annen samtale ble avtalt på forhånd med den hensikt å diskutere det spesifikke temaet med noen utenfor min egen etat. De jeg snakket med hadde alle en type stilling hvor det var forventet at de har en viss kjennskap til temaet, noe som også var bevisst fra min side. Ved å snakke med disse fikk jeg en viss følelse av hvordan temaet opplevdes blant de som jobber med det, og kunne samtidig utvikle problemstillingen på en måte som gjorde den mer aktualisert og forskbar. I tillegg tok jeg kontakt med Nasjonal Sikkerhetsmyndighet (NSM) som er definert som fag- og ekspertorgan innen digital sikkerhet i Norge, for å snakke med noen som har mye erfaring innen det området jeg ønsket å undersøke. Jeg fikk da gjennomført en telefonsamtale med en seniorrådgiver som ga meg gode innspill til det videre arbeidet med oppgaven.

3.2.1 Utvalgsstrategi

Da jeg selv har jobbet flere år i en beredskapsetat og fortsatt befinner meg i en samfunnskritisk virksomhet etter et jobbytte, ønsket jeg også å fokusere på nettopp samfunnskritiske etater når jeg skulle gjennomføre denne studien. DSB (DSB, 2016) har som tidligere nevnt utarbeidet en oversikt over de ulike kategoriene innenfor dette, og jeg valgte altså å undersøke tre ulike sektorer for å kunne sammenlikne svarene. De ulike informantene kunne ha en ulik oppfatning av fenomenet, og det var dette jeg ønsket å få bekreftet eller avkreftet gjennom undersøkelsen. Dette var i henhold til det Jacobsen (2015, s. 107) beskriver som fordelene med en studie som undersøker enheter fra ulike kontekster; man får belyst fenomenet fra ulike ståsteder og kan dermed få en rikere beskrivelse enn man ville fått gjennom å studere én enkelt enhet. Jeg endte derfor opp med én virksomhet innenfor justissektoren, én virksomhet innenfor kraftforsyning og to virksomheter innen finansielle tjenester.

Videre ønsket jeg å snakke med personer som hadde personlig erfaring med den digitale sikkerheten i egen etat, og som dermed var viktige for å forstå og beskrive fenomenet digital sikkerhetskultur (Johannessen et al., 2016, s. 116; Jacobsen, 2015, s. 181). Dette ville igjen gi meg bedre holdepunkter for å finne suksessfaktorer som andre virksomheter kunne dra nytte av. Denne måten å velge informanter på betegnes som en strategisk utvelgelse hvor forskeren foretar bevisste valg mellom ulike alternativer, og tenker gjennom hvilken målgruppe som må delta for at man skal få samlet inn nødvendig informasjon (Johannessen et al., 2016, s. 116). I og med at informantene jobbet i ulike virksomheter var det noen forskjeller i type stilling, ansvar og erfaring. Dette ga meg imidlertid enda mer variasjon i utvalget, noe som var utelukkende positivt med tanke på å oppnå en best mulig beskrivelse av fenomenet.

Jeg startet prosessen med å innhente informanter gjennom henvendelser til de respektive virksomhetene. For tre av virksomhetene tok jeg kontakt med noen jeg allerede kjente innenfor den aktuelle etaten, og ble på den måten ledet videre i retning av passende informanter. Bekjentskaper var også grunnen til at det ble to ulike virksomheter innenfor finans, mens det ble én virksomhet innen de andre sektorene. For den siste virksomheten tok jeg kontakt via telefon og sentralbord og fikk da navn og kontaktinformasjon til noen som kunne svare ut forespørselen min. Selv om jeg har måttet gå gjennom flere ledd for å komme frem til aktuelle informanter, gikk prosessen likevel overraskende enkelt og smertefritt. Jeg hadde forventet å måtte purre flere ganger og var også innstilt på at noen ikke ønsket å stille

opp, men jeg har kun møtt utelukkende positive personer som har vært villig til å både hjelpe meg med å finne informanter og å stille opp selv.

Problemstillingen min og tiden jeg hadde til rådighet i forbindelse med masteroppgaven var med på å legge føringer på antallet informanter. Ut fra hva jeg anså å være praktisk gjennomførbart tok jeg utgangspunkt i et antall informanter på rundt 8-10, hvor det var høvelig likt fordelt mellom de ulike etatene. Grounded theory legger imidlertid vekt på at man på forhånd ikke skal planlegge hvilke eller hvor mange informanter som skal undersøkes, fordi man ideelt sett skal fortsette helt til man ikke lenger får noen ny informasjon, det såkalte «metningspunktet» (Johannessen et al., 2016, s. 187; Jacobsen, 2015, s. 193). Jeg var derfor innstilt på å ta flere intervjuer hvis jeg så at det ble nødvendig for å få svar på problemstillingen min. Samtidig skulle jeg skrive oppgaven alene og visste at jeg ville ha begrenset kapasitet til å gjennomføre analyser av alle intervjuene i forhold til de som skulle skrive oppgaven som gruppe. Det kunne også bli aktuelt å følge opp enkelte informanter med flere intervjuer dersom det viste seg at disse satt med mye sentral informasjon, og det var derfor viktig for meg å skaffe et *relevant* utvalg av informanter fremfor veldig mange (Johannessen et al., 2016, s. 114). Ut fra disse forutsetningene tok jeg utgangspunkt i at jeg ønsket tre informanter fra hver etat, noe jeg også fikk gjennomført. Etter å ha gjennomført intervjuene av hver sektor så jeg at jeg stort sett fikk de samme svarene og den samme informasjonen, noe som gjorde at jeg ble ganske trygg på at jeg nådde det omtalte metningspunktet innenfor hver etat. Jeg gjennomførte derfor totalt ni intervjuer.

Sektor	**Stilling/område**	**Pseudonym**	**Erfaring** (antall år)
Finans			
	Fagleder krisehåndtering	Stian	10+
	Avdelingsleder riskostyring tredjepartsforhold	Thomas	5+
	Spesialrådgiver strategisk sikkerhet	Trine	15+
Kraft			
	IKT-sikkerhetskoordinator	Camilla	5+
	Leder IKT-sikkerhet	Mads	10+
	Beredskapskoordinator	Steinar	15+
Justis			
	Sikkerhetsrådgiver IKT-sikkerhet	Knut	15+
	Sikkerhetsanalytiker	Lars	10+
	Seniorinformasjonssikkerhetsrådgiver	Daniel	5+

Tabell 3.1. Beskrivelse av informantene og deres sektortilhørighet.

3.2.2 Intervju

Grounded theory trekker frem intervju som en godt egnet datainnsamlingsteknikk, og jeg anså også dette for å være den beste fremgangsmåten ut fra både problemstillingen min og omstendighetene for øvrig. Jeg ønsket å få fyldige og detaljerte beskrivelser, og gjennom et individuelt intervju/dybdeintervju hadde jeg mulighet til å gi informantene stor frihet til å uttrykke seg og på den måten også bedre kunne innhente deres erfaringer og opplevelser (Johannessen et al., 2016, s. 145; Jacobsen, 2015; s. 146; Tjora, 2012, s. 105).

I og med at jeg ønsket å sammenlikne dataene fra ulike sektorer var det hensiktsmessig å ha en viss grad av standardisering slik at alle som et utgangspunkt ble stilt de samme spørsmålene. Dette kan betegnes som strukturerte intervju og er et av ytterpunktene innenfor intervjudelen (Johannessen et al., 2011, s. 145-146). Jeg ønsket likevel ikke å ha faste svaralternativer de skulle krysse av fordi jeg ville at de selv skulle formidle svarene med egne ord, og ikke på forhånd putte svarene i en «bås». På grunn av dette ble intervjuene mine mer en mellomting mellom helt strukturerte og semistrukturerte intervju, rett og slett fordi jeg ønsket at empirien skulle få sin plass i datainnsamlingen (Johannessen et al., 2016, s. 148). Dette er som tidligere nevnt også fremgangsmåten for en abduktiv metode hvor empiri og teori jobber vekselvis om hverandre (Jacobsen, 2015, s. 35; Tjora, 2012, s. 26).

Jeg utarbeidet derfor en intervjuguide med overordnede tema jeg skulle innom, og noen definerte spørsmål inn under hvert tema som både kunne fungere som en støtte og som alle informantene i utgangspunktet burde svare på (Vedlegg 3). Temaene jeg satte opp var basert på min tidligere kunnskap og erfaring på området, og dreide seg dermed både om forhold innen organisasjonskultur, sikkerhetskultur og sikkerhetsstyring, da jeg anså dette for å være sentrale faktorer ut fra problemstillingen. Jeg gikk i utgangspunktet ganske bredt ut, og det ble derfor etter hvert klart at noen tema likevel ikke var så relevante for oppgaven som jeg hadde tenkt. Jeg valgte derfor å utelate noen oppfølgingsspørsmål videre i intervjuprosessen. Selv om man i komparative studier i utgangspunktet bør følge en ganske strukturert og ferdig utarbeidet intervjuguide, mener jeg likevel at man bør gjøre tilpasninger underveis dersom man anser det til å være det beste for oppgaven. Det er imidlertid viktig å være bevisst på hva man har utelatt for å sikre validiteten og påliteligheten i studien, og det viktigste var at alle informantene hadde svart på de spørsmålene som faktisk var relevante slik at sammenlikningsgrunnlaget fortsatt var til stede. Informantene var derfor alle innom samme temaer, men jeg kuttet litt ned på antall oppfølgingsspørsmål når det kom til fysisk organisering og systemutvikling. Dette gjorde i sin tur at jeg kunne gå mer i dybden på de

gjenværende temaene, noe som spisset fokuset og i mine øyne førte til en bedre oppgave til syvende og sist.

For å forsikre meg om at jeg traff riktig tenkte jeg også at det kunne være en fordel å teste intervjuguiden på noen andre i forkant av intervjuene, for å se om andre hadde noen saklige synspunkter med tanke på spørsmålsstilling og hvilken informasjon jeg faktisk endte opp med å få. Det er lett å se seg blind på eget arbeid, spesielt i slike intervjusituasjoner hvor en selv sitter med en klar formening om hvilken informasjon som bør komme ut fra spørsmålene. For andre er det likevel ikke sikkert at det er like krystallklart, og for å ikke bomme helt var det greit at noen andre gikk gjennom og så på det før selve intervjuene. Jeg fikk en bekjent av meg som jobber innen cybersikkerhet til å se gjennom intervjuguiden og komme med innspill. Vedkommende hadde imidlertid ingen store innvendinger mot verken tema eller spørsmål, noe som ga meg en viss trygghet i at intervjuguiden også ville fungere på informantene.

Jeg hadde i utgangspunktet et ønske om å gjennomføre intervjuene ansikt til ansikt, men på grunn av både Covid-19 og det faktum at jeg var hjemme i foreldrepermisjon gjorde at alle bortsett fra ett intervju ble gjennomført digitalt via videokonferanse på Teams. Dette gjorde at jeg fikk bevart de fleste fordelene ved å snakke med folk ansikt til ansikt, blant annet dette med ikke-verbal kommunikasjon som er en stor del av kommunikasjonen vår og kan ha betydning for hvordan man tolker informasjonen man får. Jeg følte derfor at jeg i stor grad klarte å plukke opp nyanser i det informantene fortalte på grunn av ansiktsuttrykk og mimikk, enn det jeg for eksempel ville fått til ved å ta intervjuene kun over telefon (Tjora, 2012, s. 140). Det å gjennomføre intervjuene på denne måten ga imidlertid også noen utfordringer med dårligere lyd og innimellom litt uklar tale. Det ble i tillegg en mer upersonlig arena, noe som jeg også merket selv ved at jeg ikke fikk til den samme relasjonsbyggingen i starten av intervjuet som det jeg kanskje hadde fått ved å ha sittet i samme rom og hatt en mer uformell og bedre kontaktetablering. Jeg har imidlertid mye erfaring fra lignende situasjoner gjennom jobben min, og tenkte på forhånd at denne erfaringen ville komme godt med i intervjusituasjonen. Det gjorde den også ved at jeg følte meg komfortabel i settingen og kunne ha en avslappet tone med informantene, til tross for de utfordringene som gjorde seg gjeldende ved å ta det digitalt.

Før intervjuene startet valgte jeg å forklare informantene litt om hvordan intervjuet kom til å foregå. Jeg hadde på forhånd sendt ut et informasjonsskriv og samtykkeskjema, men vet av erfaring at folk ikke alltid tar seg tid til å lese gjennom slike papirer. Jeg syntes derfor

det var viktig å sørge for en god gjennomgang av dette når jeg snakket med informantene ansikt til ansikt. Dette gjorde jeg for å forsikre meg om at de hadde forstått det de skrev under på, og var innforstått med hvordan opplysningene ville bli behandlet. Jeg tok også alle intervjuene på lyd, noe jeg valgte å få muntlig samtykke til i tillegg til at de hadde signert på samtykkeskjemaet. Jeg tok lydopptak i hovedsak for å kunne konsentrere meg mer om det informantene fortalte i stedet for å ta så mange notater. På den måten kunne jeg være mer «til stede» i intervjuet og i bedre stand til å fange opp nøkkelinformasjon som burde følges opp videre. Lydopptak kan imidlertid virke litt avskrekkende for mange og kan resultere i at mange kvier seg for å snakke like fritt, kanskje fordi alt man sier blir «fanget» opp og man ikke kan gå tilbake på noe man har sagt i like stor grad. Derfor var det viktig at jeg som forsker forklarte godt hvorfor jeg ønsket å ta opp intervjuet på lyd og hvordan jeg kom til å bruke det videre. Jeg fokuserte også på at jeg tok det opp for min egen del, og ikke for å «henge ut» informantene. Ingen av informantene hadde noen innvendinger mot dette, og jeg ble kun møtt av forståelse for mye materiale som måtte bearbeides i ettertid.

Spørsmålsstillingen i intervjuet kan sees på som en trakt, hvor åpne spørsmål stilles først og er viktig for å få informanten til å fortelle mest mulig fritt. Det var derfor viktig at spørsmålene ble stilt på en måte som gjorde at informantene ikke på forhånd skjønte hva jeg var ute etter, for å unngå at svarene deres ble påvirket av det. Deretter vil oppfølgingsspørsmål være avgjørende for å være sikker på at jeg får mer utdypende informasjon og flere detaljer (Tjora, 2012). Jeg så imidlertid at enkelte av informantene etter et par spørsmål om samme tema skjønte hvor jeg ville, og kanskje dermed også endret svarene sine litt i «riktig» retning. Det var likevel ikke noe jeg følte hindret dem i å gi ærlige svar, så alt i alt tror jeg de fleste svarte ut fra eget ståsted. Det var imidlertid viktig å være bevisst på at spørsmålsstillingen kan ha påvirket svarene de ga, så det ble tatt i betraktning når jeg skulle analysere dataene.

Jeg oppdaget underveis i intervjuene at jeg til tider ble mer låst til intervjuguiden enn jeg kanskje hadde håpet på. Dette kan nok ha sammenheng med det faktum at jeg skulle ha en komparativ studie hvor jeg skulle sammenligne svarene informantene kom med og dermed ble opptatt av at alle skulle innom de samme spørsmålene. Samtidig forsøkte jeg å spille videre på det informantene fortalte slik at jeg gikk mer i dybden på det de snakket om og ikke bare rørte i overflaten for å komme gjennom det jeg hadde satt opp på forhånd. Noen informanter snakket følgelig mer om enkelte tema enn om andre, men jeg rakk likevel å være

innom alle temaene med alle informantene også ble det litt opp til hver enkelt hvor mye de snakket om hvert tema.

En annen erfaring jeg gjorde meg under intervjuene var utfordringen med å snakke med fagpersoner på et område som jeg selv ikke kunne altfor mye om, samt at de var fra andre etater enn det jeg selv kjenner til. Det resulterte i at de brukte noen ord og begreper som var ukjent for meg og som kunne gjøre det vanskelig å forstå fullt ut hva de mente. Jeg måtte derfor veie opp for dette med å stille ekstra spørsmål for å unngå misforståelser. Dette tok også ekstra tid og fokus, noe som kan ha vært negativt for gjennomføringen av intervjuet. I tillegg er det viktig å ta i betraktning det faktum at også informantene tolker spørsmålene ulikt, både ut fra egen erfaring, type stilling og kunnskap om feltet. Dette var nok også med på å forme svarene de ga, men dette ser jeg mest på som en berikelse i form av at jeg da fikk større bredde og variasjon av meninger og opplevelser. I og med at jeg var ute etter å få svar på hvordan informantene opplevde den digitale sikkerhetskulturen i egen virksomhet, ville det ikke nødvendigvis ha gjort oppgaven noe bedre at alle svarte det samme. Det er jo også fordelen med en kvalitativ studie – det finnes ingen «riktige» svar.

Jeg synes jeg det var viktig å avslutte på en god måte, og jeg valgte derfor å runde av med å spørre informanten om han eller hun hadde noe mer de ønsket å tilføye eller mente var viktig å få med. På denne måten åpnet jeg opp for informasjon som kunne være viktig og sentral, men som ikke hadde blitt dekket av spørsmålene mine gjennom intervjuet, og det var en mulighet for informantene til å føle at deres bidrag var viktig selv om det gikk utenom intervjuguiden min. Dette kunne også ha vært en fin måte å revidere intervjuguiden på, men ingen av informantene hadde noe å tilføye. Det kan på den ene siden skyldes at intervjuguiden var relativt vid og dekket mye av det de selv tenkte på når det kom til temaet digital sikkerhet, men det kan også skyldes tidsbruken og at de fleste ikke hadde satt av mer enn 1-1 ½ time og dermed hadde andre arbeidsoppgaver som ventet. Videre avsluttet jeg med å spørre om det var greit om jeg kontaktet dem på et senere tidspunkt hvis det ble aktuelt slik at jeg hadde mulighet til å komme tilbake til dem dersom jeg hadde flere spørsmål. Dette ble imidlertid ikke nødvendig.

3.3 Behandling av data

Informantene i min undersøkelse måtte på forhånd samtykke til å delta på intervjuene, og jeg ga dem som tidligere nevnt et informasjonsskriv før intervjuet og gjennomgikk hovedtrekkene

av dette i starten av intervjuet for å forsikre meg om at de visste hva de deltok på og hvordan informasjonen ville bli behandlet. Jeg opplyste også om at samtykket når som helst kunne trekkes tilbake, og at opplysningene ble behandlet konfidensielt og i henhold til krav om taushetsplikt. Jeg innhentet ikke veldig mange personopplysninger, men i og med at informantene ble valgt ut fra sin stilling kunne de i ytterste konsekvens identifiseres gjennom dette. Opplysningene ble også lagret elektronisk i form av transkriberte intervjuer og lydopptak. Jeg meldte derfor prosjektet til Norsk senter for forskningsdata (NSD) for å ivareta kravene i personopplysningsloven (Johannessen et al., 2011, s. 99), og prosjektet ble godkjent i vedtak datert 11.09.20 (Vedlegg 2). All data vil bli slettet når arbeidet med masteroppgaven er sluttført.

Jeg valgte også å omtale informantene med pseudonymer, og alt dette ivaretok deres rett til selvbestemmelse og autonomi, samt krav om anonymitet og taushetsbelagte opplysninger (Johannessen et al., 2011, s. 95 og s. 100). Jeg valgte videre å kun vise til hvilken sektor de respektive informantene tilhører, men ikke navngi virksomhet eller spesifikk stillingsbeskrivelse. Dette gjorde jeg for å legge et best mulig grunnlag for å få så ærlige svar som mulig. Nielsen og Repstad (2006, s. 268) påpeker at forskeren ikke må love mer anonymitet enn vedkommende kan holde, og at man må veie hensynet til anonymiteten opp mot hensynet til presisjon og leservennlighet (Nielsen & Repstad, 2006, s. 269). Det er lett å love for mye anonymitet for å få informantene til å fortelle enda mer, og i og med at jeg selv trodde at enkelte av etatene jeg studerte kunne risikere å komme dårlig ut med tanke på resultatene, var det også viktig å tenke på at informantene ikke følte at de ble lurt til å fortelle mer enn de egentlig hadde lyst til. Flere informanter spurte spesifikt om hvor anonymisert de ble, noe som kan tyde på at de ikke hadde lyst til å fortelle alt dersom jeg kom til å navngi for eksempel hvilken virksomhet de jobbet i. Jeg følte imidlertid ikke at det var noe problem å anonymisere informantene så mye som jeg har gjort, verken med tanke på presisjon eller leservennlighet. Det var derfor ikke noe problem å holde det jeg lovet med tanke på anonymiseringen, og det virket også som om informantene ble beroliget når jeg sa at jeg kun kom til å vise til hvilken sektor de tilhørte.

I løpet av forundersøkelsene mine var det ikke gitt at informasjonen skulle bli tatt med i studien, og jeg innhentet derfor ikke noe samtykke fra de jeg har snakket med. De kan imidlertid heller ikke identifiseres, og det er dermed ingen fare for at noen skal vite at de har kommet med denne informasjonen. Intervjuene ble slik jeg ser det utført på en respektfull måte slik at informantene ikke følte de ble presset til å fortelle ting de egentlig ikke ville eller

satt igjen med en følelse av å ha gitt for mye informasjon. Dette handler om å ivareta etiske hensyn slik at man som forsker heller ikke ødelegger for andre forskere ved senere anledninger ved at folk kvier seg for å delta.

3.4 Gjennomføringen av dataanalysen

Analyse av kvalitative data dreier seg om å bearbeide tekst, og det viktigste med kvalitative data er at de må fortolkes. Dette bør gjøres av samme person som har samlet dem inn fordi forskerens forforståelse, hypoteser og teori er viktige utgangspunkter for dataanalysen (Johannessen et al., 2016, s. 29 og s.161). Dataanalysen har ifølge Johannessen et al. (2016, s. 162) to hovedhensikter, nemlig å organisere data etter tema, samt å analysere og tolke dataene. Samtidig er det viktig å huske på at analyse og tolkning ikke er nøyaktig det samme, og den største forskjellen er at analyse i stor grad dreier seg om å finne et mønster i datamaterialet, mens tolkning i tillegg betyr å forstå og forklare funnene slik at man finner en mening bak all informasjonen (Johannessen et al., 2011, s. 186). Jeg vil i de kommende punktene forklare mer inngående om hvordan jeg gjennomførte denne prosessen.

3.4.1 Transkribering og gjennomgang av intervjuene

I og med at jeg gjennomførte intervjuer med lydopptak, måtte alt dette materialet skrives om til ren tekst, såkalt transkribering. Et omfang på ni intervjuer gjorde dette til en krevende oppgave som tok relativt mye tid, spesielt siden alt ble transkribert ordrett fra alle intervjuene. Jeg fikk stort sett transkribert hvert intervju før jeg startet på neste, og siden jeg jobbet etter en abduktiv metode gjennomførte jeg også en viss grad av analyse etter hvert intervju for å utbedre og spisse intervjuguiden videre.

Lydopptakene ble som tidligere nevnt i hovedsak tatt for min egen del i det videre arbeidet med oppgaven ved at de fungerte som en ekstra buffer slik at jeg var sikker på at jeg ikke gikk glipp av viktig informasjon underveis i intervjuet. Det at jeg tok intervjuene på lyd gjorde også at det egentlig ikke ble så viktig å utføre transkriberingen rett etterpå med tanke på hukommelsen og informasjon som ble glemt. Jeg satt uansett og skrev mens jeg hørte gjennom opptaket, så all informasjonen kom med. Det som imidlertid var fordelen med å gjøre det relativt raskt etterpå var den følelsen jeg satt igjen med etter intervjuet, som igjen kunne påvirke hvordan jeg fanget opp noe av den ikke-verbale kommunikasjonen. Jeg ble

veldig bevisst på dette, og noterte meg ned punkter etter hvert intervju som jeg mente var viktig å være bevisst på både opp mot tolkningen av informasjonen og for gjennomføringen av de fremtidige intervjuene (Jacobsen, 2015, s. 200). Dette dreide seg blant annet om vedkommendes ansvarsområde og derav kjennskap til de ulike temaene, samt det generelle inntrykket jeg satt igjen med.

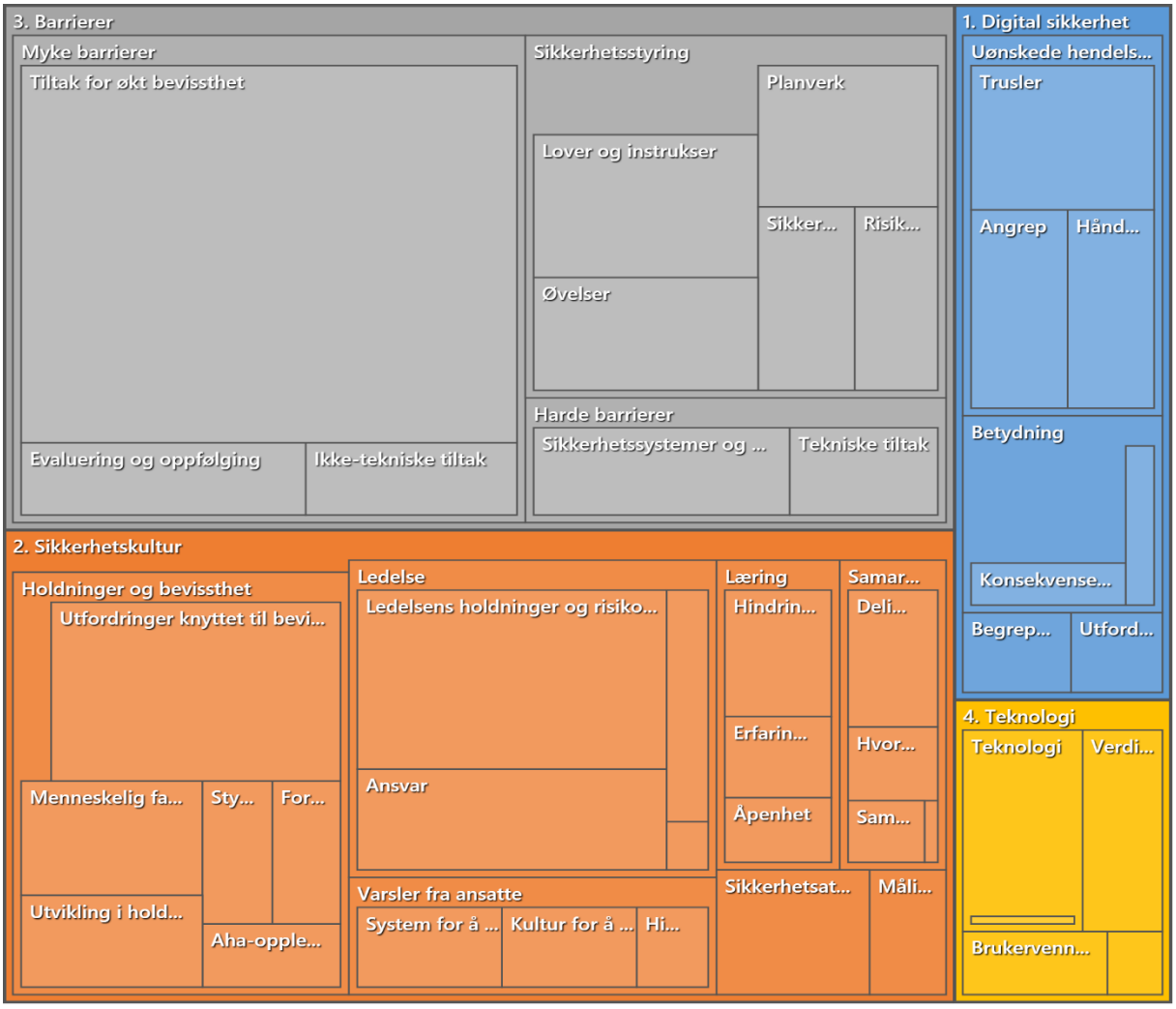
3.4.2 Koding og kategorisering

Kodingsprosessen er en omfattende del av analysen, og er den prosessen der data brytes ned, konseptualiseres, kategoriseres og bygges opp til en beskrivelse eller ren teori (Johannessen et al., 2016, s. 187). Innenfor grounded theory legges det stor vekt på denne fasen, og det er rett og slett en prosess for å bryte ned og organisere datamaterialet slik at det blir lettere å analysere det (Johannessen et al., 2016, s. 187). Den første fasen omtales som åpen koding, hvor man undersøker og sammenlikner ulike fenomener for å avdekke likheter og ulikheter. Kodene kan både være beskrivende, komme fra litteraturen og direkte fra teksten, og danner videre grunnlaget for kategoriseringen hvor beslektede data plasseres i samme kategori (Johannessen et al., 2016, s. 191).

I og med at jeg analyserte dataene underveis, ble også intervjuguiden og intervjuene mer spisset etter hvert og noen tema fikk større fokus. I starten ble kodene relativt tekstnære, det vil si at de ble hentet direkte fra teksten og det som informantene fortalte. Det ble etter hvert også klarere for meg hvilke koder som hørte sammen og som dermed kunne plasseres i samme kategori, og dette gjorde det enklere for meg å avdekke mønstre og se sammenhenger (Johannessen et al., 2016, s. 188). Etter hvert som jeg jobbet med datamaterialet ble det imidlertid klart at noen av kodene måtte revideres og endres, dels fordi jeg oppfattet sammenhenger jeg ikke hadde oppdaget fra starten av, og dels fordi jeg også begynte å lese meg opp på mer teori knyttet til de ulike funnene. Etter hvert som jeg gikk fra åpen koding mot mer selektiv koding, ble dermed kodene og kategoriene i økende grad knyttet opp mot teorien for digital sikkerhetskultur, og reflekterte på denne måten i større grad teoretiske begreper og sammenhenger – i tråd med grounded theory (Johannessen et al., 2016, s. 191; Tjora, 2012, s. 186).

I denne kode- og kategoriseringsprosessen benyttet jeg meg av programmet NVivo. Dette er et program laget for analyse av kvalitative data, og blir brukt for å bidra til å lette arbeidet i denne prosessen. Programmet var enkelt å bruke, og selv om dette arbeidet var

relativt tidkrevende synes jeg likevel det var givende og interessant å holde på med. Dette var mye fordi det både ga meg muligheten til å endelig få en struktur på all informasjonen, samtidig som jeg fikk gå grundig gjennom informantenes uttalelser og dermed også fikk et mye bedre inntrykk av hvordan oppgaven sakte, men sikkert drev fremover og hvilken retning den tok. Til slutt endte jeg opp med 4 hovedkategorier og 19 underkategorier (på første nivå). Figur 3.2 viser en oversikt over alt det kodede materialet:



Figur 3.2. Oversikt over hoved- og underkategorier i datamaterialet. Hentet fra NVivo.

Tabell 3.2 viser en oversikt over antall referanser og koder knyttet til hver enkelt informant. Tabellen gir kun et overordnet blikk på hvor mange koder (omtalt som Nodes i NVivo) hver informant er knyttet til, samt hvor mange referanser det er knyttet til hver og en av dem totalt sett. Variasjonen i antall referanser og koder er kun et resultat av at større/mindre deler av

teksten ble kodet inn, og ikke nødvendigvis et uttrykk for hvor mye informasjon de kom med eller hvor mye som er brukt i oppgaven.

Informant	Antall koder	Antall referanser
Stian	40	64
Thomas	51	94
Trine	36	71
Camilla	64	160
Mads	48	107
Steinar	42	128
Knut	38	56
Lars	44	76
Daniel	40	72

Tabell 3.2. Oversikt over antall koder og referanser tilhørende hver enkelt informant. Hentet fra NVivo.

3.4.3 Sammenlikning og søk etter litteratur

I siste fase innen grounded theory skal man sammenlikne funnene med eksisterende litteratur og teori (Johannessen et al., 2016, s. 196). I og med at jeg jobbet ut fra en abduktiv metode leste jeg meg riktignok opp på aktuell teori etter hvert som jeg oppdaget nye funn, og dette gjorde at jeg underveis fikk ny kunnskap som førte til en endring i kodene og kategoriene. Intervjuguiden var som tidligere nevnt relativt vid idet jeg startet med intervjuene, men gjennom hele denne kode- og analyseprosessen ble den spisset mer og mer. Dette gjorde også at problemstillingen ble endret opptil flere ganger, og den endelige problemstillingen og forskningsspørsmålene ble ikke utarbeidet før alt datamaterialet var gjennomgått og analysert. Datamaterialet ble altså kodet om flere ganger, men til slutt hadde alt materialet fått sin plass i systemet. Da så jeg at veldig mye av funnene dreide seg om det jeg til slutt valgte å omtale som *digital sikkerhetskultur*.

På bakgrunn av min erfaring og utdanning innen krisehåndtering og -ledelse i flere år hadde jeg som sagt allerede kjennskap til en del teorier som jeg visste var aktuelle for undersøkelsen ut fra et tradisjonelt sikkerhetsperspektiv. Jeg startet imidlertid med å ta utgangspunkt i andre teorier enn de jeg endte opp med til slutt, fordi jeg underveis i datainnsamlingen og analysen så at de teoriene jeg startet med ikke var hensiktsmessige å bruke videre. I tillegg måtte jeg finne ny forskning som var gjort på området, og jeg søkte

derfor etter relevant litteratur i ulike databaser. Jeg brukte i hovedsak Google Scholar, Oria, Sage, Science Direct og Wiley Online Library. Søkeordene var i all hovedsak knyttet opp mot digital sikkerhetskultur, cyber security culture, information security culture, cyber security awareness. og risk awareness. I tillegg benyttet jeg artikler jeg allerede hadde lest i forbindelse med emnet «Digital beredskap» ved Nord Universitet, og jobbet videre ut fra disse ved å se på referanselistene i de respektive artiklene for å finne nye relevante artikler.

De funnene som jeg ikke prioriterte å ta med videre ble fortsatt liggende i den endelige versjonen for å ha en viss oversikt over det samlede materialet. Kodingsprosessen ble derfor ganske omfattende og tok mye tid, men samtidig følte jeg at jeg fikk bearbeidet dataene veldig bra, og sitter derfor igjen med en følelse av at de funnene jeg kom frem til faktisk representerer virkeligheten.

3.5 Validitet og pålitelighet

Kvalitativ forskning skiller seg fra kvantitativ forskning og er underlagt noen andre kvalitetskriterier, og det opereres derfor også ofte med andre begreper. Reliabilitet knytter seg til undersøkelsens data og hvordan de samles inn og bearbeides, men innenfor kvalitativ forskning benyttes heller begrepet pålitelighet. Dette fordi det vil være umulig for andre forskere å duplisere en kvalitativ forskers forskning på grunn av forskerens egen erfaring og subjektive tolkning av dataene (Johannessen et al., 2016, s. 231). For å ivareta kravet om pålitelighet i min studie har jeg forsøkt å gi en detaljert beskrivelse av fremgangsmåten under hele forskningsprosessen; jeg har beskrevet hvilken metode jeg har benyttet i datainnsamlingen, intervjuene og analysen og dermed hvordan datareduksjonen har foregått og hvordan jeg har kommet frem til de kategoriene jeg har fått etter analysen, slik at andre lett kan se hvordan jeg har kommet frem til de svarene jeg legger frem i denne masteroppgaven. Dette vil også være med på å sikre best mulig bekreftbarhet, altså en kvalitativ objektivitet (Johannessen et al., 2016, s. 234).

Videre må jeg som forsker tilstrebe mest mulig validitet eller gyldighet, det vil si at mine fremgangsmåter og funn faktisk reflekterer hensikten med studien og representerer virkeligheten (Johannessen et al., 2016, s. 232; Tjora, 2012, s. 206). Det skilles mellom intern og ekstern gyldighet, og intern gyldighet styrkes gjennom å blant annet ta utgangspunkt i flere settinger. En slik kvalitativ tilnærming som jeg valgte la til rette for det Jacobsen (2015, s. 90) omtaler som intensive opplegg, hvor man studerer relativt få enheter, men mange nyanser. Et

slikt undersøkelsesopplegg vil ha høy intern gyldighet i den forstand at undersøkelsen vil være veldig virkelighetsnær, og hvor de som blir undersøkt vil oppleve undersøkelsen som relevant og kjenne seg igjen i beskrivelsen som blir gitt av virkeligheten. Dette sørger igjen for høy ekstern validitet og gjør et slikt opplegg godt egnet for videre teoretisk generalisering og overførbarhet, noe som ville være en bra kvalitet for prosjektet i sin helhet (Jacobsen, 2015; Johannessen et al., 2016, s. 233). Noe av målet mitt med studien var som tidligere nevnt å kunne overføre kunnskapen til andre etater og sektorer, og det var derfor viktig at jeg lyktes i å etablere begreper, fortolkninger og forklaringer som er nyttige på andre områder enn akkurat det jeg har studert. Dette ligger nært opptil det Tjora (2012, s. 215) omtaler som konseptuell generalisering, hvor man i tillegg til dette benytter tidligere forskning og teori som støtter opp under en større gyldighet og generaliserbarhet. Gjennom å foreta en komparativ analyse og sammenlikne flere ulike etater håper jeg å i større grad kunne trekke slutninger som gjelder på tvers av samfunnssektorer og etater. I tillegg vil jeg i drøftingskapittelet trekke funnene opp mot aktuell teori og nyere forskning, noe som gjør at jeg fanger opp sentrale trekk som kan være gjeldende også for andre utenom de aktuelle casene jeg har undersøkt (Tjora, 2012, s. 215).

Jeg måtte likevel være bevisst på en del feilkilder som kunne komme som følge av at intervjuer var hovedkilden til informasjon. Jeg som forsker ville, bevisst eller ubevisst, påvirke informantene i en eller annen grad og dette kunne føre til at de ga et svar som de trodde ble forventet av meg, den såkalte «intervjueffekten» (Johannessen et al., 2011, s. 245). Det kunne også hende at jeg la frem tema eller spørsmål på en måte som gjorde at de skjønte hvilke svar jeg var ute etter og dermed ikke ga et helt ærlig svar. Gjennom mine uformelle samtaler med kollegaer og andre bekjente merket jeg at jeg var litt forutinntatt og søkte etter informasjon som bekreftet mine egne hypoteser, en såkalt kognitiv skjevhet (Johannessen et al., 2011, s. 246, Nielsen & Repstad, 2006, s. 257). Det var dermed svært viktig at jeg var bevisst på dette når jeg utformet intervjuguiden og gjennomførte intervjuene, og evnet å være min egen «djevelens advokat» når det kom til å være kritisk overfor egen spørsmålsstilling og jakte etter både det som bekreftet og avkreftet hypotesene mine. Jeg var altså bevisst på det når jeg startet gjennomføringen av intervjuene, men jeg fikk også svar som gjorde at jeg rett og slett måtte revurdere mine egne hypoteser fordi jeg fikk informasjon som tilsa at de kanskje ikke stemte så godt likevel. Dette tror jeg gjorde at jeg klarte å være mer objektiv enn hvis jeg kun hadde fått informasjon som faktisk bekreftet hypotesene mine fra start av. Når det gjaldt utvelgelse av informanter møtte jeg som sagt utelukkende positiv respons, og jeg

føler jeg fikk snakket med personer som i aller høyeste grad var relevante og som belyste problemstillingen min på en god måte. Jeg mener derfor at jeg kan utelukke det Johannessen et al. (2011, s. 245-246) omtaler som frafallsskjevhet og dermed også klassifiseringsskjevhet.

Det finnes teknikker for å øke sannsynligheten for at studien blir mest mulig troverdig, men det er begrenset hva jeg i min masteroppgave hadde tid og ressurser til å gjennomføre. En teknikk som imidlertid var gjennomførbar for min del var å formidle resultatene av undersøkelsen min til informantene for på den måten å få bekreftet resultatet (Johannessen et al., 2011, s. 247). Jeg sendte ut resultatkapittelet til informantene for korrektur og sitatsjekk, og det var kun én av dem som ønsket å få omformulert et sitat. Dette ble gjort uten å endre på selve meningsinnholdet, i samarbeid med informanten selv.

3.6 Refleksjon over egen rolle som forsker

Det spesielle med samfunnsvitenskap er at forskeren selv er deltaker i det samfunnet han eller hun skal studere, noe som kan påvirke forskningen og resultatene (Johannessen et al., 2011, s. 35). Som jeg nevnte tidligere i kapittelet vil jeg som forsker uansett fremgangsmåte ha med meg en forforståelse inn i studien som vil være med å avgjøre hvilken mening jeg finner i teksten eller handlingen jeg studerer. Derfor er det viktig at jeg som forsker forsøker å se mitt eget fortolkningsmønster og skjønner at egne erfaringer og opplevelser vil kunne påvirke *hva* jeg observerer og *hvordan* disse observasjonene tolkes og vektlegges (Johannessen et al., 2011, s. 87; Johannessen et al., 2016, s. 35). Som nevnt under forrige punkt var det viktig å være bevisst på hvilke antakelser jeg hadde på forhånd, spesielt knyttet til egne erfaringer på området. Det at jeg hadde dårlige erfaringer med digital sikkerhet i egen etat, gjorde at det kunne være lett å ta med seg dette inn i studien og la det påvirke hvordan jeg tolket dataene jeg fikk. Jeg var imidlertid veldig bevisst på dette, og gjennom en lang og omstendelig kodingsprosess følte jeg likevel at jeg fikk god kontroll på hvordan jeg tolket de ulike dataene og hvorfor de ble vektlagt slik de ble.

I tillegg forsket jeg på egen sektor som en av tre caser, og dette kunne skape ekstra utfordringer som det var viktig at jeg som forsker var klar over. Nielsen og Repstad (2006, s. 248-253) påpeker at det både er fordeler og ulemper ved å studere egen organisasjon, og noen av fordelene er selvfølgelig at man kjenner organisasjonen godt og kan hverdagsspråket, i tillegg til at man gjerne har et personlig engasjement og ønske om å endre organisasjonen til det bedre. For min del ble dette gjeldende fordi jeg hadde noen til dels dårlige erfaringer med

feltet, og så både behovet og nytten av å styrke arbeidet på området for å bli bedre og mer robust når det kommer til digital sikkerhet. Resultatene av studien kunne dermed også vise seg å være dårlige for sektoren, noe som kunne føre til at jeg risikerte å ende i en situasjon hvor jeg måtte vurdere hvorvidt jeg skulle skrive om det eller la være, noe som igjen kunne resultere i en ugunstig filtreringsprosess (Nielsen & Repstad, 2006, s. 255). Jeg valgte imidlertid å fokusere på at funn som eventuelt viste et forbedringspotensiale var viktige å få frem, nettopp fordi ønsket mitt med oppgaven var å kunne vise til suksessfaktorer og bidra til en forbedring både innen egen og andre sektorer.

For å veie opp for disse begrensningene ved å studere egen etat er det viktig å være åpen om egne antakelser og egen forutinntatthet gjennom studien (Nielsen & Repstad, 2006, s. 257). Dette gir oppgaven en gjennomsiktighet som er viktig for at undersøkelsen skal oppfattes som troverdig og pålitelig for andre forskere og lesere. Jeg har derfor valgt å være åpen om mine egne negative opplevelser og erfaringer når det kommer til digital sikkerhet, slik at de som leser oppgaven er klar over dette og hvilken betydning det kan ha hatt for mine tolkninger. Samtidig har jeg forsøkt å legge disse erfaringene til side gjennom hele prosessen for å unngå at det har formet resultatene, samtidig som jeg har hatt en grundig kodeprosess og gått gjennom dataene flere ganger. Det at jeg på forhånd har valgt å studere fenomenet digital beredskap ut fra et organisatorisk perspektiv vil forhåpentligvis også gjøre at jeg i større grad har klart å plassere eventuelle feil og mangler til systemet fremfor hos enkeltindivider, noe Nielsen og Repstad (2006, s. 261-262) fremhever som en svakhet hos folk generelt.

3.7 Kritisk refleksjon over valgt design og metode

Selv om valgene jeg har tatt rundt bruk av metode og datainnsamling har vært gjennomtenkt og ansett å være den beste fremgangsmåten for min undersøkelse, vil det alltid være svakheter ved metoden man har valgt og andre alternativer som også kunne ha fungert like bra. Det første spørsmålet retter seg mot valget av kvalitativ fremfor kvantitativ metode, og Yin (referert i Johannessen et al. ,2011, s. 90) påpeker at casestudier med fordel kan gjennomføres ved å kombinere forskjellige metoder for å skaffe seg mye og detaljert data. En kombinasjon av metoder vil imidlertid kreve en god del mer tid og ressurser, noe som vil være en avgjørende faktor for min masteroppgave. Spørsmålet blir dermed heller om en ren kvantitativ metode kunne ha egnet seg i like godt til dette prosjektet. En spørreundersøkelse kunne til en viss grad ha fanget opp mange av de samme momentene som et intervju, men jeg ville da ha

mistet muligheten til å gå dybden på svar jeg ønsket å få utdypende informasjon rundt for å forstå fenomenet fullt ut. På den andre siden ville jeg i større grad vært i stand til å generalisere svarene jeg fikk og på den måten ha fått en større overføringsverdi til andre etater og organisasjoner.

På grunn av tidsbegrensningene valgte jeg også en tverrsnittundersøkelse, selv om en slik undersøkelse ikke vil kunne si noe om utviklingen over tid, i tillegg til at det kan være problematisk å avdekke årsakssammenhenger mellom fenomener (Johannessen et al., 2011, s. 78-79). Videre valgte jeg å gå for intervju som datainnsamlingsteknikk i studien. Observasjon kunne imidlertid ha vært en bra metode for å registrere *faktisk atferd*, men det ble ganske fort utelukket både på grunn av begrensninger i tid og ressurser, og ikke minst på grunn av Covid-19. I tillegg var jeg ute etter å innhente informasjon om hvordan mennesker *opplever* noe, og da ville det være avgjørende at jeg faktisk fikk snakke med informantene og ikke bare for eksempel observere dem.

Når det kommer til utvelgelse av informanter fikk jeg som sagt snakke med personer som satt med et fagansvar innenfor digital sikkerhet, og samtlige hadde god kunnskap om feltet og kunne besvare alle spørsmål på en god og utfyllende måte. Jeg tok på forhånd høyde for at det kunne være en mulighet for at noen ikke kunne eller ville delta som informanter, og at utvalget av den grunn enten ble redusert i sin helhet eller at jeg ikke fikk like gode informanter som først tenkt. Derfor var det viktig at jeg på forhånd hadde tenkt gjennom hva som var gjennomførbart når det kom til rekrutteringen, for på den måten skape større sjanse for at de jeg ønsket faktisk stilte opp. Nå var jeg ikke ute etter personer med en veldig særegen kompetanse eller andre faktorer som gjorde at det skulle være en stor utfordring å få tak i rette personer, men det vil alltid være et visst usikkerhetsmoment knyttet til om folk er villige og har tid til å stille opp. Det som imidlertid kan ha spilt en rolle i undersøkelsen min er at de tre virksomhetene hadde ulik størrelse, og dermed hadde også informantene til dels ulike stillingstitler. Én virksomhet er et middels stort selskap, mens en annen er mange ganger så stor og har dermed også flere personer som jobber med digital sikkerhet. Det er dermed ikke gitt at jeg fikk tak i de «rette» personene sånn sett, og at det kunne ha vært andre jeg heller burde ha pratet med. Samtidig er dette noe jeg har vært bevisst på når jeg har analysert dataene, slik at jeg også har tatt konteksten i betraktning når jeg har tolket funnene.

Det at jeg gikk relativt bredt ut i starten og utformet en intervjuguide med flere store temaer var positivt med tanke på utgangspunktet for grounded theory og det å få en empiridrevet start. Det kan imidlertid ha vært en svakhet i og med at jeg gjennomførte en

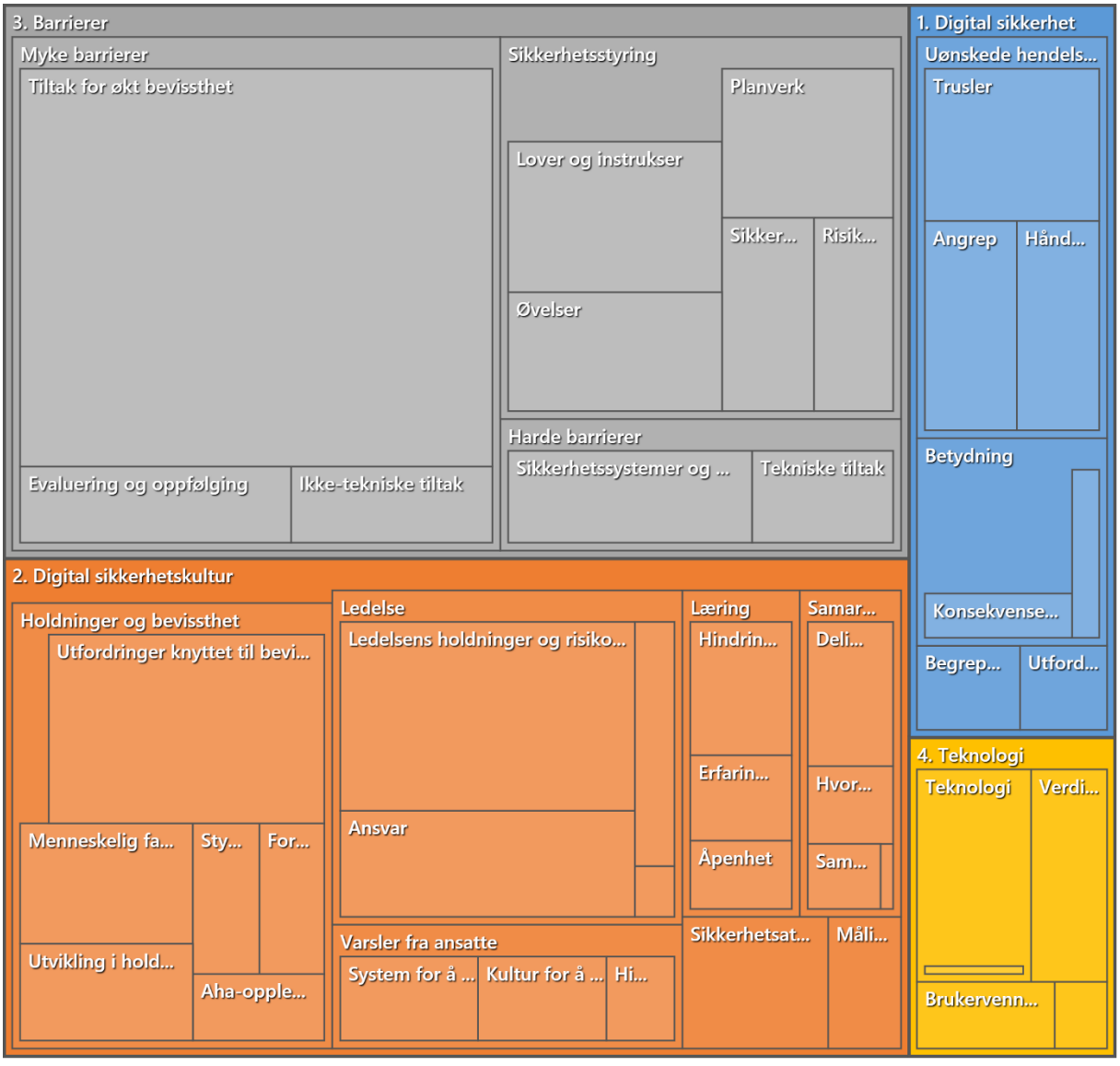
komparativ studie hvor svarene skulle sammenliknes. Selv om jeg sørget for at alle informantene var innom alle temaene, ble det likevel en viss forskjell i hvor mange oppfølgingsspørsmål de fikk i og med at noen tema etter hvert ble ansett å være mindre relevante. En komparativ studie burde kanskje ha fulgt en strukturert intervjuguide hele veien, men da måtte jeg også ha vært mer teoristyrt i starten for å kunne ha utformet en så spesifikk intervjuguide. I og med at jeg sørget for at alle informantene var innom alle temaene, mener jeg likevel at sammenlikningsgrunnlaget er til stede.

3.8 Etiske problemstillinger

All forskning er underlagt såkalte forskningsetiske prinsipper og retningslinjer, spesielt innen samfunnsforskningen da denne type forskning berører enkeltmennesker og forhold mellom mennesker i stor grad (Johannessen et al., 2016, s. 83). Momentene som gjelder her har i all hovedsak blitt redegjort for under punkt «3.3 Behandling av data», og jeg henviser derfor til dette for nærmere informasjon om de etiske hensynene som ble tatt i prosjektet.

4 Empiriske funn

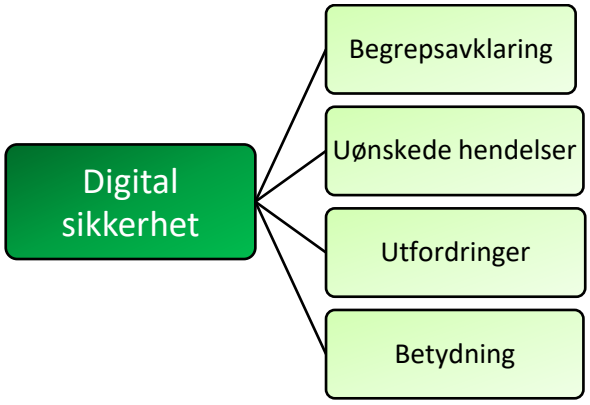
Etter å ha gjennomført en grundig transkribering og en omfattende kodeprosess gjennom programmet NVivo, kom jeg til slutt frem til 4 hovedkategorier og 18 underkategorier (på første nivå) som utpekte seg som relevante for å påpeke funn i studien og for å besvare problemstillingen. Flere av underkategoriene har igjen egne underkategorier, men disse vil bli nevnt i den løpende teksten der de hører hjemme. Figur 4.1 viser en oversikt over alt det kodede materialet:



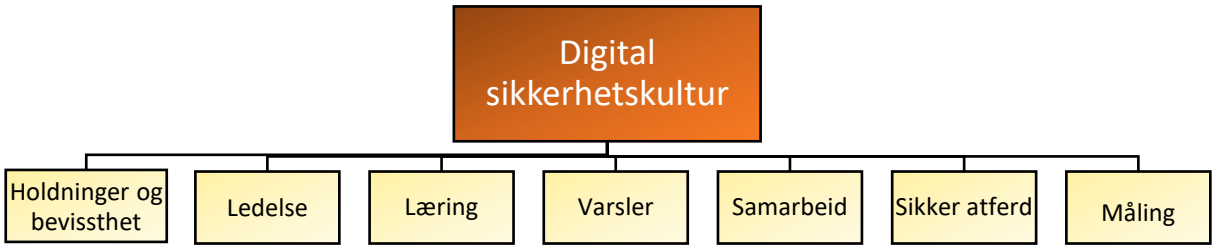
Figur 4.1. Oversikt over hoved- og underkategorier i datamaterialet. Hentet fra NVivo.

Figur 4.1 gir et innblikk i det omfattende datamaterialet, og viser også til en viss grad dybden i analysen når man ser alle de ulike underkategoriene. Som man ser av denne figuren er det

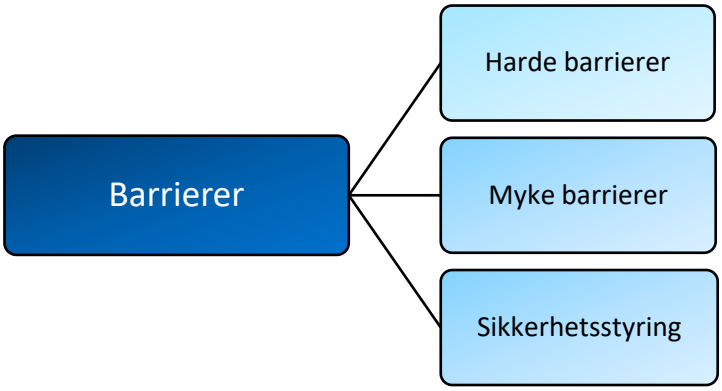
kategoriene digital sikkerhetskultur og barrierer som er desidert størst med tanke på innhold. Videre ble det naturlig for meg å ha en egen hovedkategori med digital sikkerhet da dette ble et relativt stort tema med tanke på hva informantene la i begrepet, hvilken betydning det har for dem, samt hvilke trusler og utfordringer de mener å stå overfor. Teknologi ble lagt opp som en egen kategori da mange av informantene selvsagt også var innom dette temaet når vi snakket om digital sikkerhet. I den nedenstående oversikten viser jeg alle disse fire hovedkategoriene med tilhørende 18 underkategorier da dette gir et godt overblikk over alle funnene som ble gjort. Modellene er laget med utgangspunkt i hvordan oppsettet så ut i NVivo etter endt koding:



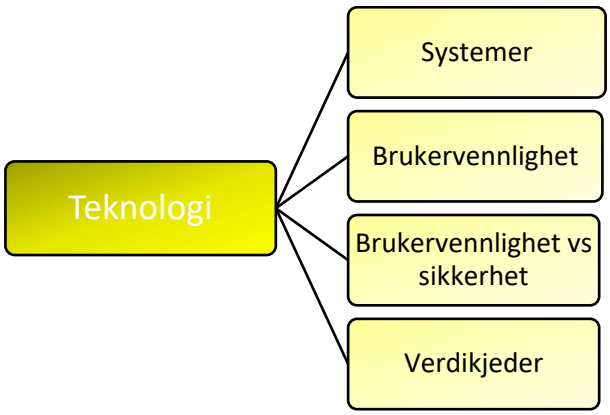
Figur 4.2. Oversikt over hovedkategorien «Digital sikkerhet», med tilhørende underkategorier.



Figur 4.3. Oversikt over hovedkategorien «Digital sikkerhetskultur», med tilhørende underkategorier.



Figur 4.4. Oversikt over hovedkategorien «Barrierer», med tilhørende underkategorier.



Figur 4.5. Oversikt over hovedkategorien «Teknologi», med tilhørende underkategorier.

I og med at fokuset mitt i oppgaven er på den organisatoriske og menneskelige delen av digital sikkerhet, har jeg valgt å se bort fra kategorien teknologi når jeg skal presentere funnene. Videre blir flere av underkategoriene til de andre hovedkategoriene slått sammen i den videre presentasjonen, dette på grunn av både leservennlighet og at flere av dem henger sammen og bør presenteres i samme avsnitt. Jeg har altså valgt å fokusere på følgende tre hovedkategorier med sine respektive underkategorier:

4.1 Digital sikkerhet

- Begrepsavklaring
- Uønskede hendelser og utfordringer
- Betydningen av digital sikkerhet

4.2 Digital sikkerhetskultur

- Holdninger, bevissthet og risikoforståelse
- Ledelse
- Varsling og læring
- Sikker atferd

4.3 Barrierer

- Forebyggende arbeid i form av opplæring og bevisstgjøring
- Spesifikke tiltak for opplæring og bevisstgjøring

Jeg vil i det følgende kapittelet presentere disse kategoriene, og empirien blir lagt frem gjennom sitater fra informantene og min egen analyse. Det vil være tilfeller hvor enkelte sitat blir brukt under ulike kategorier da det både er en viss overlapp mellom kategoriene, samt at utsagnene hadde flere betydninger og belyste ulike poenger.

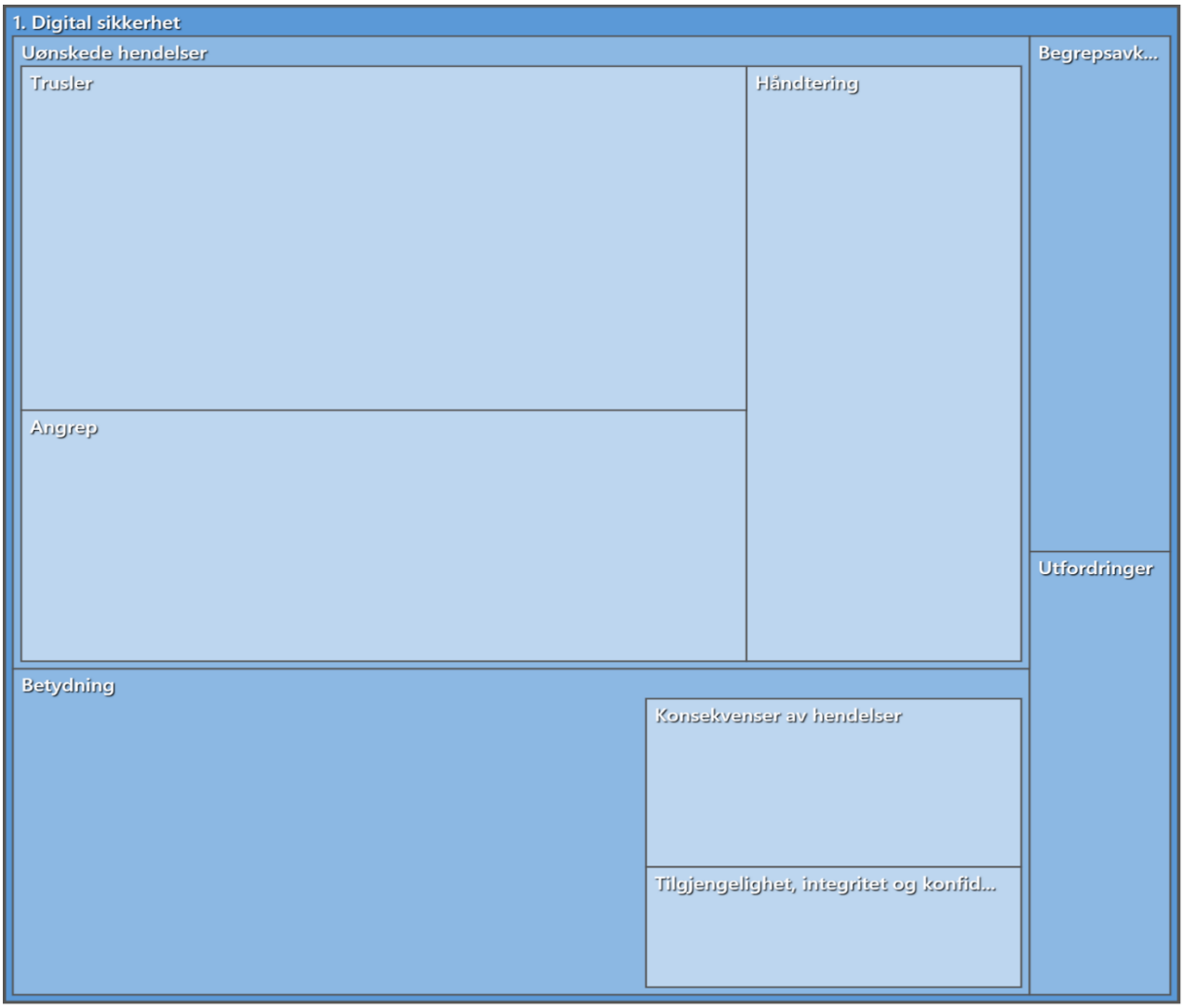
Jeg gjennomførte totalt 9 intervjuer med ansatte innenfor tre ulike sektorer. Ingen av informantene ønsket at deres virksomhet skulle bli navngitt, og tabell 4.1 viser derfor en oversikt over deres tilhørighet samt betegnelse videre i oppgaven.

Sektor	**Stilling/område**	**Pseudonym**	**Erfaring**
Finans			
	Fagleder krisehåndtering	Stian	10+
	Avdelingsleder risikostyring	Thomas	5+
	Spesialrådgiver strategisk sikkerhet	Trine	15+
Kraft			
	IKT-sikkerhetskoordinator	Camilla	5+
	Leder IKT-sikkerhet	Mads	10+
	Krisekoordinator	Steinar	15+
Justis			
	Sikkerhetsrådgiver IKT-sikkerhet	Knut	15+
	Sikkerhetsanalytiker	Lars	10+
	Seniorinformasjonssikkerhetsrådgiver	Daniel	5+

Tabell 4.1. Beskrivelse av informantene og deres sektortilhørighet.

4.1 Digital sikkerhet

I det følgende kapittelet presenteres hovedkategorien digital sikkerhet. Figur 4.3 viser en fremstilling av denne hovedkategorien med tilhørende underkategorier.



Figur 4.6. Oversikt over hoved- og underkategorier – «Digital sikkerhet». Hentet fra NVivo.

I og med at jeg på forhånd visste at det blir brukt ulike begreper rundt omkring i ulike virksomheter når det kommer til digital sikkerhet, var det viktig for meg å få informantene til å utdype hvilket begrep de selv brukte og hvilken betydning det hadde for deres virksomhet. I tillegg ønsket jeg å få en oversikt over hvilke trusler de ulike virksomhetene opplever å stå overfor, samt hvilke angrep de eventuelt hadde blitt utsatt for. Dette ville gi meg viktig bakgrunnskunnskap og forståelse som kunne være med å kaste lys over de andre funnene i

oppgaven. Noen av underkategoriene fant jeg det mest hensiktsmessig å slå sammen, og ut fra dette endte jeg opp med følgende tre underkategorier:

- Begrepsavklaring
- Uønskede hendelser og utfordringer
- Betydningen av digital sikkerhet

4.1.1 Begrepsavklaring

De fleste informantene svarte at deres virksomhet bruker begrepet IKT-sikkerhet eller informasjonssikkerhet. Begrepene blir imidlertid brukt litt om hverandre og noen benytter også begrepet cybersikkerhet, men påpekte samtidig at dette begrepet kan være litt misvisende hvis man tenker at det er informasjon som skal beskyttes – fordi dette må gjøres gjennom både digital sikkerhet, fysisk sikkerhet og personellsikkerhet. Camilla fra kraftsektoren påpekte at begrepet cyber er relativt nytt, og et begrep som kan gjøre at mange føler det som mer fremmed og ikke forstår hva det faktisk inneholder. «Jeg får litt følelsen av at hvis noen snakker om cyber, så faller mange av og skjønner ikke helt hva det faktisk inneholder. Men bruker vi IKT-sikkerhet føler jeg vi har med oss litt flere folk på lasset.» (Camilla, kraftsektoren). Mine informanter var imidlertid personer som jobbet med dette som sitt fagfelt, og for dem virket det som om bruken av begrepene ikke hadde så stor betydning da de visste hva det innebar uavhengig av begrepet som ble brukt.

Målet med digital sikkerhet er jo i stor grad å beskytte informasjon, og ut fra det er selvfølgelig begrepene informasjonssikkerhet eller IKT-sikkerhet veldig dekkende. Jeg er derimot kun ute etter den digitale siden av dette i min oppgave, og har derfor valgt å bruke begrepet digital sikkerhet selv om det ikke er det begrepet som blir brukt av virksomhetene selv. Dette ble også forklart for informantene gjennom intervjuene.

4.1.2 Uønskede hendelser og utfordringer

De fleste av informantene forteller at de daglig har spam-mail som blir stoppet av automatiske systemer som overvåker trafikken kontinuerlig, og at de ser mange forsøk på å komme seg inn i systemene deres. Ingen har imidlertid blitt utsatt for alvorlige angrep hvor uvedkommende har fått tak i sensitiv informasjon. Thomas fra finanssektoren sier at de blir angrepet flere tusen ganger daglig, og at de også regelmessig er utsatt for relativt avanserte angrep. Han

mener at deres største trussel er digitale bankranere, og gjennom en kartlegging har de sett at de mest aktive aktørene når det kommer til forsøk på dette kommer fra land som blant annet er merket som en etterretningstrussel for Norge. «Vi ser lite politisk hacking hos oss, men de digitale bankranerne er veldig aktive og de kommer fra kjente land som Nord-Korea, Iran, Russland og Kina.» (Thomas, finanssektoren).

Trine fra finanssektoren sier også at statlige aktører alltid er noe de følger med på, og at det største problemet med dem er at de har mye kapasitet og ressurser dersom de først bestemmer seg for å gå inn. Også Lars fra justissektoren trekker frem de statlige aktørene som en stor trussel, og at dette kanskje er noe som skiller seg litt ut på grunn av virksomhetens posisjon og rolle i samfunnet. «Angrepene i seg selv er nok de samme, men vi er kanskje redd for andre typer trusselaktører. Vi vet jo at det finnes statlige aktører som er mer interessert i oss enn det den generelle spam-entusiasten er». (Lars, justissektoren). Camilla (kraftsektoren) mener derimot at det ikke er de statlige aktørene som er deres største trussel, men heller de mer opportunistiske som sender ut noe til alle og håper å få napp et sted.

> Jeg tror ikke vi står på kartet til Kina eller Russland nå med det første, men selvfølgelig, vil man lamme norsk infrastruktur så er vi jo et relativt stort nettselskap og kan fort bli rammet på den måten. Men jeg tror nok sannsynligheten er større for at vi blir rammet av de som går mer ut i bredden. (Camilla, kraftsektoren).

Samtidig erkjenner hun det faktum at en mer avansert trusselaktør gjerne kan være i nettet lenge uten at de oppdager det, og at de heller ikke alltid kan klare å se hva de egentlig har gjort og hva de har funnet ut. Dette er også noe Daniel (justissektoren) poengterer, samtidig som at han er veldig klar på hvilken trussel de større aktørene faktisk utgjør og hva de kan få til hvis de virkelig vil.

> Frem til nå har vi vært prisgitt at de som ønsker å angripe oss ikke har gjort det. Det er stadig flere stater som begynner å stå bak denne type aktivitet, og hvis de bare bruker lang nok tid og dyktige nok folk, så kommer de seg inn. (Daniel, justissektoren).

Det å kjenne til den digitale verdikjeden i egen virksomhet er et av punktene som Nasjonal Sikkerhetsmyndighet mener er svært viktig for å forhindre digitale angrep. De aller fleste virksomheter har flere ulike underleverandører som de er avhengige av, og dette er noe Mads (kraftsektoren) og Thomas (finanssektoren) er veldig opptatt av. Mads poengterer at den største risikofaktoren deres er underleverandører som ikke har den samme tankegangen rundt sikkerhet som det de har, og at dette utgjør en stor trussel for muligheten til å komme seg inn i

deres systemer.

> Det er veldig ofte et stort gap mellom forventningene fra oss og det de leverer. De sier at de har sikkerhet, men ikke på det nivået vi ønsker. Derfor må vi stille litt andre krav, og det kan ofte være litt vanskelig å få gjennom. (Mads, kraftsektoren).

Thomas sier at de er helt avhengige av eksterne leverandører, og at idet de setter ut drift så har disse leverandørene tilgang til systemene deres og til informasjonen deres. Han understreker derfor at det er veldig viktig å følge opp disse og sørge for at de også har god sikkerhet.

> Vi har jo satt ut alt av tjenester, i prinsippet drifter vi ingenting selv. Og når du setter ut en tjeneste gir du i praksis en tredjepart som du kanskje ikke kjenner så godt til, tilgang til informasjonen din. Det holder dermed ikke at vi har god sikkerhet hos oss, vi er også avhengige av at leverandørene har tilstrekkelig sikkerhet. (Thomas, finanssektoren).

Noe som kjennetegner digital sikkerhet er nettopp dette med de lange og veldig ofte uoversiktlige verdikjedene. De fleste har det slik som Thomas beskriver; de har kanskje noen egne systemer, men i all hovedsak er de avhengige av andre leverandører for å drifte virksomheten. Det blir dermed svært viktig for sikkerheten å ha kontroll på virksomhetens verdikjeder, for å vite hvem som faktisk har tilgang til hvilken informasjon. Har man en leverandør som ikke tar sikkerhet på alvor, vil dette kunne medføre store svakheter og sårbarheter hos aktuell leverandør, noe som igjen vil svekke din egen virksomhets sikkerhet.

4.1.2.1 Oppsummering uønskede hendelser og utfordringer

Det varierer hvilke aktører de ulike virksomhetene mener er deres største trussel. Dette kan skyldes at de ikke har opplevd reelle angrep fra store aktører eller at de mangler informasjon om aktørene, men det kan også være et uttrykk for hvilken evne og vilje de har til å innse hvilken risiko de står overfor. Dette er sentralt innenfor teorier om sikkerhetskultur, hvor kognitive faktorer som risikooppfatning og -erkjennelse har stor betydning. Det er likevel en felles oppfatning av at de som samfunnskritiske funksjoner er spesielt utsatt og interessante for både kriminelle og statlige aktører. Alle sier at de kontinuerlig overvåker trafikken som foregår på utsiden av systemene deres, og mange påpeker at de aller fleste angrepene fremstår usofistikerte og ikke-målrettede. Dette kan imidlertid også skyldes at angrepene har blitt stoppet på et tidlig tidspunkt, og at de dermed ikke har nok informasjon til å si om det var et

mer bevisst angrep. I tillegg vil det å ha kontroll over virksomhetens verdikjede være svært viktig for å kunne sørge for at alle underleverandører tar sikkerhet på alvor slik at sårbarhetene blir færrest mulig.

4.1.3 Betydningen av digital sikkerhet

Informantene fra finanssektoren skilte seg tydelig ut med å understreke hvor viktig det er for deres eksistens at de har et høyt digitalt sikkerhetsnivå. Som de selv påpekte er de i aller høyeste grad en digitalisert virksomhet som er avhengig av god digital sikkerhet for å i det hele tatt å overleve – en nedetid på bare noen minutter kan være kritisk og gi store konsekvenser for virksomheten. «Vi er i høyeste grad en digitalisert virksomhet, det er veldig lite verdier vi skaper som ikke skjer digitalt. Det gjør også at krav til systemer, back-up, redundans, og oppe-tid er ganske høyt.» (Stian, finanssektoren). Thomas trekker også frem det faktum at de blir angrepet flere tusen ganger daglig, og at høy sikkerhet dermed er essensielt for å opprettholde kritiske betalingssystemer som brukes av befolkningen i hele Norge. «Sånn sett har digital sikkerhet førsteprioritet hos oss, for vi er avhengig av god sikkerhet for å overleve siden vi ikke tåler noe særlig nedetid.» (Thomas, finanssektoren). Dette viser at de har et stort fokus på det at de er en samfunnskritisk funksjon som landet i sin helhet er avhengig av at fungerer, samtidig som de også har en egeninteresse i dette i form av å overleve og konkurrere i markedet.

Daniel (justissektoren) påpeker på sin side en veldig viktig faktor når det kommer til digital sikkerhet, nemlig at IKT-tjenestene i stor grad er sentralisert og dermed rammer mye bredere dersom de går ned enn hva en fysisk hendelse gjør som rammer ett sted eller én lokasjon. I tillegg er det vanskeligere å avdekke aktivitet, noe som gjør det ekstra utfordrende.

> IKT-systemene er i stor grad sentraliserte, slik at dersom du slår ut IKT-systemer generelt så vil konsekvensene ramme alle som er avhengige av de IKT-systemene. I tillegg er det ikke så lett å avdekke aktivitet, så det kan foregå ting i systemene som vi ikke har full kontroll over. (Daniel, justissektoren).

Denne «usynligheten» samtidig med at veldig mange kan bli rammet, gjør digitale hendelser mer utfordrende både å håndtere og å forebygge. De forholder seg ikke til verken fysiske eller organisatoriske grenser, og vil kreve stor innsats fra flere tverrfaglige hold både i forkant og i etterkant av en hendelse.

I kraftsektoren kan man få inntrykk av at digital sikkerhet ikke har så mye fokus som det har innen finanssektoren spesielt, og Mads (kraftsektoren) beskriver dette gjennom å fortelle at han har jobbet mye med å få alle ansatte til å innse at digital sikkerhet er en viktig del av organisasjonens oppgaver. «Jeg har jobbet mye med det å løfte IKT-sikkerhet fra å være noe noen driver med, til at det er noe vi alle driver med.» (Mads, kraftsektoren). Camilla (kraftsektoren) sier at dette kan ha sammenheng med den utviklingen kraftsektoren har vært gjennom de siste årene, hvor mer og mer har blitt digitalisert og at det ikke lenger er så vanntett mellom det administrative systemet og driftskontrollsystemet. Samtidig påpeker hun at de mer tradisjonelle hendelsene fortsatt er den største trusselen hos dem, og at det er viktig at man tar hensyn til alle typer hendelser:

> Jeg er veldig opptatt av IKT-sikkerhet og tenker at det er kjempeviktig, men det er jo de tradisjonelle hendelsene som fortsatt er den mest reelle og sannsynlige trusselen hos oss. Det er derfor viktig at vi har respekt for alle typer hendelser som kan gjøre skade på driften vår. (Camilla, kraftsektoren).

En virksomhet som ikke kan sies å være «heldigitalisert» står dermed overfor flere andre områder som også må prioriteres og tas hensyn til. Hvis man i tillegg anser andre typer hendelser som mer sannsynlige, vil digital sikkerhet naturlig nok i større grad konkurrere om både tid, fokus og ressurser.

4.1.3.1 Oppsummering betydningen av digital sikkerhet

Finanssektoren skiller seg ut gjennom deres oppfatning av hvor viktig digital sikkerhet er for å opprettholde den funksjonen de er satt til å ivareta som en samfunnskritisk funksjon. Justissektoren er også veldig klar på hvor bredt en digital hendelse rammer og hvor mye som blir satt ut av spill sammenlignet med mer tradisjonelle hendelser. Samtidig understreker også de, i likhet med kraftsektoren, at digital sikkerhet i større grad er ett av *flere* områder hvor virksomheten må ha fokus, og at det dermed blir en av flere oppgaver som må konkurrere om tid og ressurser. Dette er nok ikke noe som er spesielt for disse sektorene, de fleste virksomheter må i stor grad forholde seg til flere sikkerhetsområder som alle krever en viss oppmerksomhet. I tillegg er digital sikkerhet et relativt nytt felt og et område som er lite synlig og til dels fremmed for mange, noe som også kan bidra til mindre fokus. Mange virksomheter må derfor jobbe aktivt med å skape en bedre forståelse blant sine ansatte og deres rolle i arbeidet med digital sikkerhet slik at den kollektive bevisstheten øker.

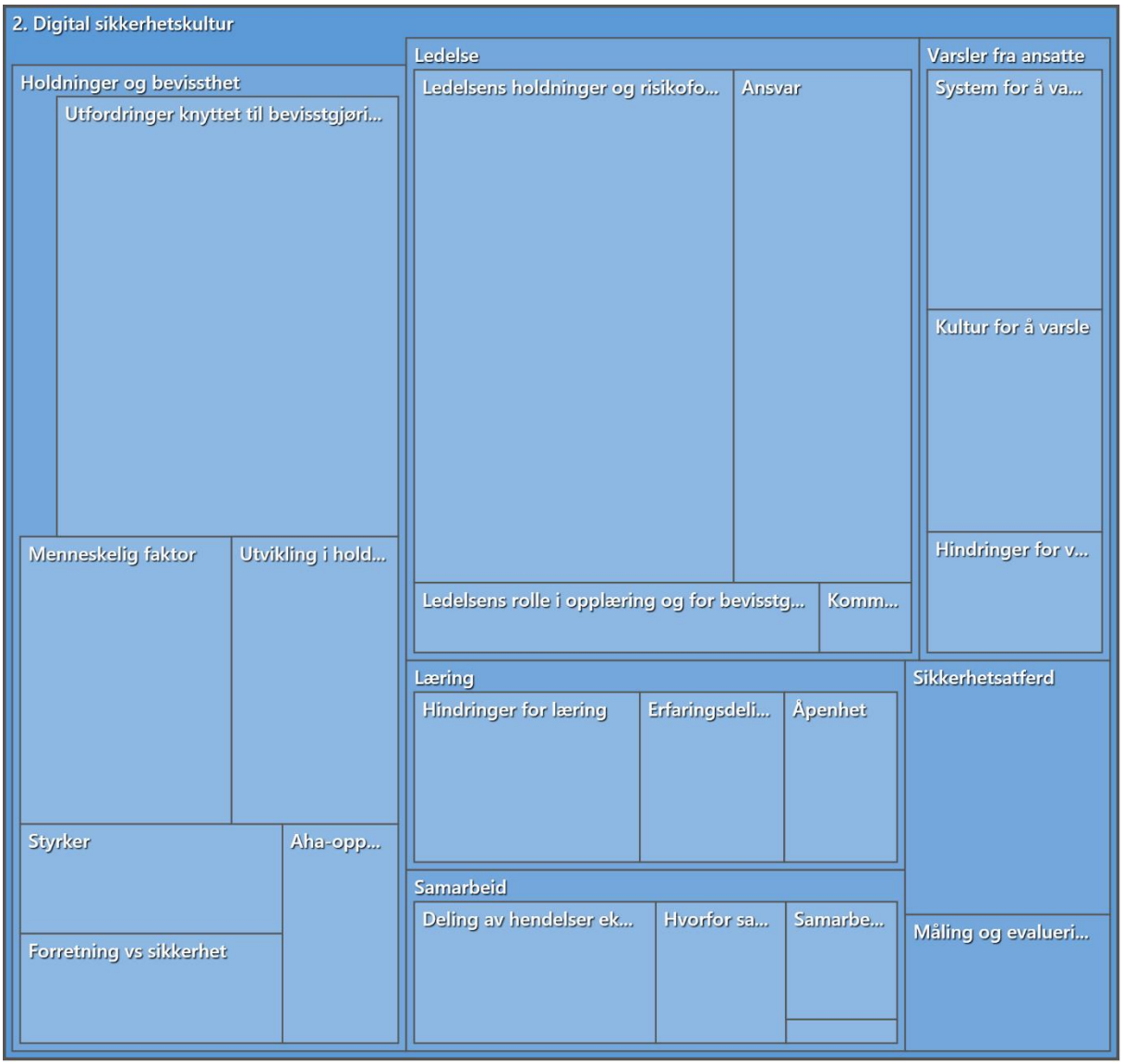
4.1.4 Oppsummering digital sikkerhet

Det varierer hvilke aktører virksomhetene mener er deres største trussel. Innen finans- og justissektoren har de fokus rettet mot store statlige aktører fra land som Kina, Nord-Korea, Iran og Russland, og det påpekes at disse aktørene har stor kapasitet og mange ressurser dersom de først ønsker å ta seg inn i systemene deres. Kraftsektoren mener derimot at de ikke står på radaren til disse aktørene, men at det heller er de små og mer opportunistiske som sender ut til mange som er deres mest sannsynlige trusselaktør. I tillegg trekker noen frem virksomhetenes verdikjeder som en risiko i form av underleverandører som ikke har den samme risikoforståelsen og tankegangen når det kommer til sikkerhet. Ulikhetene i oppfatningen av risiko og trusselutøvere man står overfor kan gjerne skyldes det faktum at for eksempel kraftsektoren ikke har sett noen tegn til at de statlige aktørene er interessert i deres virksomhet, men det kan også skyldes manglende risikoforståelse eller -erkjennelse. Det er derfor viktig at virksomhetene har en god og realistisk risikotilnærming når de lager planverk og instrukser for digital sikkerhet.

I likhet med oppfatningen om trusselaktører, er det også variasjoner når det kommer til hvilken betydning digital sikkerhet har for hver av virksomhetene. Mens finanssektoren ser på seg selv som en heldigitalisert bedrift hvor digital sikkerhet er avgjørende for å overleve i markedet, er det bare ett av flere områder som krever fokus og ressurser innen kraft- og justissektoren. Dette gjør at digital sikkerhet i større grad må «konkurrere» mot mer tradisjonelle hendelser, noe som betyr at det kanskje ikke er like lett å få fokus på det verken blant ledelsen eller de ansatte. I tillegg er det et relativt nytt felt for veldig mange, og det er i stor grad mindre synlig enn rent fysiske hendelser. Dette gjør at det kan oppleves som fremmed for mange, med det resultat at det høyst sannsynlig krever mer bevisstgjøring enn de tradisjonelle hendelsene.

4.2 Digital sikkerhetskultur

I dette kapittelet presenteres hovedkategorien digital sikkerhetskultur. Fra teorien har jeg tidligere forklart at begrepet sikkerhetskultur har flere ulike definisjoner, men felles for de fleste er at de inneholder holdninger, verdier og kompetanse innen sikkerhet og atferdsmønstre knyttet til etterlevelse av virksomhetens sikkerhetsprogrammer. Figur 4.7 viser en fremstilling av denne hovedkategorien med tilhørende underkategorier:



Figur 4.7. Oversikt over hoved- og underkategorier – «Digital sikkerhetskultur». Hentet fra NVivo.

Flere av underkategoriene har også egne underkategorier, men disse vil bli gjennomgått i den løpende teksten der de hører hjemme. Noen av underkategoriene fant jeg det også mest hensiktsmessig å slå sammen, og ut fra dette endte jeg opp med følgende fire underkategorier:

- Holdninger, bevissthet og risikoforståelse
- Ledelse
- Varsling og læring
- Sikker atferd

4.2.1 Holdninger, bevissthet og risikoforståelse

Digitaliseringen har kommet for fullt de siste årene, og for mange betyr det at digital sikkerhet er et relativt nytt begrep. Det er riktignok varierende hvor stort fokus det har fått i de ulike sektorene, og hvordan de ansatte forholder seg til det. Holdninger til digital sikkerhet kan i stor grad være med på å forme hvilken bevissthet og risikoforståelse de ansatte har. Det er også ulike utfordringer som gjør seg gjeldende i de ulike sektorene, og jeg vil nå gjøre rede for dette i den videre del av oppgaven. Følgende underkategorier vil bli presentert:

- Aha-opplevelser
- Sikkerhet versus forretning
- Menneskelig faktor
- Utfordringer med bevisstgjøring
- Utvikling i holdninger

4.2.1.1 Aha-opplevelser

En viktig faktor for å øke fokuset på digital sikkerhet i virksomhetene er det jeg har valgt å kalle aha-opplevelser, hvor informantene påpeker at fokuset har økt når man har sett andre store virksomheter bli rammet av digitale angrep. Det å se at andre og sammenlignbare virksomheter blir rammet av til dels avanserte angrep som har kostet millioner av kroner, gjør at bevisstheten øker og at både ansatte og ledere innser at dette faktisk er noe som kan ramme dem også. Camilla (kraft) sier at slike hendelser har hjulpet masse når det gjelder å få fokus på digital sikkerhet, ikke minst dersom det har vært en hendelse som er i en bransje nær dem:

> Den hendelsen med Hydro tror jeg skremte dem litt, og da var det nok mange som tenkte «Oj, tenk om det hadde vært oss». Så det hjelper veldig mye å få fokus på ting når det skjer slike hendelser, alle er jo litt redde for at man skal være nestemann ut. (Camilla, kraftsektoren).

Også i justissektoren ser vi noe av det samme:

> Vi ser jo at det må litt ekstreme hendelser til for at folk skal våkne og henge med, så den hendelsen på Stortinget hjalp oss masse. Vi som jobber med IT sitter jo og leser en del IT-nyheter og ser at det skjer angrep på myndigheter i andre land, men det har på en måte vært litt distansert før det plutselig også skjer her hjemme. (Lars, justissektoren).

Det å få hendelser mer tett på kroppen er altså noe som gjør at både ansatte og ledelse får øynene opp for at det kan skje dem også. Dette kan ha direkte sammenheng med helt primære kognitive funksjoner hos mennesker, nemlig det faktum at vi vurderer risiko ut fra subjektive kriterier. Det at det rammer noen som man kan sammenlikne seg med og som kanskje står en nær, gjør at man opplever risikoen som større enn hvis det skjer med noen man ikke relaterer seg like mye til.

I tillegg nevner informanter fra alle sektorene at de også gjerne kjører scenarioer og presentasjoner hvor de legger frem verstefallseksempler med rot i virkeligheten, slik at deltakerne skal kunne se hva som faktisk kan skje på grunn av allerede manglende sikkerhetstiltak eller manglende bevissthet. Alle har erfart at dette har vært med på å skape økt bevissthet rundt de truslene man står overfor. Lars forteller at han har kjørt demonstrasjoner av hvordan han selv ganske enkelt kan komme seg forbi antivirusprogrammer, og dermed vist at man ikke kan stole fullt og helt på slike programmer.

> Jeg er litt tilhenger av skremselstaktikk og å faktisk demonstrere et verstefallsscenario slik at man kan se hvordan det ser ut. Når jeg gjorde dette med et antivirusprogram og viste hvor lett det var å komme seg forbi det, var det mange som ble overrasket fordi de trodde antivirusen beskytter dem 100%. (Lars, justissektoren).

Thomas sier at de bevisst velger scenarioer som omhandler systemer de vet har for dårlig sikkerhet, nettopp for å belyse problematikken med manglende sikkerhetstiltak.

> Vi velger å være litt kyniske når vi lager scenarioer, og velger hendelser som vi vet kan skje i virkeligheten. Og når vi da får spørsmål om dette faktisk kunne ha skjedd så kan vi faktisk svare «Ja, for de tiltakene som mangler i dette scenarioet, de mangler også i virkeligheten.». (Thomas, finanssektoren).

Camilla legger vekt på at det å være åpen og ærlig om hvor stor trusselen er, er noe som er viktig for å skape mer forståelse. Hun forteller at de har vist pågående trafikk fra de ulike systemene på flere samlinger, hvor deltakerne tydelig kan se at det hele tiden er mange som forsøker å komme seg inn i nettet deres. «Da har vi fått vist litt live på en måte, og fått vist den trafikken som går. Og da ser man jo alle de som står utenfor og banker på døra, og at det skjer ting hele tiden». (Camilla, kraftsektoren).

Oppsummering aha-opplevelser

Flere informanter forteller at alvorlige digitale hendelser som har rammet andre har bidratt til å sette mer fokus på digital sikkerhet innad i deres egen virksomhet. I tillegg bruker de bevisst scenarioer og praktiske eksempler som stammer fra deres egen virkelighet når de presenterer det for ledelsen og andre, slik at de skal få øynene opp for hvor sårbare de faktisk er for trusler og angrep utenfra. Dette er en god måte å få mer oppmerksomhet på, spesielt siden mennesker generelt har en tendens til å vurdere risikoen som større hvis de føler at det kan ramme dem selv. Når informantene bruker ord som «skremte/skremsel» og «kyniske» gir det meg et inntrykk av at dette er noe de helst skulle sett at de slapp, men at det blir et slags nødvendig onde for å øke bevisstheten blant andre ansatte.

4.2.1.2 Sikkerhet versus forretning

Noe av utfordringen med sikkerhet er at det forebyggende arbeidet sjelden kan måles i penger. Og det som ikke kan måles i penger, blir ofte nedprioritert til fordel for andre ting. Balansegangen mellom sikkerhet og produksjon er vel kjent, men det var bare informantene fra finans- og kraftsektoren som trakk frem dette som et viktig tema når det kom til sikkerhetsarbeidet. Både Thomas og Stian (finanssektoren) påpeker at forretningsfokuset ofte har blitt prioritert foran sikkerhet, og at noe av grunnen til dette er at forretningssiden ikke måles på sikkerhet og heller ser på dette som merarbeid. De legger til at noen forretningsområder har kommet lengre enn andre og at det har blitt større fokus på sikkerhet også fra ledelsen, men at det generelt sett hersker en iboende målkonflikt mellom sikkerhet og forretning.

> «Time to market» gjør at det ofte rulles ut en mindre sikker løsning enn det som kunne blitt gjort. Noen ganger vil folk fra sikkerhet si at en løsning som ble rullet ut var en dårlig opplevelse på grunn av det sikkerhetsmessige aspektet, men spør du noen fra forretning så mener de det var kjempebra fordi det ble en markedsmessig suksess og da lyktes vi. (Stian, finanssektoren).

> Forretningssiden måles jo ikke på sikkerhet, og da møter du ofte motstand når du må gjøre prosesser vanskeligere for å sikre dem best mulig. Det gjør jo at de får masse tilleggsarbeid med risikoanalyser og ekstra kontroller, og de ser ikke alltid nødvendigheten av det. (Thomas, finanssektoren).

Camilla poengterer på sin side det stadig økende kravet om effektivisering, og dermed også økt behov for automatiserte prosesser. Det kan igjen bidra til at man velger mindre sikre løsninger uten at man kanskje i det hele tatt tenker over det. «Da er det jo fort gjort at også ledelsen tenker at dette var smart og kjører på uten å tenke på at det kanskje ikke ble gjort på en sikker måte». (Camilla, kraftsektoren). Samtidig sier hun at en holdning som ser på sikkerhet som tungvint og vanskelig også kan føre til at mange *bevisst* velger å ta mindre sikre snarveier, noe som gjør virksomheten ekstra sårbar for angrep. «Vi kan ikke gjøre det for strengt heller, for da finner bare folk en bakvei som antakelig er mye verre.» (Camilla, kraftsektoren).

Det er altså en utfordrende oppgave å få sikkerhet til å bli prioritert på lik linje med det forretningsmessige, og det krever en kollektiv bevissthet om hvorfor sikkerhet er viktig. Kanskje er det også her gunstig å legge frem noen verstefallsscenarioer slik at de ansatte får en felles forståelse for hva man faktisk risikerer å tape dersom man velger å omgå sikre tiltak.

Oppsummering sikkerhet versus forretning

Sikkerhet vil alltid måtte konkurrere med andre områder i en virksomhet, og de som ikke måles på sikkerhet vil heller ikke prioritere det. Det å gjøre prosesser sikrere innebærer ofte at man må gjøre noen ekstra grep som man ellers ikke hadde trengt å gjøre. Hvis ikke de ansatte har forståelse for hvorfor man er nødt til å gjøre det sånn, vil det både kunne føre til at de tar mer usikre snarveier for å spare tid, og at sikkerhet blir sett på som ekstraarbeid som står i veien for et raskt og effektivt arbeid.

Som nevnt innledningsvis ble disse motsetningene kun poengtert av informantene innen finans- og kraftbransjen, og kanskje kan dette skyldes at dette er private bedrifter som i større grad lever i et konkurransemarked hvor det å skape verdier er det som står øverst på prioriteringslisten. Justissektoren er i stor grad en del av offentlig sektor hvor virksomhetene slipper å forholde seg til det å overleve i et stadig tøffere marked. Dermed er ikke sikkerhet og produksjon nødvendigvis like fremtredende motsetninger som det er for private aktører.

4.2.1.3 Menneskelig faktor

Mye av fokuset i denne oppgaven ligger på betydningen av den menneskelige faktoren når det kommer til digital sikkerhet, og blant informantene var det til dels sprikende oppfatninger

rundt dette. Flere av informantene erkjenner at mennesker spiller en viktig rolle, men er litt reserverte i forhold til hvor stor betydning de faktisk har. Stian fra finanssektoren forteller at de selvfølgelig ser på den menneskelige interaksjonen når det kommer til phishing og sosial manipulasjon, men understreker samtidig at mennesker *ikke* er det viktigste forsvarsleddet de har – det er de digitale løsningene. Han er imidlertid klar på at et vellykket angrep også krever at mennesker har sviktet, og sier at bevissthet blant de ansatte er viktig:

> Ethvert suksessfullt angrep er basert på at både de digitale forsvarsverkene har sviktet, og at de menneskelige har gjort det. Så vi kan ikke gå rundt og tro at IT-løsninger vil berge oss hele tiden, og det krever en bevissthet hos de ansatte. (Stian, finanssektoren).

Også Knut fra justissektoren påpeker denne todelingen i et angrep:

> Systemer har blitt vanskeligere å hacke rent teknisk, og på grunn av det er det ofte en menneskelig komponent også. På den ene siden har du brannmurer og alt av teknologisk sikkerhet, og på den andre siden har du menneskelig feil. Folk må forstå at de kan bli brukt i et angrep. (Knut, justissektoren).

Selv om flere er inne på at mennesker utgjør en del av et angrep, er det interessant å se at det likevel er de tekniske systemene som får mest oppmerksomhet. Dette kan ha sammenheng med det Thomas fra finanssektoren forteller om «kampen» mellom IT-avdelinger og de som jobber med mer tradisjonell sikkerhet:

> Mange IT-avdelinger har nok en holdning som tilsier at det egentlig ikke nytter å drive med opplæring fordi mennesker uansett kommer til å gjøre feil. De mener det er bedre å satse på systemene, og da blir det nok ofte sånn at fokus og penger tilføres de tekniske løsningene – for de vil på en måte fungere uansett. (Thomas, finanssektoren).

Denne holdningen blir understøttet av Daniel fra justissektoren. Han tegner et ganske dystert, men samtidig realistisk, bilde av menneskers feilhandlinger:

> Jeg tror man må erkjenne at man ikke kommer til å komme dit at ansatte slutter å gjøre feil. Mennesker kommer til å gjøre feil, det er liksom noe av det vi driver med. Hvis man virkelig vil sørge for høy sikkerhet, tror jeg derfor løsningen er å designe det inn i arkitekturen. (Daniel, justissektoren).

Det fremstår som om Daniel har et litt mer pessimistisk syn på mennesker og deres evne til å bidra til høy sikkerhet. Det kan virke som om han ikke har så stor tro på tiltak som skal bidra til å øke bevisstheten hos de ansatte, men at man heller skal bruke ressurser på tekniske tiltak

som man vet leverer på høy sikkerhet. Lars, som kommer fra samme sektor, er imidlertid den eneste av alle informantene som sier at den menneskelige faktoren er der de har størst forbedringspotensiale, og at menneskelige feil er den største faktoren når det kommer til sikkerhet:

> Den menneskelige faktoren er der hvor jeg ser at vi må jobbe mest. Men det er helt naturlig av den grunn at vi bytter ut mennesker – folk begynner og slutter hele tiden, det er nye former for trusler som dukker opp og det er nye måter å angripe tjenester på. Dette gjør at den menneskelige faktoren, uansett hvor mye man jobber med den, er den biten som vi må være best på – menneskelige feil er den største faktoren når det kommer til sikkerhet. (Lars, justissektoren).

Også Camilla fra kraftsektoren påpeker betydningen av den menneskelige faktoren:

> Det er jo ikke tvil om at den menneskelige biten er veldig, veldig viktig. Mennesker er et av de svakeste leddene vi har. Man kan ha alt mulig av gode systemer, men det skal ikke så mye til. Et klikk eller en åpning av et vedlegg så er vi der. (Camilla, kraftsektoren).

Det er altså delte meninger om den menneskelige faktoren. Ikke nødvendigvis uenighet om viktigheten av den i seg selv, men det virker å være mer rettet mot hvor stort fokus den skal få i forhold til de teknologiske løsningene. Mennesker vil alltid gjøre feil, men nettopp fordi en menneskelig feil er det som vil kunne sette en sikker teknologisk løsning ut av spill burde man kanskje også ha et like stort fokus på å prøve å unngå disse feilene.

Oppsummering menneskelig faktor

Synet på den menneskelige faktoren er sprikende blant informantene, og jeg synes det var interessant at såpass mange av dem hadde mer fokus rettet mot det å bruke ressursene på tekniske løsninger fremfor det å jobbe med å øke bevisstheten til de ansatte. Samtidig er det et par av informantene som sier at mennesker er en av de viktigste faktorene innen sikkerhet, så det er åpenbart delte meninger om dette. Kanskje kan det skyldes det som blir omtalt som en «kamp» mellom de som jobber med IT og de som jobber mer overordnet med tradisjonell sikkerhet, men det er også variasjoner mellom disse. Dette viser at mye av holdningene er personavhengig, og kanskje knyttet opp mot hvilke erfaringer den enkelte har. Det er imidlertid ingen tvil om at mennesker kommer til å fortsette å gjøre feil, og at det å prøve å

unngå at disse feilene blir gjort burde få like mye fokus som det å ha sikre teknologiske løsninger, spesielt siden det er en menneskelig feil som til syvende og sist vil kunne sette det teknologiske systemet ut av spill. I neste del vil jeg se noe videre på dette da jeg gjør rede for hvilke utfordringer informantene ser når det kommer til bevisstgjøring av de ansatte.

4.2.1.4 Utfordringer med bevisstgjøringen

Ikke overraskende blir det nevnt mange utfordringer knyttet til det å øke de ansattes bevissthet opp mot digital sikkerhet. Det er imidlertid mange ulike faktorer som kommer frem, noe som viser kompleksiteten i arbeidet med bevisstgjøring. Informantene fra kraftsektoren er de eneste som trekker frem manglende strategi og fokus på digital sikkerhet som en utfordring, og knytter dette opp mot den utviklingen som har skjedd i kraftbransjen de senere årene. Tidligere var det mye mer manuelt arbeid og et veldig isolert system for selve styringen av strømnettet, mens det nå har blitt stadig mer digitalisert og automatisert.

> Man gjorde ikke så mye digitalt før, det var mye mer manuelle prosesser. Man dro ut på stasjonen og dro i en spak for å koble ut strømmen, mens nå sitter man på driftssentralen og trykker på en knapp for å legge om strømmen en annen vei. Man så dermed ikke de helt store truslene når det kom til digital sikkerhet tidligere. (Camilla, kraftsektoren).

Selv om de andre informantene ikke spesifikt nevner manglende fokus og strategi som en utfordring, mener imidlertid informanter fra alle sektorene at manglende forståelse blant de ansatte er en av de største utfordringene. Dette kan likevel ha sammenheng med det som Camilla forteller, nemlig at fokuset på digital sikkerhet ikke har vært der det burde være og at viljen og ønsket om å øke forståelsen blant de ansatte dermed ikke har vært til stede. Flere knytter dette opp mot mangel på kunnskap og kompetanse, og at dette også styrer hvilket fokus man har. Den manglende forståelsen dreier seg gjerne om at man ikke skjønner omfanget av digital sikkerhet og hvor mange potensielle trusler man står overfor, samt en holdning om at «dette gjelder ikke oss» og et inntrykk av at en selv er lite betydningsfull for mulige angripere. Lars fra justissektoren utdyper dette:

> Det som mangler opp mot digital sikkerhet er generell forståelse, for det er veldig mange som uttaler ting som: «Jamen, hva er det folk vil med meg da, jeg er jo ikke interessant på noe som helst nivå». Det å faktisk måtte forklare ansatte at de ikke skal

> ha passord2020 som passord og at de ikke skal klikke på alt av lenker, det viser at den generelle bevisstheten må opp. (Lars, justissektoren).

Over halvparten av informantene trekker også frem problemer med å nå ut til alle i organisasjonen som en av hovedutfordringene, og dette kan kobles direkte opp mot både interesse og forståelse. Fra teorien vet vi at det sjelden eksisterer bare én felles organisasjonskultur, men at flere ulike subkulturer eksisterer side om side innad i virksomheten. Ulike interesser og tilhørighet skaper dermed ulike kulturer, og dermed også ulike holdninger til blant annet digital sikkerhet. Trine (finanssektoren) trekker frem dette når det kommer til utfordringer med å drive opplæring for hele organisasjonen:

> Det er veldig flinke folk som jobber her, på økonomiområdene er de best i klassen fra universitet og høyskoler og de er vant til å være sånne «flinkiser». (…) Så hvis du skal drive med noe opplæring må du passe på at det er helt nøyaktig, at du ikke har noen skrivefeil og ikke skriver noe rart. Så det er ganske viktig å kjenne kulturen i virksomheten sin. (Trine, finanssektoren).

Det er også interessant at fire av informantene forteller at sikkerhet og sikkerhetstiltak har en tendens til å bli oppfattet som «kjedelig», «støy» og «styr» og noe de blir «lei av». Dette vitner om en negativ innstilling til sikkerhet, som igjen kan skyldes mangel på forståelse.

«Det er ikke så lett å nå ut til folk. Det blir jo veldig mye støy, for de har jo veldig mye annet å drive med også kommer dette her litt sånn på toppen.» (Thomas, finanssektoren).

«Vi må prøve å gjøre det litt spennende og interessant sånn at sikkerhet ikke bare blir kjedelig og gjør alt mer tungvint, men at de forstår bakgrunnen for det.» (Camilla, kraftsektoren).

«Det oppleves som styr fordi folk ikke skjønner behovene og konsekvensene hvis det går galt.» (Mads, kraftsektoren).

«Man må passe på at ansatte ikke blir lei, at det ikke blir for mye på en gang. Noen blir jo lei av at det står om sikkerhet hele tiden.» (Trine, finanssektoren).

Alle disse utfordringene viser at arbeidet med bevisstgjøring av ansatte ikke nødvendigvis er enkel. Det vil kreve kontinuerlig arbeid over tid, noe som krever både ressurser og dedikasjon. Som jeg nevnte i det foregående kapittelet var det mange av informantene som hadde mest fokus på å ha sikre tekniske systemer, og Knut fra justissektoren viser også noe av denne holdningen når han avslutter temaet bevisstgjøring: «Man kan alltids bli bedre på

bevisstgjøring, men så er spørsmålet hvor mye man skal investere i det.» (Knut, justissektoren).

Kost versus nytte er dermed det som står igjen som en slags oppsummering på utfordringer knyttet til bevisstgjøring av de ansatte. Det kan virke som om flere mener at bevisstgjøring ikke har noe for seg, og at det dermed er tilnærmet bortkastet tid og ressurser. Lykkes man derimot med en god bevisstgjøring vil man også høyst sannsynlig «spare inn» dette gjennom færre uønskede hendelser med blant annet phishing og sosial manipulasjon.

Oppsummering utfordringer med bevisstgjøringen

Det å lykkes med bevisstgjøring av ansatte kan være utfordrende, og informantene har pekt på mange ulike forhold som er med på å påvirke dette arbeidet. Camilla og de to andre informantene fra kraftsektoren påpekte at manglende fokus på digital sikkerhet og manglende strategi for bevisstgjøring har gjort at mange ansatte i deres virksomhet ikke har sett på digital sikkerhet som et område de må jobbe med, og som de dermed heller ikke har hatt interesse for. I tillegg poengterte flertallet av informantene at ansatte mangler en grunnleggende forståelse for hva digital sikkerhet er og hvordan de ansatte selv er en del av det, noe som igjen kan skyldes for lite fokus på temaet. Sikkerhet blir også ofte sett på som noe negativt og kjedelig og noe som hindrer effektivitet, mye på grunn av ulike fagmiljøer og kulturer innad i virksomheten. Mange synes derfor at det er vanskelig å nå ut til alle, og arbeidet med bevisstgjøring krever derfor at det settes fokus på temaet fra topp til bunn, og at det gis nok tid og ressurser til å drive *god* bevisstgjøring slik at man faktisk øker de ansattes forståelse for digital sikkerhet. Får man til dette er det større grunn til anta at man også får resultater i form av at færre klikker på linker og vedlegg som de ikke burde, og at nytten dermed er større enn kostnaden.

4.2.1.5 Utvikling i holdninger

Felles for alle virksomhetene er at det har vært og er en positiv utvikling når det kommer til holdninger til sikkerhet generelt, og digital sikkerhet spesielt. Stian (finanssektoren) viser dette med å fortelle om hvordan ulike sikkerhetsarrangementer har gått fra å være «noe sikkerhet driver med» til å bli arrangementer hvor konsernsjefen holder åpningstalen og hvor

hele virksomheten er representert. For kraftbransjen sin del har fokuset på digital sikkerhet kommet i takt med digitaliseringen og utviklingen i arbeidsprosessene.

> De fleste strøm- og nettselskap har nok hatt mye fokus på de mer fysiske truslene, som uvær, flom og liknende. I tillegg var det mye mer manuelle prosesser før, man gjorde ikke så mye digitalt. Noen stusset nok for en stund siden på om det i det hele tatt var nødvendig å ha IKT-sikkerhet som en del av beredskapsplanen, men det er alle godt innforstått med nå. (Camilla, kraftsektoren).

Mads påpeker også at det har skjedd en endring i hele organisasjonen: «Det har vært et generasjonsskifte etter hvert, som har gjort at vi har fått inn nye folk med et nytt syn på ting, blant annet mye mer fokus på IKT-sikkerhet.» (Mads, kraftsektoren).

Mens både kraftsektoren og justissektoren peker på en markant endring i fokuset på digital sikkerhet, forteller Thomas i finanssektoren at deres hovedfokus i lengre tid har vært på digital sikkerhet fremfor andre mer tradisjonelle sikkerhetshendelser. Dette henger nok sammen med at de er en heldigitalisert bedrift og dermed i hovedsak kun står overfor digitale trusler.

> Vi identifiserer oss veldig som et IT-selskap, og fokuset vårt de siste årene har helt klart vært på digitale hendelser, for vi ser jo at det er det eneste som treffer oss. Hvis det er snakk om å velte banken så er det mest sannsynlig noe innenfor IT. (Thomas, finanssektoren).

Dette står altså i motsetning til det kraftsektoren forteller om at digital sikkerhet først har kommet på banen de siste årene. Alle informantene i justissektoren peker på sin side på en annen utvikling, nemlig at det tidligere har vært veldig mye fokus på hemmelighold fremfor det å informere og ha fokus på hva sikkerhet er for noe og hvordan det fungerer. Dette er noe de ser på som et hinder for å skape gode holdninger og økt forståelse for digital sikkerhet og sikkerhetstiltak. «Integritet og tilgjengelighet er mye viktigere enn konfidensialitet, men tradisjonelt sett har det vært mye mer fokus på konfidensialitet.» (Knut, justissektoren).

> Man skal ikke veldig mange år tilbake i tid før alle statlige institusjoner fokuserte på hemmelighold fremfor sikkerhet. Vi har ligget litt bak i noen år, men jeg opplever at vi har vært flinke til å hente oss inn nå. (Lars, justissektoren).

> Litt av utfordringen innenfor en del sikkerhetsmiljøer er at man har hatt en tendens til hemmelighold – man tror man driver med veldig spesielle ting og ser på seg selv som veldig spesiell og hemmelighetsfull. (Daniel, justissektoren).

Et slikt hemmelighold kan sies å være en misforstått oppfatning av hva konfidensialitet faktisk er, og hvis det er her fokuset har vært er det heller ikke så rart om man opplever manglende forståelse for den digitale sikkerheten og tiltakene som har blitt iverksatt. Hvis de ansatte ikke får noen forklaring på hvorfor prosesser må gjøres mer tungvinte, kan man heller ikke forvente at de uten videre skal etterleve disse kravene.

Oppsummering utvikling i holdninger

Innen finanssektoren har fokuset i flere år vært rettet mot digitale sikkerhetshendelser, mens det i både kraft- og justissektoren er noe som har fått større fokus de siste årene, i takt med økende digitalisering og bruk av automatiserte arbeidsprosesser. I tillegg poengterer justissektoren at man sakte, men sikkert har klart å gi litt slipp på det å skulle holde ting hemmelig og heller satse på økt tilgjengelighet og bevissthet blant de ansatte. Det er imidlertid interessant å se at selv om fokuset til finanssektoren lenge har vært rettet mot digitale trusler og angrep, møter de likevel på utfordringer når det kommer til ansattes holdninger og forståelse for ulike sikkerhetstiltak som blir iverksatt. De sliter dermed med de samme utfordringene som virksomheter som ikke har hatt like mye fokus på digital sikkerhet.

4.2.1.6 Oppsummering holdninger, bevissthet og risikoforståelse

Det å se at andre virksomheter blir rammet av digitale angrep, har bidratt til å sette fokus på temaet også hos virksomhetene til mine informanter. De har sett hva det har kostet av både penger og omdømme hos andre, og da har det også vært lettere å innse hvilke konsekvenser det kan ha for deres egen del. Dette er helt i tråd med elementære kognitive prosesser hos oss mennesker, og noe man kan bruke bevisst for å øke oppmerksomheten rundt temaet. Virksomhetene består imidlertid av mange ulike fag- og arbeidsmiljøer, og flere understreker den iboende målkonflikten mellom sikkerhet og produksjon/forretning. For de som ikke måles direkte på sikkerhet, oppfattes ulike sikkerhetstiltak som unødvendige og tungvinte, noe som igjen fører til at de heller finner andre og usikre snarveier. Det kreves derfor en økt forståelse for den digitale risikoen og de ansattes egen rolle i arbeidet for å forhindre angrep.

Noen av informantene mener at mennesker aldri vil slutte å gjøre feil, og at det dermed er bedre bruk av penger og ressurser å satse på sikre teknologiske systemer heller enn bevisstgjøring og opplæring. Samtidig påpeker andre at mennesker er den største faktoren når det kommer til sikkerhet, og at man er helt avhengig av at også menneskene er bevisst for å unngå at de gjør feil som setter de sikre systemene ut av spill. Dette viser en interessant variasjon blant fagspesialister på området, og det viser også hvor vanskelig det kan være å veie disse tiltakene opp mot hverandre. Spørsmålet om hva som er best bruk av penger og ressurser bør derfor ta i betraktning hvor mye man sparer på at ansatte i større grad *unngår* å trykke på lenker og vedlegg som i verste fall kan gi uvedkommende tilgang til virksomhetens sensitive systemer. Gode holdninger til digital sikkerhet og menneskenes rolle i det er videre noe som må forankres i ledelsen, og neste kapittel vil derfor omhandle ledelse og deres holdninger og bevissthet rundt digital sikkerhet.

4.2.2 Ledelse

Det er ingen tvil om at ledelsen har stor påvirkning når det kommer til det å skape en god sikkerhetskultur, og teorien legger stor vekt på ledelsens forpliktelse til sikkerhet. Deres holdninger og bevissthet er med på å forme de ansattes oppfatninger, og det er derfor avgjørende for en god digital sikkerhetskultur at ledelsen setter fokus på digital sikkerhet og dens betydning for virksomheten i sin helhet. Det er imidlertid flere utfordringer som både ledelsen selv står overfor, men også når det kommer til kommunikasjon med ledelsen og deres holdninger til sikkerhetsarbeidet. Følgende underkategorier vil bli presentert:

- Fragmenterte ansvarsområder
- Ledelsens holdninger og risikoforståelse
- Ledelsens rolle i opplæring og bevissgjøring

4.2.2.1 Fragmenterte ansvarsområder

Alle sektorene forteller om fragmenterte og til dels uklare ansvarsområder når det kommer til digital sikkerhet. Dette er kanskje ikke så rart i og med at utvikling av sikre teknologiske systemer krever inngående kunnskap og kompetanse innen IT, og dermed er noe som naturlig har tilfalt IT-avdelingene i virksomhetene. Samtidig har vi sett at holdningene til digital sikkerhet har båret preg av å ha hatt fokus på de rent tekniske løsningene, og at det menneskelige aspektet dermed har kommet litt i skyggen av dette. Ifølge Daniel

(justissektoren) har dette ført til uklare ansvarsforhold, spesielt med tanke på opplæring og bevisstgjøring:

> Det er litt uklare ansvarsforhold, spesielt når det kommer til dette med opplæring og hvem som har myndighet overfor de ansatte til å drive med det. Vi sitter med fagkompetansen innen IKT-sikkerhet, men vi sitter ikke med noe opplæringsansvar overfor medarbeiderne generelt. (Daniel, justissektoren).

Trine sier at dette er en vanlig problemstilling i flere organisasjoner, og påpeker viktigheten av å ha et koordinerende miljø for å få ting til å flyte bedre:

> Vi sliter litt organisatorisk med at virksomheten har sitt eget IT-miljø som har ansvaret for sin del, også sitter vi med noen forhold som kanskje berører både oss og dem og da kan det blir noen utfordringer. Men mange organisasjoner har veldig mange oppdelte miljøer, og da kan det være lurt å ha en koordinerende enhet som får støtte fra ulike fagmiljøer. (Trine, finanssektoren).

Camilla fra kraftsektoren er på sin side mer positiv i sin omtale av delingen av ansvarsområder, og trekker frem godt samarbeid som nøkkelen til dette:

> Det er egentlig konsernet som har fokus på den menneskelige biten, det er de som i hovedsak jobber ut mot de ansatte. Men vi har veldig godt samarbeid på tvers av selskapene, så jeg jobber mye med de som jobber med sikkerhet i konsernet om hvordan vi skal forbedre bevisstheten til de ansatte. (Camilla, kraftsektoren).

Camilla påpeker samtidig at de er et relativt lite selskap, noe hun mener fremmer et godt samarbeid på tvers av enhetene til tross for oppdelte ansvarsområder. Knut (justissektoren) forteller derimot at deres avdeling må ta unna «alt», og at de rett og slett sitter med for mye ansvar fordi de både må jobbe med det strategiske samtidig som de også må ta det operative som å håndtere varsler fra ansatte om e-poster og liknende. Han understreker derfor at de hele tiden er nødt til å foreta prioriteringer på hva som haster mest.

> Vi jobber på en måte på dugnad, hvor vi prøver å ta unna det som kommer inn. Utfordringen er å både jobbe med det strategiske samtidig som du skal svare på alle e-postene fordi folk har trykket på en link. Sikkerhet blir ofte en flaskehals, og vi må bare klare å prioritere hva som må besvares raskest. (Knut, justissektoren).

Det er altså problemer knyttet både til det å ha uklare ansvarsområder og det å ha for mye ansvar, og en klar strategi og policy for digital sikkerhet vil være med på å avklare dette i større grad slik at man unngår disse utfordringene.

Oppsummering fragmenterte ansvarsområder

Digital sikkerhet har nok lenge vært et felt som har tilhørt IT-avdelingene i de respektive virksomhetene, naturlig nok i og med at fokuset har vært på teknologiske løsninger. Etter hvert som søkelyset på den menneskelige faktoren gradvis har økt, har det imidlertid oppstått uklarheter rundt hvem som har ansvaret for hva, spesielt med tanke på opplæring og bevisstgjøring av de ansatte. Trine fra finanssektoren trekker frem det å ha et koordinerende miljø som løsning på problemet, mens Camilla fra kraftbransjen mener størrelsen på selskapet spiller inn på hvor godt samarbeid man klarer å ha. Jeg trekker også dette videre og ser det i sammenheng med det som blant annet ble nevnt tidligere av informantene i kraftsektoren, nemlig mangel på fokus og strategi for digital sikkerhet. Får man dette på plass er det også mer sannsynlig at ansvarsområdene blir klarere, at man får et bedre samspill på tvers av avdelingene, samt at man slipper at enkelte avdelinger blir overarbeidet på grunn av for mye ansvar.

4.2.2.2 Ledelsens holdninger og risikoforståelse

Hvilke holdninger ledelsen har til digital sikkerhet påvirker gjerne også risikoforståelsen deres. Samtidig påvirker ledelsens holdninger også hvordan de ansatte ser på ting, da ledelsen er med på å sette søkelyset på det de mener er viktig og bør prioriteres. Og nettopp prioriteringer er noe som flere av informantene trekker frem som veldig relevant for arbeidet med digital sikkerhet, og de påpeker at ledelsens holdninger og bevissthet er direkte knyttet opp mot bevilgninger og ressurser.

> Det er kjempeviktig at vi har et konsernstyre og styrer i selskapene som faktisk er bevisst på at dette må være et satsningsområde, og at det ikke skal være noen problemer med å få bevilgninger til å bruke penger på tiltak innenfor området. (Mads, kraftsektoren).

Både Knut, Lars og Daniel fra justissektoren forteller at deres avdeling har fått et betydelig løft det siste året, blant annet med økt bemanning. Dette skyldes at ledelsen har fått økt fokus

på digital sikkerhet og økt forståelse for hvilke trusler og farer man faktisk står overfor. Daniel oppsummerer dette med å peke på viktigheten av ledelsens holdninger:

> Holdningene til ledelsen er så viktig, for det er de som sitter på rammebetingelsene og det er de som kan ansette folk, skaffe penger til systemer og liknende. IKT-sikkerhet er absolutt ikke gratis, så det kommer ikke av seg selv. (Daniel, justissektoren).

For å kunne påvirke ledelsens holdninger til digital sikkerhet, og dermed også øke sjansene for større bevilgninger, må imidlertid risikoen og truslene man står overfor synliggjøres og kommuniseres til ledelsen. Så godt som alle informantene trakk frem dette som et sentralt poeng, og alle var enige i at det å klare å kommunisere truslene de står overfor er avgjørende for å øke ledelsens forståelse. De fleste forteller at de regelmessig oppdaterer ledelsen på trusselbildet, men tre av informantene nevner noe jeg finner spesielt interessant. Stian fra finanssektoren sier at noe av utfordringen med å kommunisere risiko innen digital sikkerhet er at cyberdomenet oppleves veldig lite håndfast for mange, og at dette gjør at de ikke klarer å se de truslene de står overfor. Han legger derfor vekt på at informasjonen må legges frem på en pedagogisk og konkret måte slik at det blir lettere for dem å forstå hva det er snakk om.

> Jeg tror at mange sliter med å forholde seg til cyberrisiko fordi det er så lite håndfast. Tar du derimot en litt mer tradisjonell tilnærming til det og viser helt konkret hvilke aktører det er som utgjør en risiko, hvordan de jobber og hvordan de har klart å komme seg inn i andres systemer, så er det mye lettere å forstå hva cyberrisiko er. Så det er i bunn og grunn en kommunikasjonsutfordring å øke forståelsen hos ledelsen. (Stian, finanssektoren).

Thomas (finanssektoren) peker på sin side på utfordringer internt i sikkerhetsmiljøet, hvor det er ulike meninger om ønsket sikkerhetsnivå og hvor de er i dag. Slike uenigheter internt gjør det vanskelig å tydeliggjøre overfor ledelsen hva man faktisk trenger, og dermed blir sikkerheten svakere enn den burde være. «På enkelte områder er sikkerheten svakere enn den burde være, men på grunn av delte meninger innad i sikkerhetsmiljøet har ikke det blitt kommunisert opp på en hensiktsmessig måte.» (Thomas, finanssektoren).

Det å klare å kommunisere risiko på en god og fornuftig måte er også utfordrende for justissektoren. Det er ingen tvil om at det i en byråkratisk organisasjon kan være vanskelig å nå frem til ledelsen på toppen – informasjonen skal gå gjennom mange ulike nivå, og gjennom flere ulike personer. Daniel (justissektoren) sier at dette har stor betydning for hvilken forståelse ledelsen til syvende og sist blir sittende med:

> For hvert nivå du går opp i en organisasjon, så er det et filter. Og jo flere nivåer du har, desto mer filtreres kommunikasjonen og jo mindre kommer frem. Det fører til at vi sitter og vet at ting er annerledes enn det ledelsen står og prater om, men på grunn av det hierarkiske systemet har vi ikke nådd frem med beslutningsgrunnlaget. (Daniel, justissektoren).

Daniel forteller også at ulike rapporter har kommet med kritikk og påpekt viktigheten av at virksomheten sikrer IKT-systemene, og at det virker å ha gått opp for ledelsen at de må gjøre noe. Han peker imidlertid samtidig på et annet veldig viktig poeng, nettopp om dette skyldes en genuin forståelse av at IKT-systemer er sårbare og må beskyttes, eller om det bare er fordi de har fått kritikk i en rapport. Dette kan underbygges av det Knut fra samme sektor sier, hvor han kommer med et konkret eksempel på at øverste ledelse i sektoren åpenbart ikke har forstått kompleksiteten og sårbarheten i de digitale systemene:

> Enkeltpersoner i ledelsen mente at det var så tungvint å bruke to-faktor pålogging for å se kalenderen på mobilen, at de absolutt ønsket å få den overført til deres personlige mobil. Man er så vant til det man kan gjøre på egen pc og mobil at mange mangler forståelse og aksept for at en slik smidig dataoverførsel mellom virksomhetens kalendersystem og private mobiler kan utgjøre en sårbarhet. Det er nettopp slike smidige, men ikke godt nok sikrede e-post og kalenderløsninger som ble utnyttet i angrepene på Stortinget. (Knut, justissektoren).

Knuts formulering gir meg et tydelig inntrykk av en frustrasjon over manglende forståelse fra den øverste ledelsen, og at dette gjør arbeidet med digital sikkerhet ekstra krevende. Trine (finanssektoren) viser noe av det samme når hun forteller om enkelte ledere som mener at det opplegget de i utgangspunktet må gjennom for å øke bevisstheten, er noe de ikke forstår viktigheten av og som de mener ikke gjelder dem selv: «Min erfaring er at mange ledere rundt omkring tenker at «nei, det der er noe som de ansatte skal gjøre, det der har ikke jeg tid til».» (Trine, finanssektoren). Dette ser jeg på som et paradoks da Mads (kraftsektoren) påpeker nettopp det at det er de på toppen som ofte er mest utsatt da det er de som sitter på viktige tilganger og har navn og kontaktinformasjon liggende ute på nettsidene til de respektive selskapene. Samtidig er det kanskje ikke å forvente at ledere som ikke jobber med sikkerhet fullt ut skal forstå omfanget og viktigheten av sikkerhet, men Thomas (finanssektoren) påpeker at enkelte ledere bevisst tar mer risiko enn det de kanskje burde gjort:

> Jeg tror det er mange ledere som er villig til å ta litt risiko på noe de tror det er veldig lav sannsynlighet for at skal skje, fremfor å bruke masse tid på sikkerhet hvis de stort sett tenker at det går fint og at de måles på helt andre ting. (Thomas, finanssektoren).

Også her gjør altså motsetningene mellom sikkerhet og forretning seg gjeldende, men heldigvis påpeker mange av informantene at de ser en positiv utvikling når det kommer til ledelsens forståelse av digital sikkerhet.

Oppsummering ledelsens holdninger og risikoforståelse

Ledelsens holdninger kan direkte påvirke arbeidet med digital sikkerhet gjennom hva som blir prioritert og hvor mye penger og ressurser som tildeles de som jobber med det. For å sørge for gode holdninger blant lederne er det avgjørende at man klarer å kommunisere risikoen og truslene man står overfor på en god og saklig måte, spesielt siden digital sikkerhet er lite håndfast og til dels ukjent for mange. Det er imidlertid ikke alltid like lett å nå gjennom med den informasjonen man sitter med, hvert fall ikke hvis man jobber i en byråkratisk organisasjon. Da vil informasjonen bli filtrert og justert mellom hvert nivå man skal gjennom, noe som gjør at beslutningsgrunnlaget blir manglende eller i verste fall feil. Manglende forståelse kommer også til uttrykk gjennom holdninger som at ledere ikke har tid til å gjennomføre opplæring, og at de er villige til å ta større risiko enn de burde gjøre fordi de ikke blir målt på sikkerhet.

4.2.2.3 Ledelsens rolle i opplæring og bevisstgjøring

Som jeg allerede har vært inne på vil ledelsens holdninger generelt påvirke de ansattes oppfatninger av hva som er viktig i virksomheten. Hvordan ledere forholder seg til digital sikkerhet og det opplegget som kjøres for opplæring og bevisstgjøring vil ha stor betydning for oppslutningen rundt disse tiltakene, og mange av informantene påpeker viktigheten av at ledelsen går foran som gode rollemodeller:

> Vi har mye fokus på å snakke med ledelsen og presentere trusselbildet og hva vi må fokusere på. Sånn sett har vi fått et godt fokus høyt oppe, og det er der vi må starte. Så må vi dra det nedover til alle ansatte. (Camilla, kraftsektoren).

«Det gjelder å prøve å få litt gehør hos toppledelsen, for å bruke de litt som bjellesauer.» (Thomas, finanssektoren).

> Vi var litt heldige, for finansdirektøren i konsernet klarte å gå på en falsk e-post en gang. Men hun skjønte hva det var og fikk stoppet det ganske greit fordi hun sa ifra. Og da har vi brukt det som eksempel for andre ansatte – hvis ikke hun er redd for å si ifra må det gjelde alle andre også. (Mads, kraftsektoren).

Dette viser at informantene har skjønt hvor viktige ledelsen er når det kommer til holdningsskapende arbeid, og at man kan få mye igjen hvis de er med på laget og sprer gode holdninger videre. Det er imidlertid ikke alle som har positive erfaringer med dette, og Knut fra justissektoren forteller om et eksempel som høyst sannsynlig også gjelder flere andre virksomheter og organisasjoner:

> Vi hadde en phishing-kampanje i fjor, men vi fikk ikke lov til å sende ut det i år. Jeg fikk inntrykk av at det var de ulike sikkerhetslederne rundt omkring som stoppet det. Jeg vet ikke helt hvorfor, men jeg har en sterk mistanke om at noen av dem var flaue fordi de selv gikk på det. Så da kan man jo stille spørsmålstegn ved hvor godt de forstår det faktiske problemet. (Knut, justissektoren).

Dersom ledelsen selv ikke skjønner viktigheten av eller poenget med tester som faktisk er med på å måle hvor god virksomheten er på digital sikkerhet, vil dette mest sannsynlig også gjelde for mange av de ansatte. Ledelsen har uten tvil en stor påvirkningskraft, og da er det viktig at de ikke setter sin egen frykt for å tape ansikt foran virksomhetens sikkerhet.

Oppsummering ledelsens rolle i opplæring og bevisstgjøring

Klarer man å oppnå en genuin forståelse blant lederne for viktigheten av arbeidet med opplæring og bevisstgjøring innen digital sikkerhet, kan man utnytte dette ved å bruke dem som såkalte «bjellesauer» for resten av organisasjonen. Det er imidlertid ikke alltid at dette er tilfelle, og noen ganger kan de til og med stikke kjepper i hjulene for de som driver med dette ved å hindre dem i å gjennomføre ulike tiltak for å øke bevisstheten blant de ansatte. Dette er svært uheldig da det både begrenser muligheten for å øke forståelsen for digital sikkerhet, men også at man skaper en kultur hvor det å lære ikke blir verdsatt. Dette er noe jeg vil gå nærmere inn på i neste del av oppgaven.

4.2.2.4 Oppsummering ledelse

Tidligere har digital sikkerhet i stor grad vært noe som har tilhørt IT-avdelingene rundt om i virksomhetene. Etter hvert som den menneskelige faktoren har fått større fokus, har dette ført til uklarheter rundt ansvaret for den digitale sikkerheten, spesielt når det kommer til opplæring og bevisstgjøring. Dette kan igjen ha en sammenheng med manglende fokus og strategi for digital sikkerhet. Teorien legger stor vekt på ledelsens forpliktelse til sikkerhet i arbeidet med å skape en god sikkerhetskultur, og ledelsens holdninger og risikoforståelse er derfor veldig viktig for å få prioritert dette feltet. Flere av informantene peker imidlertid på ulike kommunikasjonsutfordringer når det kommer til det å få formidlet riktig og relevant informasjon om det faktiske trusselbildet de står overfor. Dette kan i sin tur føre til at ledere tar mer risiko enn de burde gjort, både bevisst og ubevisst. Videre har ledelsen en viktig rolle som forbilder og agendasettere i egen virksomhet, og det å bruke de som «bjellesauer» i arbeidet med bevisstgjøring og opplæring kan være svært nyttig. Dette krever imidlertid en ledelse som er opptatt av åpenhet og læring, noe som dessverre ikke alltid er tilfellet. Jeg vil i det neste kapittelet presentere funn om varsling fra ansatte og læring i organisasjonen.

4.2.3 Varsling og læring

For å kunne lære av egne og andres feil er det avgjørende at man er åpen og deler informasjon på tvers av både avdelinger og virksomheter. Innen digital sikkerhet står de fleste overfor samme type utfordringer, og som jeg har nevnt tidligere har alle virksomhetene fått mer fokus på digital sikkerhet gjennom at andre organisasjoner har blitt utsatt for ulike typer angrep. Det er derfor av stor nytte at det legges til rette for varsler fra egne ansatte om feil og svakheter de oppdager, og at disse varslene kan settes i et system for å tilrettelegge for videre læring. Følgende underkategorier vil bli presentert:

- System for å varsle
- Kultur for å varsle
- Læring

4.2.3.1 System for å varsle

Alle virksomhetene har et visst system for varsling fra de ansatte, men det varierer i hvor stor grad dette virker etter hensikten. Både finanssektoren og kraftsektoren forteller at de har egne

rutiner og et eget system for rapportering av for eksempel phishing-mail, mens justissektoren på sin side sier at dette må varsles via brukerstøtten eller direkte kontakt til de som sitter som rådgivere eller som jobber med teknisk sikkerhet. «Vi har både aktiv brukerstøtte og direkte kontakt til oss som mulighet for å varsle. Og vi prøver å kontinuerlig være flinke på å informere om at disse kanalene eksisterer og minne folk på om at vi fins.» (Lars, justissektoren). Denne uttalelsen gir meg inntrykk av at det ikke finnes noe konkret system for å varsle, men at det er avhengig av at den enkelte tar seg tid til å sende en mail eller ringe til brukerstøtten. Det at de prøver å være flinke på å informere om hvor det skal varsles viser også at de ikke har noen innarbeidede rutiner på dette, men at det blir litt mer tilfeldig når og om det varsles. Samtidig sier Knut fra samme sektor at det er såpass mange som sier ifra at de ikke har kapasitet til å håndtere alle henvendelsene, men kobler dette også opp mot for dårlig bemanning og organisering.

> Det er nok folk som sier ifra til at vi ikke har kapasitet til å håndtere det som kommer inn. Vi må få bruker- og kundeservice til å i større grad håndtere det grunnleggende, for vi har ikke kapasitet til å besvare alle. (Knut, justissektoren).

Både Stian, Thomas og Trine fra finanssektoren sier på sin side at noe av utfordringen er at det må være enkelt å varsle, og at det må være et lavterskeltilbud. I en ellers travel arbeidshverdag er det viktig at det å melde ifra om feil og uønskede hendelser ikke oppleves som merarbeid. «Ansatte og brukere må vite hvor de skal varsle. Og at det er enkelt å varsle, at det ikke blir en høy terskel for det.» (Trine, finanssektoren). Stian (finanssektoren) forteller at de akkurat har satt i drift en såkalt sikkerhetsportal som er nettbasert og hvor brukerne kan gå inn og melde fra om ulike hendelser. Han påpeker at dette har gjort det enklere både for brukerne og de som mottar henvendelsene: «Tidligere måtte man melde inn ting på mail, men nå er det litt enklere å få ting inn i systemet. Det fører til bedre sporbarhet og lavere terskel for å mede inn uønskede hendelser.» (Stian, finanssektoren).

Selv om man legger til rette for at det skal være enkelt å varsle om uønskede hendelser, trekker Stian (finanssektoren) likevel frem et viktig poeng: «Det er forskjell mellom det målte nivået og det reelle nivået. I et stort konsern vil det alltid være underrapportering av slike hendelser, så da må vi forsøke å ettergå det og finne ut hvor rapporteringen har stoppet.» (Stian, finanssektoren). En mulig forklaring på dette kan være det som Camilla (kraftsektoren) forteller om en travel arbeidshverdag hvor ting som dette fort kan gå i glemmeboka:

> Jeg tror nok mange ville ha sagt ifra hvis de plutselig åpnet et vedlegg som så litt spesielt ut. Men fordi det ikke nødvendigvis skjer noe med pcen der og da, er det fort gjort å glemme å varsle om det. De fleste har en travel hverdag, og kanskje var de på vei inn i et møte og glemte det etterpå. (Camilla, kraftsektoren).

Dette er nok litt av utfordringen med digital sikkerhet og digitale trusler og angrep. Det er ikke alltid det skjer noe med en gang, og ofte er det heller ikke synlig for den enkelte ansatte at noen har kommet seg inn via brukeren deres og fått tilgang til ulike systemer. Hvis man da ikke har kunnskapen eller bevisstheten til å forstå dette er det også større sannsynlighet for at man glemmer eller ikke tenker på å varsle.

Oppsummering system for å varsle

Flere av infomantene påpeker at det må være enkelt å varsle, noe som mest sannsynlig vil føre til at flere velger å melde ifra om uønskede hendelser. De fleste har en travel arbeidshverdag og da er det ikke alltid man verken husker eller tenker på at man burde sende en mail eller ringe noen for å si ifra om noe man gjorde eller oppdaget. Finanssektoren virker å ligge lengst fremme når det kommer til dette gjennom å ha utarbeidet et nettbasert system hvor man raskt og enkelt kan trykke seg gjennom noen punkter som så sendes videre til riktig avdeling for oppfølging.

4.2.3.2 Kultur for å varsle

I tillegg til å ha et godt system for å varsle, er det også viktig at de ansatte opplever det som trygt og greit å si ifra. Det å skape en slik kultur er viktig både for å sikre at man i større grad fanger opp det som skjer der og da, men ikke minst for å legge til rette for videre læring. Flere av informantene påpeker at redsel og frykt er noe som ofte er knyttet til det å gjøre feil, og at det er denne holdningen man må prøve å endre for å få til en god varslingskultur.

> Vi forsøker å skape en kultur hvor det er greit å bli lurt, men det er ikke greit å ikke si ifra. Hvor godt vi får det ut i organisasjonen er litt mer vanskelig å si, men det enkle svaret er at du aldri når nok ut til at du kan være helt fornøyd. (Stian, finanssektoren).

«Jeg tror folk blir mindre og mindre redde for å si ifra.» (Mads, kraftsektoren).

> Vi prøver å predikere at man skal ha lav terskel for å si ifra, at alle kan dumme seg ut og trykke på noe de ikke burde ha gjort, og at man heller da sier ifra enn å tenke at det sikkert går bra. Det er et budskap det kan være vanskelig å få inn og som man må jobbe med over tid. (Trine, finanssektoren).

Det er spesielt interessant å se at det innad i finanssektoren fremstår som ekstra vanskelig å nå ut til alle med denne holdningen, blant annet på grunn av sterke profesjonskulturer. Trine og Stian trekker frem dette som en klar utfordring: «Det er veldig flinke folk som jobber her, på økonomiområdene er de best i klassen fra universitet og høyskoler og de er vant til å være sånne «flinkiser». Og de er ikke så glade i å gjøre feil». (Trine, finanssektoren).

> Det fins jo enkelte miljøer hvor du vet at incentivstrukturen er lagt opp slik at det skal veldig mye til at folk melder inn at de har gjort feil, for da får de kanskje ikke den bonusen på en million. Der kan du jobbe mye og lenge uten nødvendigvis å nå gjennom. (Stian, finanssektoren).

Selv om disse profesjonskulturene står veldig sterkt i deres virksomhet, nevner også Camilla fra kraftsektoren det faktum at mange kan bli litt fornærmet hvis de har trykt på noe de ikke skulle, og at dette igjen kan hindre dem i å si ifra. Det er nok naturlig for de fleste mennesker å ikke like å gjøre feil, så det å prøve å snu denne holdningen kan være vanskelig da det rokker ved en ganske grunnleggende holdning. Ser man dette i sammenheng med ledelsens rolle når det kommer til bevisstgjøring og holdningsendring, viser Mads (kraftsektoren) hvordan ledelsen kan bidra til en god varslingskultur ved å gå foran som gode eksempler:

> Vi var litt heldige da, for finansdirektøren i konsernet klarte å gå på en falsk e-post en gang. Men hun skjønte hva det var og fikk stoppet det ganske greit fordi hun sa ifra. Og da har vi brukt det som eksempel for andre ansatte – hvis ikke hun er redd for å si ifra må det gjelde alle andre også. (Mads, kraftsektoren).

Ledelsen har altså stor betydning for hvordan de ansatte velger å forholde seg til det å varsle om feil man har gjort. Og selv om ledelsen selv kanskje ikke gjør noen personlige feil, er det likevel viktig at de fronter hvor viktig det er å si ifra.

Oppsummering kultur for å varsle

Det er interessant å se hvor mange av informantene som er opptatt av det å skape et godt klima for å si ifra om man har gjort noe feil, men de påpeker samtidig at det til tider også kan

være vanskelig å nå ut med dette i hele organisasjonen. Både Trine og Stian (finanssektoren) understreket dette med å vise til en sterk profesjonskultur innad i økonomi- og forretningsmiljøene hvor det å gjøre feil ikke blir akseptert. Som jeg har vært inne på tidligere består en virksomhet i større grad av flere subkulturer enn én felles kultur, og det å da skulle skape en felles varslingskultur på tvers av alle disse gjør at man må jobbe kontinuerlig og målrettet over ganske lang tid. I tillegg vil også ledelsen ha stor innvirkning hvis de går foran som gode eksempler dersom de har gjort en «feil».

4.2.3.3 Læring

Læring er i stor grad basert på at man er åpen og deler erfaringer om ting man opplever og har blitt utsatt for. I og med at digital sikkerhet er et såpass nytt felt for mange betyr dette at samarbeid både internt og eksternt er en viktig faktor. Alle virksomhetene trekker frem de ulike CERT-ene innenfor egen bransje som et forum hvor det deles informasjon. Det er imidlertid likevel ikke et uttalt fokus på *læring*, og dette er dermed ikke satt i system. Camilla fra kraftsektoren sier følgende:

> Når det skjer en hendelse tror jeg mange har en tendens til å drive brannslukking helt til alt er bra igjen, også stopper man der. Men det er jo da man har en kjempemulighet til å lære av det som har skjedd – se på hva som gikk galt og hvordan man kan forbedre seg. Det er de prosessene vi jobber mye for å få på plass nå. (Camilla, kraftsektoren).

Det å ta vare på de mulighetene man har for læring *etter* at en hendelse har inntruffet, er viktig for å være bedre forberedt neste gang. Men for å kunne lære av en hendelse må man også dele erfaringer. Både Mads og Steinar fra kraftsektoren trekker frem at det varierer i hvilken grad ulike virksomheter er villig til å dele informasjon om uønskede hendelser de har vært utsatt for.

> Jeg har inntrykk av at erfaringsdelingen blir bedre og bedre. Vi har nok vært litt foregangs innen vår sektor og fortalt om det vi opplever, men første gangen jeg på en samling fortalte om et virus vi hadde hatt i et kraftverk, fikk jeg reaksjoner på at andre ikke hadde turt å fortelle det dersom det hadde vært dem. (Mads, kraftsektoren).

Mens Mads forteller om noe jeg tolker som en slags frykt for å være åpen om feil man har gjort, forteller Steinar at han opplever at det både kan skyldes flauhet og det faktum at man er en samfunnskritisk funksjon som har mye taushetsbelagt informasjon:

> Jeg tror det er en kombinasjon av at man har informasjon som er taushetsbelagt, og at man kanskje også er litt flau fordi det viser at man ikke har hatt god nok kontroll og mange føler kanskje at de ikke har gjort jobben sin godt nok. (Steinar, kraftsektoren).

Lars (justissektoren) er derimot klar på at han ikke mener at det er flauhet som er grunnen til at noen ikke vil dele informasjon, men heller det som også Steinar nevner om taushetsbelagt og kritisk informasjon: «Min oppfatning er definitivt at man velger å ikke dele informasjon fordi man faktisk har en sikkerhetsbekymring med tanke på å dele for mye, enn at det skyldes at man er flau over det som har skjedd.» (Lars, justissektoren). Lars påpeker altså at man må være litt kritisk med tanke på å dele for mye informasjon da dette også er noe som kan bli misbrukt. Han opplever samtidig at privat sektor deler mer aktivt enn det statlige organer gjør, og da spesielt de som ligger under justissektoren. Han sier at deres virksomhet kanskje er mer restriktiv med dette på grunn av at de er mer bekymret for skadevirkningene rent sikkerhetsmessig sett. Samtidig mener har at det er god kommunikasjon på tvers av både etater og sektorer, og at det finnes gode kontaktpunkter for å dele informasjon, uten at han ønsker å utdype dette noe mer.

Åpenhet er dermed noe som kanskje er en større utfordring for samfunnskritiske funksjoner enn andre med tanke på det faktum at man sitter på mye informasjon som ikke uten videre kan deles med andre. Samtidig er det interessant å se at det kun er kraft- og justissektoren som nevner dette, mens informantene fra finanssektoren selv sier at de er ganske åpne når det kommer til hvilke trusler og angrep de opplever. Dette samsvarer altså med den opplevelsen Lars (justissektoren) sitter med, og Thomas fra finanssektoren påpeker viktigheten av å dele erfaringer med andre som blir utsatt for mye av det samme: «Vi deler definitivt informasjon med FinansCERT og de andre bankene, for vi ser jo at vi blir angrepet av de samme trusselaktørene og da er det viktig å dele erfaringer rundt angrepsmetoder og liknende.» (Thomas, finanssektoren). Steinar (kraftsektoren) påpeker på sin side at de gjerne kan dele informasjon, men at det da er viktig at informasjonen ikke spres videre. «Jeg mener det er viktig å dele informasjon, læring krever at vi er åpne om ting. Men da må alle være med på det og det må være i et lukket forum.» (Steinar, kraftsektoren).

Det virker altså som om finanssektoren i større grad har etablert bedre rutiner for informasjons- og erfaringsdeling, men at både kraftsektoren og justissektoren viser en positiv holdning til dette med de restriksjoner som må være på plass for å beskytte viktig informasjon.

Oppsummering læring

Alle virksomhetene forteller at de deler informasjon om digitale hendelser både internt og eksternt, men at det ikke er satt i noe system for å sikre læring. Selv om mine informanter ser verdien av å dele erfaringer, påpeker både Mads og Steinar (kraftsektoren) at frykt og flauhet hindrer mange i å ønske å dele informasjon om hendelser de har vært utsatt for. Samtidig blir det også poengtert av både justis- og kraftsektoren at åpenhet kan være en utfordring på grunn av at dette gjerne er taushetsbelagt informasjon som de ikke alltid ønsker å gå ut med. Lars (justissektoren) påpeker at slik informasjon bevisst kan bli misbrukt og at de dermed er mer restriktive med tanke på det å dele opplysninger om trusler og angrep. Finanssektoren er på sin side mer åpen og begrunner dette med at man stort sett står overfor de samme trusselaktørene og -metodene, og at det derfor er viktig å dele erfaringer for å forhindre angrep. For de andre sektorene kan dette utnyttes bedre hvis det blir mer aksept for å være åpen om det man opplever, og at alle er innforstått med at det som deles blir innenfor den gruppa. Læring knyttes selvfølgelig også opp mot selve opplæringen, men det vil jeg gå inn på senere i kapittelet.

4.2.3.4 Oppsummering varsling og læring

For at ansatte skal gidde å ta seg tid til å varsle må det være et enkelt og raskt system slik at det blir lav terskel for å si ifra om uønskede hendelser. De fleste har stort sett en travel arbeidsdag, og dersom det å varsle blir noe som krever lang tid vil det ikke bli gjennomført. Samtidig er det også utfordrende å klare å skape en varslingskultur på tvers av hele virksomheten, mye på grunn av sterke profesjonskulturer innad i organisasjonen som har andre verdier og dermed ikke ser nytten av å melde ifra. Ledelsen vil være en viktig brikke i dette arbeidet dersom de går foran med gode holdninger og ikke er redd for å si ifra selv dersom de har gjort en feil.

Åpenhet kan være en utfordring innen samfunnskritiske funksjoner på grunn av mye taushetsbelagt informasjon som kan misbrukes dersom det kommer i feil hender. Samtidig mistenker også flere at frykt og flauhet er viktige grunner for at noen ikke vil dele erfaringer. Dette kan nok henge sammen med hvilken kultur man har innad i virksomheten, og om åpenhet og erfaringsdeling er verdier man prioriterer og fremmer i organisasjonen. Får man imidlertid på plass et godt system for varsling, samt klarer å nå ut til de fleste for å skape en god varslingskultur, er det også lettere å bli en lærende organisasjon som i større grad ser viktigheten av å dele informasjon både internt og eksternt. Som Thomas (finanssektoren) påpeker står man innenfor samme sektor stort sett overfor de samme trusselaktørene, og erfaringsdeling vil derfor være svært viktig for å forhindre fremtidige angrep.

4.2.4 Sikker atferd

Selv om man har mange krav, rutiner og prosedyrer som sier hvordan man skal handle, er det ingen garanti for at de ansatte faktisk følger dem og handler på en sikker måte. «Jeg vil si at vår største utfordring er at man har masse sikkerhetskrav, også er det å få folk til å faktisk etterleve kravene.» (Stian, finanssektoren). Dette utsagnet viser til en utfordring som høyst sannsynlig også gjelder andre virksomheter og organisasjoner. Sikkerhet oppleves som tidligere nevnt ofte som merarbeid og et hinder for effektivt arbeid. En sikker atferd krever ifølge Daniel (justissektoren) derfor en forståelse for både truslene og tiltakene som iverksettes:

> Hvis ikke brukerne opplever tiltakene som hensiktsmessige, så bypasser de dem heller. Målet vårt er derfor å forklare litt rundt det, slik at folk forstår hva som er hensikten med tiltakene våre. På den måten tror vi at det er større sjanse for at de velger å følge dem selv om det oppleves litt tungvint iblant. (Daniel, justissektoren).

Disse utsagnene viser noe av problemstillingen med sikkerhetstiltakene som blir iverksatt for å bedre den digitale sikkerheten, nemlig en manglende forståelse for risikoen man står overfor. Lars (justissektoren) sammenlikner det å ha en usikker atferd på nett med det å pusse et våpen eller håndtere en hammer, og påpeker at man burde ha samme holdning til begge deler fordi det kan få fatale konsekvenser dersom man er uforsiktig:

> Hvis du er jeger og skal pusse rifla di, så sitter du ikke med ansiktet nedi løpet. På samme måte skal du ikke klikke på alle linker du ser og laste ned alle vedlegg du får heller. (…) Og digital sikkerhet for meg er det samme som å forstå at en datamaskin er

> potensielt farlig, akkurat som en hammer kan være et verktøy eller det kan være et våpen. (Lars, justissektoren).

Thomas (finanssektoren) sier på sin side at de veier opp for en potensiell uforsiktig atferd med å sette inn tekniske tiltak som at ansatte blir tvunget til å klassifisere dokumenter og mailer som sendes. Han mener at dette også er med på å øke bevisstheten til den ansatte om hva som er sensitiv informasjon som må beskyttes.

> Sånn som det er nå så må hver eneste mail klassifiseres før du får sendt den. Det er sånne ting jeg har veldig tro på; en kombinasjon av tekniske tiltak og det å tvinge menneskene til å ta stilling og være mer bevisste. (Thomas, finanssektoren).

Dette er noe som Steinar fra kraftsektoren sier at de er i ferd med å innføre hos dem også, og han mener også at dette vil være med på å øke bevisstheten til de ansatte. Samtidig sier Stian (finanssektoren) at man ofte kanskje ikke tar innover seg brukerperspektivet når man utvikler de sikre systemene og løsningene, og at dette gjør at brukerne i større grad opplever tiltakene som unødvendige og tungvinte. Lars (justissektoren) og Daniel (justissektoren) trekker også frem dette og påpeker at det ofte kan være en vanskelig vurdering: «(…) brukervennlighet og sikkerhet er jo to motsatte dyr, de er jo ikke det samme i det hele tatt.» (Lars, justissektoren). «Det er viktig det der altså, for blir ting lite brukervennlig så finner man andre måter å bypasse de sikkerhetsmekanismene på, og da er resultatet at du får dårligere sikkerhet.» (Daniel, justissektoren). Dette viser dermed at man ikke bare kan sette inn tiltak for å bedre sikkerheten uten å også vurdere hvordan det blir mottatt av brukerne og hvordan det fungerer i praksis.

Knut (justissektoren) påpeker i tillegg at de ansatte virker å være bekymret, men at de samtidig bruker det samme passordet til flere tjenester. Han stiller derfor spørsmålstegn ved hvorvidt den økte bevisstheten faktisk har ført til sikrere atferd:

> Folk har et generelt bekymringsnivå, men så er de usikre på om de kan gjøre noe med det og bruker det samme passordet til alt. Så det at den bevisstheten faktisk har ført til handling, det er jeg usikker på. (Knut, justissektoren).

Han påpeker også noe veldig interessant idet han sier at de er «usikre på om de kan gjøre noe med det». Dette kan kobles opp mot følelsen av kontroll og det å til en viss grad kunne styre og påvirke omgivelsene våre, et såkalt aktør/brikke-perspektiv. Både Camilla (kraftsektoren) og Stian (finanssektoren) påpekte tidligere at mange opplever digital sikkerhet som noe

fremmed og skremmende, og det er dermed ikke usannsynlig at denne følelsen kan ha direkte påvirkning på de ansattes faktiske atferd fordi de føler at det som skjer i «cyberdomenet» er utenfor deres kontroll og at det derfor ikke spiller noen rolle hva de egentlig gjør.

4.2.4.1 Oppsummering sikker atferd

Som så mye annet jeg har vært inne på kan også sikker atferd knyttes til kulturen(e) i virksomheten, fordi de uformelle verdiene som eksisterer innad i en subkultur ofte kan veie tyngre enn skrevne regler, instrukser og krav som blir satt. Sikker atferd krever derfor at forståelsen for digital sikkerhet og ulike sikkerhetstiltak økes slik at tiltakene følges selv om det oppleves tungvint. Samtidig er man også nødt til å tenke på de som faktisk skal bruke systemene, og se på hvordan de sikre løsningene fungerer i praksis. Ser man dette i sammenheng med at produksjon ofte trumfer sikkerhet, kan det være en fordel at de sikre løsningene som blir installert blir utviklet i samarbeid med de som skal bruke systemene, slik at det blir tatt mest mulig hensyn til brukervennlighet samtidig som forståelsen for tiltakene også kanskje øker. Men er det nok å øke forståelsen? Knut (justissektoren) påpeker at folk er bekymret, men at de er usikre på om de kan gjøre noe med det, og på grunn av det fortsetter å ha en usikker atferd. Cyberhendelser er noe nytt og til dels skremmende for veldig mange, og derfor også noe som kan føles å være utenfor deres kontroll. Ifølge det såkalte aktør/brikke-perspektivet kan dette føre til at man blir passiv og forventer at andre skal ordne opp uten at man selv gjør noe aktivt for å forbedre situasjonen.

4.2.5 Oppsummering digital sikkerhetskultur

Det må gjerne skje noe alvorlig enten med en selv eller noen andre man sammenlikner seg med, for å innse hvilke trusler man står overfor og hvilke konsekvenser det kan ha for egen virksomhet. Det at det må noen aha-opplevelser til for å få mer fokus er imidlertid ikke noe som er spesielt for digital sikkerhet, dette er noe som gjelder for de fleste krisehendelser uavhengig av type krise. Dette handler om risikoforståelse og -erkjennelse, og viser bare at man også innen digital sikkerhet kanskje ofte ligger litt «bakpå» og ikke innser alvorligheten før en selv eller noen andre rammes, og da kan det være for sent. Man kan derfor stille seg spørsmålet om virksomhetene har en god nok risikoforståelse når det kommer til digital sikkerhet, og hvor oppdaterte de er på trusselbildet de står overfor. Teorien trekker frem dette

som et viktig punkt i arbeidet for en bedre sikkerhetskultur, og det bør ligge i bunn av alle avgjørelser man tar videre i prosessen.

Ulike fagmiljøer med egne profesjonskulturer gjør også at det er vanskelig å nå ut til alle ansatte med opplæring og bevisstgjøring. De har egne holdninger og verdier som gjerne skiller seg fra de man burde ha i en god sikkerhetskultur, noe som kan ha sammenheng med at de som ikke måles direkte på sikkerhet heller ikke prioriterer det i den grad de kanskje burde. Sikkerhet og produksjon vil alltid stå i et motsetningsforhold til hverandre, og flere informanter påpeker at dersom de ansatte ikke har en forståelse for sikkerhet og de tiltak som blir iverksatt for å forhindre angrep, vil de ha lettere for å ta snarveier på siden av de sikre løsningene. Samtidig må man ha to tanker i hodet samtidig, og også tenke på hvordan disse tiltakene fungerer i praksis for de som faktisk skal bruke dem, slik at de oppleves som mest mulig effektive med tanke på brukervennligheten. Man burde derfor jobbe mot en økt kollektiv bevissthet slik at alle drar i samme retning og bidrar til å forhindre angrep som kan skade hele virksomheten.

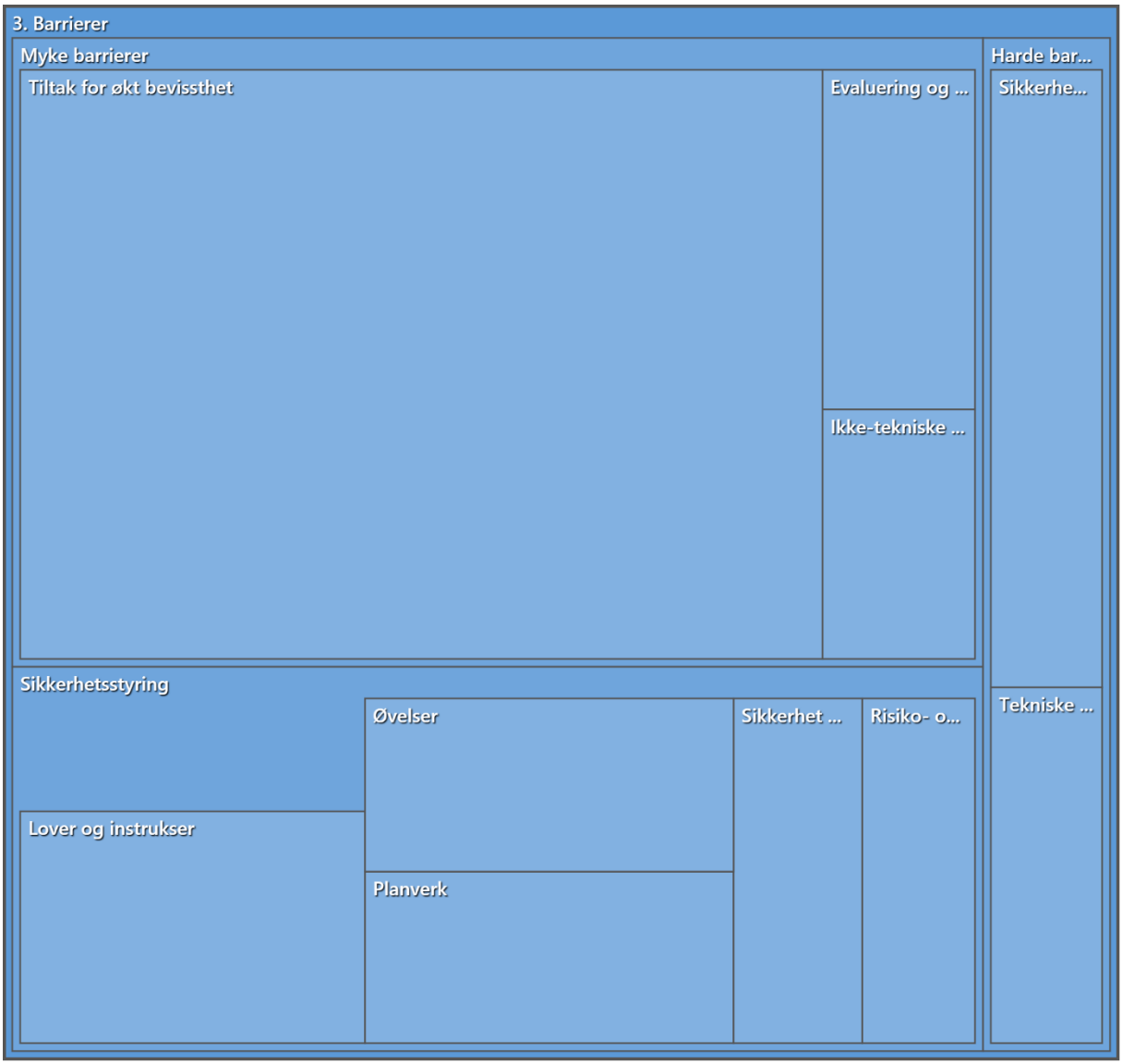
Mennesker vil nok aldri slutte å gjøre feil, men man vil nok heller ikke klare å lage så sikre systemer at en menneskelig feil ikke vil kunne sette systemet ute av spill. Dette gjør at den menneskelige faktoren har kommet for å bli, enten man vil eller ikke. Fokuset virker imidlertid fortsatt å være på de teknologiske løsningene fordi det er der man mener man får mest igjen for det og at det er en bedre løsning enn å «satse på» at man får bevisste ansatte. For å være bedre i stand til å lykkes med opplæring og bevisstgjøring kreves det imidlertid stor grad av forpliktelse fra ledelsen, og de må gå foran som gode eksempler. Selv om utviklingen har vært positiv, er det også her en utfordring med subkulturer og ledere som mener at sikkerhet bare er styr og genererer masse merarbeid. God kommunikasjon og gode arenaer for å dele riktig informasjon om trusselbildet og risikoen man står overfor, er avgjørende for at også ledelsen skal få en god forståelse og bevissthet rundt digital sikkerhet og dermed sørge for at det blir et prioritert område for virksomheten.

En lærende organisasjon legger vekt på åpenhet, erfaringsdeling og samarbeid, og ser verdien i at ansatte varsler om uønskede hendelser. Skal man lykkes med det må man i første omgang ha et system for varsling som er enkelt å bruke og som ikke legger beslag på mye tid i en ellers travel arbeidshverdag. I tillegg må man bruke tid på å bygge opp en varslingskultur hvor man er opptatt av å fange opp feil, og hvor det å melde fra om feil blir verdsatt og ikke straffet. Frykt og flauhet er følelser som må erstattes av et ønske om å dele og bidra med innspill for å kunne forhindre fremtidige digitale angrep. Dette kan være utfordrende da en

slik kultur må bygges på tvers av alle subkulturene som eksisterer i virksomheten. Videre må dette settes i et system for å sikre *læring* og ikke bare rapportering, og klarer man dette ligger mye til rette for å få ansatte som ikke bare tenker sikkerhet, men også handler i tråd med de verdier og holdninger man har skapt. Varig sikker atferd krever imidlertid både en grunnleggende forståelse for digital sikkerhet i kombinasjon med gode holdninger til sikkerhet generelt, samtidig som de ansatte må føle at de blir tatt hensyn til når det kommer til brukervennlighet og effektivitet. Det å skape en god digital sikkerhetskultur er dermed ingen «quick-fix», og krever kontinuerlig arbeid over tid, god støtte fra ledelsen, og et opplærings- og bevisstgjøringsløp som fungerer etter hensikten.

4.3 Barrierer

Teorien sier at barrierer er tiltak som skal redusere muligheten for at ulykker og uønskede hendelser oppstår, og/eller begrenser konsekvensene dersom noe slikt inntreffer. Et overblikk over funnene i denne kategorien vises i figur 4.8, og her ser man at kategorien i utgangspunktet har tre underkategorier; myke barrierer, harde barrierer, og sikkerhetsstyring. Jeg er imidlertid i all hovedsak ute etter de proaktive organisatoriske tiltakene som virksomhetene har innen digital sikkerhet, altså de såkalte «myke» barrierene. Det er også her hovedvekten av funn ligger, spesielt innenfor tiltak for økt bevissthet. Jeg har derfor valgt å utelate de «harde» barrierene i form av teknologiske sikkerhetssystemer og -løsninger i den videre delen av oppgaven. Selv om både planverk, instrukser og risikoanalyser også er viktige myke barrierer i arbeidet med digital sikkerhet, nøyer jeg meg med å oppsummere at samtlige virksomheter har et planverk for digital sikkerhet, noen mer utviklet enn andre. De følger også gjeldende lover og regler for egen sektor, og har til en viss grad også egne instrukser i tillegg. Kraftsektoren skiller seg ut ved at dette er et arbeid de holder på med akkurat nå, mens de andre sektorene allerede har dette på plass. Alle virksomhetene påpeker at de jobber kontinuerlig for å få sikkerhet til å bli en del av den hverdagslige prosessen i organisasjonen, og ikke bare et hinder på siden som kompliserer arbeidet til de ansatte.



Figur 4.8. Oversikt over hoved- og underkategorier – «Barrierer». Hentet fra NVivo.

Videre har jeg altså valgt å legge vekt på tiltakene som retter seg mot opplæring og bevisstgjøring da jeg ser på disse som mest relevante for det holdningsskapende arbeidet, og dermed også for å bedre den digitale sikkerhetskulturen. Jeg har derfor kommet frem til følgende underkategorier i hovedkategorien «Barrierer»:

- Forebyggende arbeid i form av opplæring og bevisstgjøring
- Spesifikke tiltak for opplæring og bevisstgjøring

4.3.1 Forebyggende arbeid i form av opplæring og bevisstgjøring

Selv om det forebyggende arbeidet er veldig viktig, blir det likevel ikke alltid anerkjent på lik linje som det hendelseshåndterende – rett og slett fordi det ikke kan måles i verken tid, penger eller ressurser. Mislykkes man i å *håndtere* en hendelse er det mye mer synlig utad, og dermed er det også lett å fokusere mer på å være god på den reaktive responsen. Daniel (justissektoren) påpeker nettopp denne manglende synligheten av forebyggende innsats som en utfordring med tanke på det å få tildelt ressurser og penger til å jobbe langsiktig og systematisk for å forhindre uønskede hendelser:

> Det er litt tungt å få gjennom ting, spesielt når det kommer til det forebyggende arbeidet. Det er ikke alltid så lett å se at vi må gjøre noe for å unngå å havne på forsiden av VG, men du ser det veldig fort dersom du ikke klarer å håndtere en hendelse. Derfor blir ofte fokuset på det reaktive og hendelseshåndterende. (Daniel, justissektoren).

Selv om god håndtering av en hendelse er viktig, bør det likevel ikke være noen tvil om at det å *forhindre* at slike hendelser oppstår i utgangspunktet, er vel så viktig. Opplæring og bevisstgjøring er en del av dette forebyggende arbeidet, og det er også noen av de proaktive tiltakene som får mye oppmerksomhet i litteraturen som omhandler digital sikkerhet. Som jeg har vært inne på tidligere har den menneskelige faktoren kommet for å bli, og selv om det fortsatt ser ut til å være mest fokus på teknologiske løsninger, blir det stadig større anerkjennelse for at teknologi alene ikke forhindrer et angrep. Manglende forståelse kan igjen henge sammen med manglende eller dårlig opplæring, eller at opplæringen ikke fungerer etter hensikten. Lars (justissektoren) påpeker viktigheten av å ha en pedagogisk tilnærming, og sier at dersom man ikke har flinke folk som evner å formidle budskapet på en god måte, så er man like langt.

> Vi må passe på at de som skal lære opp andre er flinke til å formidle. Det spiller ikke noen rolle hvor god du er på noe, hvis du ikke klarer å formidle det du vet. Da kommer du ingen vei. (Lars, justissektoren).

Kanskje er det også dette som er årsaken til det som Camilla (kraftsektoren) omtaler som «manglende interesse». I deres virksomhet har de som tidligere nevnt ikke noen god strategi på bevisstgjøring av ansatte, og mye av informasjonen som er tilgjengelig krever at den enkelte ansatte selv klikker seg inn på artikler og liknende for å lese seg opp på temaet. Har

man ikke interesse for temaet, er det heller ikke sannsynlig at man bruker tid på å lese noe om det. Dette er også noe Steinar (kraftsektoren) trekker frem som en utfordring:

> Det blir informert veldig mye om det, det kommuniseres mye både på intranett og gjennom mailer som blir sendt ut. Men det er jo avhengig av at folk selv aktivt trykker seg inn på det, og det er jo noe av utfordringen. (Steinar, kraftsektoren).

Dette medfører at det i stor grad er de som allerede er interessert i feltet som trykker seg inn på dette og dermed lærer mer, mens de som ikke er interessert lar være og mister muligheten til å øke forståelsen. For å unngå dette kreves det god opplæring og en velfungerende strategi for bevisstgjøring, og det er derfor interessant å se at den eneste informanten som forteller om et innarbeidet opplegg for opplæring og bevisstgjøring, er Trine fra finanssektoren. I deres virksomhet er det egne ansatte som jobber med «awareness», og dette er noe de har hatt i lengre tid. De som driver med dette jobber systematisk med ulike opplæringsprogrammer, og oppdaterer disse jevnlig gjennom året. Helt i tråd med det litteraturen sier er den beste løsningen, har de har også fokus på fornyelse og tilpasning for å unngå at ansatte går lei, samt at de er opptatt av at det heller skal være lite og ofte enn mye og sjelden:

> Det gjelder å fange oppmerksomheten hos forskjellige brukere rundt omkring, så man må gjerne bruke ulike verktøy til ulike målgrupper. Utfordringen er å sørge for en fornyelse slik at de ansatte ikke går lei av det, samt ta små opplæringer i ny og ne. På den måten unngår vi at det blir for mye på en gang, og vi holder det samtidig litt varmt gjennom hele året. (Trine, finanssektoren).

De har altså tatt innover seg de utfordringene som ofte gjør seg gjeldende når det kommer til det å drive bevisstgjøring av ansatte, og har også innsett at det er så viktig at de har egne ansatte kun dedikert til dette. I den andre virksomheten innenfor finans har de også et obligatorisk opplæringskurs, men dette er noe som er felles for alle, og som ikke er tilpasset ulike miljøer og ansatte. Dette kan ifølge Stian (finanssektoren) føre til mindre interesse blant de ansatte, og de har derfor begynt å se på mer tilpasset opplæring mot spesielt utsatte miljøer:

> De kursene er sånn som alle ansatte skal gjennom, og det betyr at alle synes det er like lite relevant. Vi har derfor et gryende fokus på å ha litt mer differensiert opplæring mot spesielt utsatte miljøer, og jobbe ut fra en trusselbasert forståelse. (Stian, finanssektoren).

Det at de har innsett at opplæringen og bevisstgjøringen bør tilpasses ulike miljøer viser at de tar dette på alvor og at de ønsker å gjøre det på en bedre måte. Trine (finanssektoren) understreker imidlertid at selv om man forsøker å tilpasse opplæringen til ulike miljøer, vil det alltid være noen de mest sannsynlig aldri når uansett. De legger også vekt på at de ikke skal *tvinge* ansatte til å gjennomføre opplæring, men at de forsøker å legge det frem på en måte som gjør at de selv skal ha *lyst* til å gjennomføre det, men det er ikke alltid at dette fungerer. «Vi når ganske mange gjennom å ha fokus på lyst fremfor tvang. Men så er det kanskje en liten gjeng vi aldri når, men vi må alltid prøve noe nytt for å se om vi treffer nye miljøer.» (Trine, finanssektoren). Dette har nok en sammenheng med det jeg var inne på tidligere i oppgaven om ulike subkulturer i virksomheten, og viser bare at det å nå ut til alle kan være en tøff oppgave som krever kontinuerlig arbeid over tid.

Alle informantene fra finanssektoren forteller også at de blant annet gjennomfører sikkerhetskulturundersøkelser og holdningsundersøkelser, og at dette gir dem en viss pekepinn på hvor opplyst de ansatte er og hva de trenger mer opplæring i. De påpeker imidlertid at det er veldig vanskelig å måle holdninger, og at disse undersøkelsene ikke nødvendigvis fanger opp den faktiske tilstanden i virksomheten, men at det likevel er et godt verktøy i arbeidet med å blant annet utvikle og evaluere opplæringsprogrammer. «Én ting er å ha et opplæringsløp, noe annet er jo hva den reelle effekten av det opplæringsløpet er.» (Stian, finanssektoren).

> Vi har blant annet kjørt holdningsundersøkelser som hjelper oss å måle hvilke holdninger og kunnskap de ansatte har. Det er jo ikke noe eksakt, men det gir oss en pekepinn på om det er temaer vi synes man er for dårlig i og som vi kan justere til neste opplæringsperiode. Men det er selvfølgelig vanskelig å måle holdninger, det er det. (Trine, finanssektoren).

Dette er veldig viktige poenger når det kommer til det å skulle måle sikkerhetskulturen i virksomheten. På en side er det bra å forsøke å måle hvilke holdninger de ansatte har fordi det ikke bare sier noe om hvilken atferd de har her og nå, men også hvilken atferd de mest sannsynlig kommer til å ha i fremtiden. På den andre siden kan man likevel ikke være sikker på at disse undersøkelsene gir det riktige bildet fordi ansatte kanskje svarer det de tror de *bør* svare, heller enn det de faktisk mener. Har man mulighet, bør man derfor kombinere dette med andre måleparametre slik at man kan få et mer helhetlig og komplett bilde av hvordan det står til.

Innenfor kraft- og justissektoren fremstår det som om dette opplæringsarbeidet er noe de er i gang med og har et mål om å bli bedre på, men at det ikke finnes noe rammeverk eller strategi for bevisstgjøring og opplæring av ansatte per i dag. Alle virksomhetene har imidlertid noen tiltak rettet mot dette, selv om det ikke nødvendigvis er et systematisk arbeid med det. Camilla og Steinar (kraftsektoren) påpeker begge at det legges ut mye informasjon med den hensikt å bevisstgjøre og lære opp ansatte, men at det ikke er noe mer opplegg enn det: «Det legges ut mye informasjon, men vi har ikke noe mer system for opplæring enn det.» (Camilla, kraftsektoren). «Vi har den informasjonen som vi deler på intranett, men ikke noe direkte opplæring utover det.» (Steinar, kraftsektoren). Det samme gjelder for justissektoren, og både Steinar (kraftsektoren) og Lars (justissektoren) stiller spørsmåltegn ved om den opplæringen de har i dag fungerer etter hensikten. Har man ikke noe ordentlig system eller strategi for opplæring og bevisstgjøring, har man mest sannsynlig heller ikke noen form for evaluering eller måling for å se om de tiltakene man har faktisk fungerer, og dette bekreftes gjennom at de ikke har gjennomført noen måling av holdninger eller kultur. Dette viser derfor at en overordnet strategi og plan for opplæring bør være på plass slik at man også har noen ting å måle tilstanden opp mot – og på den måten kunne tette det gapet som eventuelt eksisterer.

4.3.1.1 Oppsummering forebyggende arbeid i form av opplæring og bevisstgjøring

Det kommer frem at forebyggende arbeid ikke alltid blir prioritert fordi det ikke er like synlig som det hendelseshåndterende. Det er imidlertid vel så viktig siden det faktisk kan spare virksomhetene for mye tid, stress og penger dersom man klarer å forhindre fremtidige angrep. Opplæring og bevisstgjøring av ansatte er viktige forebyggende tiltak innen digital sikkerhet, men likevel er det bare én av informantene som forteller at de har et ordentlig system for dette. I denne virksomheten er det egne ansatte som jobber nettopp med bevisstgjøring, og de jobber kontinuerlig for å tilpasse, fornye og holde ved like kunnskap og kompetanse hos de ansatte. Nettopp det å tilpasse opplæringen til ulike grupper er noe som trekkes frem som viktig også av andre informanter for å bidra til at det oppleves som relevant og noe man ser verdien av. Samtidig påpekes det at enkelte miljøer likevel vil være svært vanskelig å nå ut til, noe som krever målrettet arbeid over tid. I tillegg ser man svakheter ved at informasjon bare legges ut for eksempel på intranett, noe som krever at ansatte selv aktivt går inn og ser på det. Det er ingen tvil om at interesse styrer mye av det vi velger å lære mer om, og med denne

løsningen er det gjerne de som allerede er interessert i digital sikkerhet som går inn og leser, og ikke de som kanskje heller burde ha gjort det fordi de ikke kan nok om det.

Det å gjennomføre sikkerhetskultur- og holdningsundersøkelser kan være med på å gi et bedre bilde av hvor opplyst de ansatte er, hvilke holdninger de har og hva de eventuelt trenger mer opplæring i. Samtidig blir det poengtert at det å måle holdninger er krevende, og at det heller ikke gir noen fasit på hvordan tilstanden faktisk er. Det bør derfor, rent teknisk sett, kombineres med andre måleparametere for å få et mer helhetlig bilde av situasjonen. Det kan likevel være en god pekepinn på dagens tilstand og avdekke et eventuelt gap mellom der man er og der man ønsker å være, og på den måten fungere som et godt utgangspunkt for å legge opp til et bedre opplæringsløp. Jeg vil i neste kapittel gå nærmere inn på de spesifikke opplæringstiltakene virksomhetene har iverksatt for å øke de ansattes bevissthet rundt digital sikkerhet.

4.3.2 Spesifikke tiltak for opplæring og bevisstgjøring

Selv om det varierer i hvilken grad virksomhetene har noe fastsatt opplegg når det kommer til opplæring og bevisstgjøring, er det likevel mange av de samme tiltakene som nevnes – kampanjer, e-læring, foredrag og samlinger, informasjon på intranett, sikkerhetssamtaler og phishing-tester. Tabell 4.2 viser en fordeling av disse tiltakene ut fra sektor:

	Finans	**Kraft**	**Justis**	***Totalt***
Opplæringstiltak				
Kampanjer	2	2	3	*7*
Intranett	2	3	2	*7*
Foredrag og samlinger	2	2	1	*5*
Phishing-tester	1		1	*2*
E-læring	1	1		*2*
Sikkerhetssamtaler	1	1		*2*
Totalt	6 av 6 tiltak	5 av 6 tiltak	4 av 6 tiltak	

Tabell 4.2. Oversikt over ulike tiltak for opplæring og bevisstgjøring av ansatte.

(Tabellen viser tallet på informanter som har nevnt de aktuelle tiltakene på spørsmål om hvilke tiltak virksomheten deres har opp mot opplæring og bevisstgjøring av ansatte. Det betyr likevel ikke at de virksomhetene eller informantene som ikke har nevnt det ikke har tiltakene, men kunnskapen kan være litt ulik ut fra hvilken stilling informanten har, samt at intervjuene ikke var fullt ut strukturert og at det dermed kan være variasjon i hvilke spørsmål som ble stilt de ulike informantene. Det er heller ikke alle som ser på disse tiltakene som opplæring, men har likevel nevnt det som en del av det de gjør for å øke bevisstheten til ansatte.)

4.3.2.1 Kampanjer

Selv om ikke alle informantene sier noe om det, er likevel alle virksomhetene representert under denne kategorien. Det er i hovedsak én kampanje som blir nevnt, og det er Nasjonal sikkerhetsmåned. Flere trekker frem denne som et veldig godt tilskudd til opplæring, og noe som virksomhetene satser hardt på. Denne kampanjen virker å ha fått godt fotfeste blant virksomhetene, og utnyttes ofte ekstra ved å legge til virksomhetsspesifikke moduler som de ansatte må igjennom. Stian fra finanssektoren oppsummerer det som virker som en gjennomgående holdning blant alle virksomhetene: «Vi satser veldig hardt på Nasjonal sikkerhetsmåned hvert år, der kjører vi beinhardt og der er det mye opplegg. Der har vi med hele toppledelsen og det er ganske bra.» (Stian, finanssektoren).

Kampanjer kan absolutt ha mye for seg, men problemet er at de kun kommer en gang iblant og dermed ikke sørger for en jevn tilføring av informasjon og kunnskap. Mye av det man har lært gjennom en kampanje er derfor gjerne glemt neste gang man har en liknende kampanje, og da kan man ofte si at «vinninga går opp i spinninga». Nasjonal sikkerhetsmåned har imidlertid blitt en anerkjent kampanje innen digital sikkerhet, og gjør kanskje at temaet også får mer oppmerksomhet generelt, både hos ledelsen og de ansatte.

4.3.2.2 Intranett

Det å legge ut informasjon på intranettet hos de ulike virksomhetene er et av hovedvirkemidlene for å nå ut med informasjon til de ansatte i arbeidet med å gjøre dem mer bevisste på digital sikkerhet. Også her er alle virksomhetene representert, og alle som nevner dette sier at de legger ut informasjon om ting ansatte bør være obs på, pågående kampanjer, hendelser som har skjedd enten internt eller hos andre virksomheter, i tillegg til tips og triks om hvordan de skal opptre for å ivareta den digitale sikkerheten. Selv om intranett virker å være hovedkilden til informasjon ut til de ansatte, påpeker blant annet Camilla (kraftsektoren) at det er et problem med dette, nemlig det faktum at man er avhengig av at de ansatte selv aktivt går inn og leser på det: «Det ligger jo under IT-siden på intranettet, og jeg regner ikke med at alle går inn der og ser.» (Camilla, kraftsektoren).

Hun sier videre at de har mulighet til å hente ut noe statistikk med tanke på hvor mange som har vært inne og lest de ulike artiklene, men at det likevel ikke er noe godt måleinstrument for å si noe om hvor godt de når ut med informasjonen. Mange sier likevel at de opplever økt aktivitet når det kommer til antall henvendelser og spørsmål fra ansatte i

etterkant av ulike publiseringer, og tolker dermed dette som et tegn på at det fanger en viss interesse. Lars (justissektoren) forteller at de har noe de kaller «Sikkerhetsbloggen» hvor de får «likes» på artikler som legges ut. Han sier at det virker som om dette når ut til de ansatte og at det viser seg i antall henvendelser i etterkant. «Vi har fått tilbakemeldinger på at andre seksjoner har vært veldig positivt innstilt til og begeistret for en del av blogginnleggene, og det gjenspeiles også i antall likes og henvendelser fra hele etaten.» (Lars, justissektoren).

Intranett er altså en god og tilsynelatende effektiv arena for å nå ut til mange ansatte, men som flere av informantene påpeker er den største utfordringen at det krever et aktivt engasjement og initiativ fra de ansatte selv. Når vi vet at de fleste har en travel arbeidshverdag samtidig som at ikke alle er interessert i verken sikkerhet eller digital sikkerhet, er det altså ikke et tiltak som bør stå alene som fullverdig opplæring, men heller som et supplement til andre metoder.

4.3.2.3 Foredrag og samlinger

Alle virksomhetene kjører også en form for foredrag eller samlinger hvor det informeres om digital sikkerhet, dog i litt ulike fora og med ulike deltakere. Camilla (kraftsektoren) påpeker at hun tror effekten av å holde presentasjoner og forklare litt rundt hvilke trusler de står overfor og liknende, er mye bedre enn å kun få de ansatte til å gjennomføre e-læringer og lese ting på intranett. «For man kan skrive mye på nettet og man kan få de til å ta e-læringsoppgaver, men jeg tror at når det blir fortalt og vist litt så gjør det et mye større inntrykk.» (Camilla, kraftsektoren).

Dette kan øke bevisstheten til de ansatte i større grad ved at de får et bedre bilde av hva som faktisk skjer og hvorfor det er viktig at alle er med på å bidra. Disse foredragene kan også i større grad tilpasses og gjøres mer relevante for de man holder presentasjonen for, og på den måten vekker man kanskje også mer interesse enn mer generelle opplæringsopplegg. «Vi kjører noen mer spesifikke foredrag for de miljøene vi syns det er spesielt viktig for. Da kan det være om trusler, klassifisering av informasjon eller et annet tema som er relevant for den avdelingen.» (Trine, finanssektoren).

Et tilpasset foredrag eller samling hvor man kan legge frem litt om de faktiske truslene virksomheten står overfor, er derfor et godt tiltak for å øke bevisstheten blant de ansatte. Det å få presentert historier «fra virkeligheten» og som man kan relatere seg til, gjør helt klart mer inntrykk enn å bare få det servert for eksempel som en del av en mer generell e-læring. Det er

imidlertid en mer tid- og ressurskrevende metode, og bør derfor kombineres med andre tiltak som koster mindre og når ut til flere.

4.3.2.4 E-læring

Utenom Nasjonal sikkerhetsmåned er det kun Camilla fra kraftsektoren og Trine fra finanssektoren som sier at de kjører eller har kjørt e-læringsprogrammer jevnt gjennom året. Trine (finanssektoren) forteller at de sender ut slike programmer månedlig og at de skreddersyr tema for hver gang. Hun påpeker også hvor enkelt dette er og at det fins tilnærmet ferdige løsninger som virksomheter kan få tak i slik at det blir et veldig overkommelig opplæringsprosjekt.

> Nano-learningen sender vi ut ca en gang i måneden. Da får vi statistikk på avdelingene og følger opp at det blir gjennomført. Det fins masse verktøy som tilbyr så å si ferdige nano-learninger, så for de som ikke har begynt med dette finnes det mange enkle muligheter. (Trine, finanssektoren).

Camilla forteller på sin side at de gjennomførte e-læringer i virksomheten hennes før hun begynte, men at det ble avsluttet på grunn av misnøye med leverandøren. De skal imidlertid få noe liknende på plass igjen, og også hun understreker viktigheten av at dette er noe som blir sendt ut på jevnlig basis og ikke bare noe som kommer én gang: «Man må selvfølgelig kjøre slike e-læringsseksjoner på jevnlig basis, for det hjelper ikke bare med én gang – man må inn igjen og igjen og igjen.» (Camilla, kraftsektoren). Samtidig ser hun også utfordringene med denne type opplæring ved at de fleste ansatte er veldig opptatt, og at man risikerer at disse e-læringene blir noe man bare klikker seg gjennom uten å følge ordentlig med. Hun har derfor troen på en kombinasjon av både dette og presentasjoner eller foredrag som kan være med å gjøre en slik opplæring mer spennende: «Hvis man får gjort noe spennende rundt det og fortalt en historie som setter seg litt, så ligger det kanskje litt mer i bakhodet når man skal gjennomføre en sånn e-læringskampanje senere.» (Camilla, kraftsektoren).

E-læring er et effektivt og kostnadsbesparende opplæringstiltak som når ut til mange og som ikke trenger å ta lang tid å gjennomføre. Det kan imidlertid stilles spørsmåltegn ved om e-læring i seg selv er nok for å øke de ansattes bevissthet. Har man dårlig tid, manglende forståelse for digital sikkerhet og sin egen rolle i det, kan en slik e-læring fort bli noe enkelte bare klikker seg igjennom fortest mulig uten å egentlig ha lært noe. Kombinerer man det

derimot med et foredrag eller presentasjon som viser virkelighetens sårbarheter, vil det kunne føre til mer motivasjon og læring.

4.3.2.5 Phishing-tester

Det er kun Trine (finanssektoren) og Knut (justissektoren) som sier at de har kjørt eller kjører phishing-kampanjer, men både blant dem og blant de som vurderer å kjøre det er det den samme problemstillingen som går igjen, nemlig at det fort kan oppleves som en kampanje hvor folk blir uthengt og at det skaper negative reaksjoner.

> Hvis man vil gjøre noe med problemet må man kjøre sånne tester. For vår del økte det interessen, og det var flere av de som sa at det var bra og som ville ha mer av det, enn de få som følte seg uthengt. Selvsagt er det ingen som liker å få påpekt at man har gjort feil, men hvilket alternativ har man? (Knut, justissektoren).

> Hvis vi skal gjennomføre slike tester er det viktig at det brukes riktig, for det er veldig lett at ansatte kan oppfatte det som en utdritningskampanje. Nøkkelen er nok hvordan du bruker de dataene, og ikke nødvendigvis publiserer og går ut og sier hvem som er best og dårligst. (Stian, finanssektoren).

Dette er veldig interessant hvis man ser det i sammenheng med den åpenheten og erfaringsdelingen som jeg var inne på under «Varsling og læring». Der ble også flauhet og frykt trukket frem som mulige faktorer for manglende deling av erfaringer, og dette virker altså også å ha betydning for gjennomføringen av disse phishing-testene. Trine (finanssektoren) påpeker derfor viktigheten av at slike tester blir gjennomført på en god og saklig måte, og at man ikke går etter enkeltpersoner som bevisst eller ubevisst har trykket på noe de ikke skal:

> Det er jo et eget område å tenke gjennom hvordan man vil gjennomføre slike tester. Noen synes at det er å lure de ansatte til å trykke på noe, men vi gjør det ikke for å være slemme eller henge ut noen. Vi gjør det for at de som kanskje har trykket da blir ledet inn i en opplæringsmodul for å lære seg teknikker på hvordan de skal avsløre phishing. Men det er krevende å lage gode sånne tester, enten er de for lette eller så er de for vanskelige, og hvis du lager den vanskelig så vil jo mange gå på den uansett. (Trine, finanssektoren).

Phishing-tester er altså en helt konkret undersøkelse som gir svar på hvor mange av de ansatte som hadde latt seg lure av et svindelforsøk. Dette kan være svært nyttig informasjon for virksomhetene da det sier noe om hvilken sårbarhet de står overfor når det gjelder de ansattes atferd på nett. Likevel er det mange ledere og ansatte som er negative til denne typen tester, og det virker som om dette skyldes en frykt for å komme dårlig ut selv og dermed risikere å tape ansikt. Man må derfor tenke gjennom hvordan man vil bruke resultatene slik at det oppleves som læring og ikke uthengning. Slik jeg ser det henger dette på sin side sammen med hvilken kultur virksomheten har når det kommer til varsling og rapportering, og reaksjonene på slike tester kan derfor være et tegn på at man kanskje må starte med holdningsendring her før man gjennomfører slike tester.

4.3.2.6 Sikkerhetssamtaler

Trine (finanssektoren) forteller at de tar en samtale med alle nyansatte hvor de forklarer hvorfor sikkerhet er så viktig hos dem, og gir dem en kort innføring i virksomhetens sikkerhetsinstruks. Dette gjør de for å sikre et minimum av kunnskap siden de ansatte kommer med svært ulik bagasje når det kommer til det å håndtere informasjon og generell sikkerhet.

> Vi har jo alt fra studenter som aldri har jobbet noe sted og som ikke er vet hvordan man skal forholde seg til dette med informasjonssikkerhet, til ansatte fra andre bedrifter eller andre land og kulturer. Meningen er derfor å forklare litt om hvorfor sikkerhet er så viktig for oss. (Trine, finanssektoren).

Steinar (kraftsektoren) forteller derimot at de nå skal begynne å gjennomføre sikkerhetssamtaler med *alle* ansatte som har tilgang til sensitiv informasjon, noe de ikke har hatt tidligere. Bakgrunnen for at de ønsker å innføre dette er blant annet for å øke bevisstheten til alle ansatte, ikke bare de nyansatte. Han påpeker at det gjerne er de som allerede er ansatt som er den største trusselen og som oftest blir brukt i et eventuelt angrep, og at det derfor er viktig at de blir minnet på dette og viktigheten av sikkerhet. «Det er ikke nødvendigvis de som er nyansatt som er den største trusselen, det er stort sett vi som allerede er ansatt. Vi har jo allerede de tilgangene som en aktør vil være interessert i.» (Steinar, kraftsektoren).

Én-til-en-samtaler hvor man går gjennom virksomhetens policy og regler for digital sikkerhet virker å være en god mulighet til å øke den enkelte ansattes forståelse for temaet. Ut fra egen erfaring er det imidlertid viktig at dette ikke bare blir en samtale hvor man får ramset opp en hel liste med paragrafer og instrukser, for da er sjansen stor for at en som i

utgangspunktet ikke er interessert i feltet faller av og ikke lærer noe mer. Denne samtalen bør derfor også tilpasses den man prater med, og legge opp til en god diskusjon hvor man får forklart den enkelte ansattes rolle i å forhindre digitale angrep mot virksomheten.

4.3.2.7 Oppsummering spesifikke tiltak for opplæring og bevisstgjøring

Selv om ikke alle virksomhetene har et ordentlig system for opplæring og bevisstgjøring, er det likevel de samme tiltakene som går igjen. Nasjonal sikkerhetsmåned er noe alle virksomhetene bruker aktivt som en kampanjeperiode med mye fokus på digital sikkerhet, og det virker også å ha støtte blant ledelsen. Man må likevel huske på at kampanjer er vel og bra mens de står på, men dersom man ikke kjører noen oppfriskning i mellomtiden er mye ofte glemt når man kommer til neste kampanje. Det samme gjelder også for e-læring, noe som er en enkel og lite tidkrevende læringsmetode. De som har dette på programmet påpeker at også dette må kjøres jevnlig, og at det er bedre å kjøre lite og ofte enn mye og sjelden. I tillegg ser flere på det som en fordel om dette kombineres med foredrag og samlinger hvor man kan forklare og vise praktiske eksempler på de truslene og den sårbarheten virksomheten står overfor, slik at de ansatte i større grad kan relatere seg til det.

Et annet tiltak som blir brukt av alle virksomhetene er å legge ut informasjon på intranett. Dette er nok en god kommunikasjonsplattform for å kunne nå ut til mange, men problemet er at det krever at de ansatte selv aktivt går inn og klikker på det. Det er ingen tvil om at interesse styrer oppmerksomheten vår med tanke på hva vi ønsker å lære mer om, og da vil det gjerne være de som allerede er interessert og kan noe om det fra før som klikker seg inn og lærer enda mer. Man når kanskje dermed ikke de som faktisk har mest behov for det.

For å måle hvor godt de ansatte klarer å avsløre sosial manipulasjon er det mulig å gjennomføre såkalte phishing-tester. Dette er imidlertid noe som flere påpeker at man må være varsom med fordi det kan skape mye negative reaksjoner og oppleves som en «utdritningskampanje». Det er derfor viktig å gjennomføre de på en saklig måte og å bruke resultatene konstruktivt i arbeidet videre med opplæring og bevisstgjøring.

4.3.3 Oppsummering barrierer

Det å forhindre kriser er noe av det mest lønnsomme en virksomhet kan gjøre, men til tross for dette blir ofte det forebyggende arbeidet nedprioritert til fordel for den reaktive responsen.

Dette kan skyldes at forebyggende arbeid sjelden lar seg måle i tid, penger og ressurser, og i tillegg er det mindre synlig enn den hendelseshåndterende biten. Innen digital sikkerhet ligger mye av fokuset innen forebygging på opplæring og bevisstgjøring når man snakker om organisatoriske og menneskelige tiltak. Det er likevel kun én av virksomhetene som har et innarbeidet opplegg for dette, mens de andre virker å ta det litt sporadisk her og der. Dette gjør at man ikke vet helt hvordan ståa i virksomheten er når det kommer til kunnskap og kompetanse om digital sikkerhet, og det blir også veldig tilfeldig hvordan og hvilken opplæring de ansatte får.

Skal man klare å øke de ansattes forståelse for digitale trusler og angrep, og få dem til å innse hvor viktige de selv er for å forhindre dette må det et mer systematisk og tilrettelagt opplegg på plass. I den ene virksomheten som har et slikt opplegg følger de «læreboka» og sørger for jevnlig påfyll av informasjon, legger vekt på frivillighet fremfor tvang, tilpasser opplæringen til ulike grupper og fagmiljøer, kombinerer ulike opplæringstiltak og er opptatt av å fornye opplegget slik at de ansatte ikke går lei. Ser vi dette i sammenheng med læring er det viktig å ikke bare få de ansatte til å *gjennomføre* læringen, men også å legge til rette for refleksjon slik at de innser verdien av denne opplæringen og øker forståelsen for *hvorfor* de bør gjennomføre den, såkalt dobbelkretslæring. Dette vil i sin tur være med på å skape en større kollektiv bevissthet rundt digital sikkerhet og de ansattes viktige rolle i arbeidet med å forhindre fremtidige angrep mot virksomheten.

5 Analyse

Problemstillingen min i oppgaven er: *«Hva kjennetegner den digitale sikkerhetskulturen i samfunnskritiske funksjoner, sett fra fagansattes perspektiv?»*

Gjennom denne og mine underliggende forskningsspørsmål som dreier seg om risikoforståelse, holdninger, ledelse, varsling, læring og forebyggende tiltak, har jeg fått et omfattende empirisk grunnlag. Jeg vil nå se på dette i et metaperspektiv og gjennomføre en grundigere analyse hvor jeg drøfter funnene opp mot relevant teori innenfor begrepet sikkerhetskultur, og besvarer forskningsspørsmålene mer direkte. Tabell 5.1 gir en kort oppsummering av de empiriske funnene sett opp mot forskningsspørsmålene, og det er disse som vil bli drøftet og diskutert mer inngående i denne delen av oppgaven.

Forskningsspørsmål	**Hovedfunn**
Hvilken digital risiko opplever virksomhetene at de står overfor?	Mange tusen forsøk på å komme seg inn hver eneste dag, men ingen som har blitt utsatt for alvorlige angrep hvor sensitiv informasjon har blitt stjålet. Litt ulik oppfatning av hvem trusselaktørene er. Digital sikkerhet oppleves for mange ansatte som noe nytt og fremmed – naivt syn på egen betydning.
Hvilke holdninger eksisterer opp mot digital sikkerhet?	Produksjon og forretning prioriteres foran sikkerhet. Ulike miljøer har ulike holdninger – mange ser på sikkerhet som en hindring, og det kan være utfordrende å nå frem. Mennesker vil aldri slutte å gjøre feil – uenighet om kost/nytte med tanke på tiltak rettet mot dette i forhold til teknologiske løsninger.
Hvilken rolle spiller ledelsen i arbeidet med digital sikkerhetskultur?	Mye uklare ansvarsforhold når det kommer til digital sikkerhet. Variasjon i holdninger, men en positiv utvikling. Lederne må brukes aktivt som «bjellesauer».
Hvordan ivaretar man varsling og læring i virksomheten?	Noe manglende system for effektiv og enkel varsling. Frykt, flauhet og mangel på aksept for å innrømme feil står fortsatt i veien for åpenhet. Utfordringer med å skulle dele taushetsbelagt informasjon med andre. Manglende strategi og system for læring og opplæring.
Hvilke utfordringer opplever de med tanke på sikker digital atferd?	Naive holdninger og manglende forståelse sees i sammenheng med mindre sikker atferd. Ansatte tar snarveier forbi de sikre løsningene – kan skyldes dårlig brukervennlighet. Usikker atferd på tross av økt bevissthet og kunnskap.
Hvilke forebyggende tiltak har de for å styrke den digitale sikkerhetskulturen?	Forebyggende arbeid blir ofte nedprioritert til fordel for det hendelseshåndterende. Oppleves som vanskelig å nå frem til alle pga ulike kulturer innad i virksomheten. Kun én av virksomhetene har et innarbeidet opplegg for opplæring og bevisstgjøring av de ansatte. Sikkerhetskulturundersøkelser kan være et godt utgangspunkt for videre tiltak. Spesifikke tiltak: Kampanjer, e-læring, intranett, foredrag og samlinger, phishing-tester og sikkerhetssamtaler.

Tabell 5.1. Kobling mellom forskningsspørsmål og empiriske funn.

Teorien som ble presentert i kapittel 2 vil være grunnlaget for analysen, sammen med en del nyere internasjonal forskning på området digital sikkerhetskultur. De to hovedkategoriene «Digital sikkerhetskultur» og «Barrierer» som ble introdusert i kapittel 4, vil bli videreført gjennom denne analysen. Hovedkategorien «Digital sikkerhet» er innlemmet i disse to da dette fremsto som mest hensiktsmessig opp mot analysen og drøftingen.

De viktigste funnene i oppgaven dreier seg om holdninger, bevissthet og risikoforståelse rundt digital sikkerhet, ledelsens påvirkning, varsling og læring, hvilke tiltak virksomhetene har for å øke de ansattes bevissthet og forståelse om digital sikkerhet, og hvorvidt disse fører til en sikrere digital atferd blant de ansatte. I denne analysen har jeg valgt å slå sammen enkelte tema og kategorier fra funnkapittelet siden flere av dem henger sammen og det er mer hensiktsmessig å se de i sammenheng kontra hver for seg. På denne måten blir det også mer dybde i analysen sammenlignet med det å «isolere» funnene og trekke teorien opp mot hvert enkelt tema.

Til å begynne med vil jeg ta for meg de funnene som jeg har valgt å samle under kategorien «Digital sikkerhetskultur». Begrepet sikkerhetskultur favner relativt bredt, og det er derfor nødvendig å se funnene som en helhet da de gjensidig vil påvirke hverandre gjennom hele prosessen. Etter dette vil jeg drøfte kategorien «Barrierer», hvor fokuset mitt som sagt er på organisatoriske tiltak for å øke bevisstheten rundt digital sikkerhet. Jeg vil derfor se på det forebyggende arbeidet i form av det som blir kalt «myke» barrierer og utfordringer med dette, for så å drøfte de konkrete tiltakene virksomhetene har i arbeidet med opplæring og bevisstgjøring.

Til slutt i oppgaven vil jeg presentere konklusjonen og se på hvilke faktorer som kjennetegner den digitale sikkerhetskulturen i virksomhetene og hvilke tiltak virksomhetene har for å ivareta den, herunder om tiltakene virksomhetene har fungerer etter hensikten og faktisk bidrar til økt bevissthet og sikrere atferd i organisasjonen. Jeg vil også presentere oppgavens praktiske og teoretiske implikasjoner.

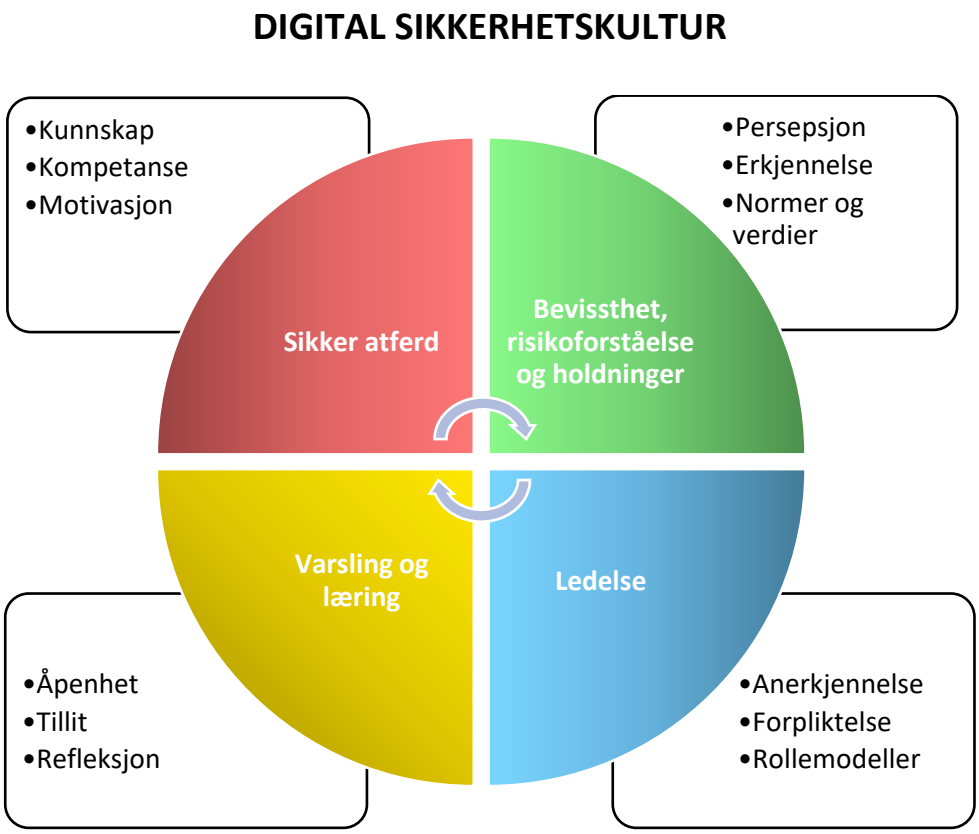
5.1 Digital sikkerhetskultur

Ut ifra de empiriske funnene jeg har gjort i denne oppgaven, er det som tidligere nevnt fire kategorier som utmerker seg i omfang og dybde innen hovedkategorien digital

sikkerhetskultur. Det er altså her hovedvekten av funn ligger ut fra hva informantene fortalte om deres arbeid med digital sikkerhet. Disse fire kategoriene er:

1) Bevissthet, risikoforståelse og holdninger
2) Ledelsens rolle
3) Varsling og læring
4) Sikker atferd

Disse kategoriene er også sentrale momenter som går igjen i teorien, og jeg har utarbeidet en modell som viser en oversikt over dette i figur 5.1. Her har jeg også har knyttet de viktigste funnene opp mot hver enkelt kategori. Dette er dermed en forenklet modell som viser noe av innholdet i kategoriene, samtidig som det viser at arbeidet med digital sikkerhetskultur er en kontinuerlig prosess hvor de ulike faktorene påvirker hverandre og virker i et samspill.



Figur 5.1. En overordnet modell som viser de ulike komponentene i digital sikkerhetskultur, basert på teori og mine empiriske funn i oppgaven.

I den videre drøftingen er disse kategoriene delt noe opp for å gjøre det mer leservennlig og oversiktlig, og fordi noe av innholdet drøftes mer inngående enn andre. Overskriftene videre i oppgaven er derfor som følger:

- Bevissthet og risikoforståelse
- Sikkerhet og produksjon – målkonflikter og subkulturer
- Ledelsens rolle i arbeidet med å skape en god digital sikkerhetskultur
- Lærende organisasjoner – et resultat av åpenhet, varsling og refleksjon
- Bevisstgjøring – er det verdt det?
- Sikker digital atferd – selve målet med en god digital sikkerhetskultur

5.1.1 Bevissthet og risikoforståelse

Camilla (kraftsektoren) påpekte at det som skjer i cyberdomenet er ganske nytt for mange, og at det derfor oppleves som fremmed og skummelt og noe som man ikke helt vet hvordan man skal forholde seg til. Dette kan sin tur ha betydning for hvilke trusler og sårbarheter man ser at man står overfor, nettopp fordi at det å vurdere risiko i høy grad er noe subjektivt (Aven et al., 2004). Oppfattet sannsynlighet og konsekvens vil ha stor innvirkning på hvilken stor risiko man tror man står overfor, og dersom man ikke har erfaring fra tilsvarende forhold vil det være enda vanskeligere å forestille seg mulige utfall og konsekvenser (Moldjord et al., 2007). I tillegg kan det i den digitale verdenen faktisk *være* vanskeligere å vite hvilke trusler man står overfor og hvem som står bak, rett og slett fordi det som skjer er mye mindre synlig og vanskeligere å avdekke (Nätt& Heide, 2015; Boin, 2019). Samtidig kan det også virke mindre alvorlig fordi det ikke nødvendigvis rammer en selv personlig, men heller rammer virksomheten eller organisasjonen som helhet i form av tapte penger og dårlig omdømme (Gjertsen, Gjære, Bartnes & Flores, 2017).

Tap av materielle verdier vekker ikke de samme følelsene som tap av liv og helse, og dette kan gjøre det vanskeligere å bedømme risikoen fordi man ikke assosierer de «riktige» følelsene med denne typen trusler og angrep (Moldjord et al., 2007; Eid & Johnsen, 2005). Lars fra justissektoren belyser dette veldig godt i sin uttalelse hvor han poengterer at mange har en naiv holdning hvor de tenker: «Jamen, hva er det folk vil med meg da, jeg er jo ikke interessant på noe som helst nivå?». Dette er et godt eksempel på at mange ikke forstår eller klarer å sette seg inn i hvordan digitale angrep foregår, og dermed også sitter igjen med en feilaktig oppfatning av trusselen, og et inntrykk av at det er lite de kan gjøre for å forhindre

slike angrep (Smith & Ali, 2019; Cone, Irvine, Thompson & Nguyen, 2007; Nätt & Heide, 2015; Bergsjø et al., 2020). Mange av informantene påpekte derfor at de bevisst bruker hendelser som har rammet andre sammenlignbare virksomheter for å øke bevisstheten rundt digitale hendelser. Det å presentere hendelser på en måte som tydelig viser at det likså godt kunne skjedd i egen virksomhet, kan derfor føre til at det oppleves nærmere og dermed gi økt forståelse for truslene man står overfor (Moldjord et al., 2007, Eid & Johnsen, 2005).

Det å ha en korrekt risikoforståelse og -bevissthet er avgjørende for å lykkes i arbeidet med sikkerhet (Aven et al., 2004; Reason, 1997, s. 113). En god risikoanalyse og -vurdering er i utgangspunktet relativt objektiv, og er derfor viktig for å få fokuset over på fakta fremfor følelser. En slik tilnærming vil også være lettere å formidle videre da man kan vise til konkrete tall og analyser, og det blir noe mer håndfast å forholde seg til. Stian (finanssektoren) understreker viktigheten av at man har en god trusselbasert tilnærming til risiko, hvor det å kartlegge trusselaktører og mulige angrepsformer er særdeles viktig for å øke forståelsen og sette inn gode tiltak. Det var riktignok uenighet blant informantene om hvilke trusselaktører de stod overfor, og mens to av tre sektorer svarte at store land som Russland, Kina, Nord-Korea og Iran stod for mange av angrepene mot dem, mente kraftsektoren at de ikke stod på kartet til disse landene. Dette kan enten skyldes det faktum at de faktisk ikke har avdekket noe aktivitet som tilsier at disse landene står bak angrep mot dem, eller så kan det være at de ikke har tatt innover seg at også deres virksomhet kan være interessante for disse landene fordi det kanskje føles litt voldsomt og lite aktuelt. I tillegg blir underleverandørers manglende fokus på sikkerhet trukket frem som en ekstra risikofaktor blant noen av informantene. Alt dette kan sees i sammenheng med det Turner (1978) hevdet om risikovurderinger; de kan være problematiske nettopp av den grunn at risiko blir oppfattet og tolket ulikt av ulike interessenter. Det er dermed ikke sikkert at man tolker risikoen man står overfor på en hensiktsmessig måte fordi det ikke stemmer overens med organisasjonens oppfatning om hvordan ulykker skjer (Turner, 1978). En god risikovurdering baserer seg derfor på at man faktisk evner å erkjenne de truslene og sårbarhetene man står overfor, slik at tiltakene man setter inn blir tilpasset risikoen. I og med at digitale hendelser gjerne oppfattes som mer fremmed enn de fysiske og mer tradisjonelle hendelsene, blir dette arbeidet ekstra viktig da man i større grad risikerer å ikke sette inn hensiktsmessige tiltak fordi risikoen feilbedømmes.

Generelt sett fremstod det imidlertid som om mine informanter hadde en god digital risikoforståelse; de var veldig bevisste på sårbarhetene og utfordringene de står overfor, og de

var innforstått med at digital sikkerhet ikke bare dreier seg om gode teknologiske løsninger. Men, dette er personer som *jobber med* digital sikkerhet og dermed både har mer kompetanse og interesse for feltet enn hva den «vanlige» ansatte gjerne har. En av de største utfordringene virket derfor å være for dårlig forståelse blant *andre ansatte* i organisasjonen, også til dels ledelsen. Risikoforståelsen bygger altså på kunnskap og kompetanse rundt det aktuelle feltet, og dette er derfor sentralt i alle teoriene rundt sikkerhetskultur og høypålitelige organisasjoner (Reason, 1997; Turner, 1978; Weick & Sutcliffe, 2015; Kvalnes, 2010; NorSIS, 2020; Bergsjø et al., 2020). I og med at risiko vurderes subjektivt, er det derfor avgjørende at alle ansatte opparbeider seg mer kunnskap om digital sikkerhet og får en forståelse for hvilke trusler de faktisk står overfor. En god og korrekt risikoforståelse er det som legger grunnlaget for gode holdninger til det videre sikkerhetsarbeidet.

5.1.2 Sikkerhet og produksjon – målkonflikter og subkulturer

Ifølge Reason (1997, s. 3) er det i en ideell verden en perfekt balanse mellom sikkerhet og produksjon, hvor nivået av sikkerhet gjenspeiler de farene som er forbundet med produksjonen. I den virkelige verden ser man imidlertid at produksjon ofte «vinner» over sikkerhet, blant annet fordi det er produksjonen som tross alt skaper ressursene som trengs for å kunne jobbe med sikkerhet. I tillegg vil et vellykket sikkerhetsarbeid kun vises gjennom fraværet av uønskede hendelser – noe som kan fremstå veldig vagt og diffust for mange. Det var derfor ikke overraskende at mange av informantene trakk frem nettopp denne evige målkonflikten mellom sikkerhet og produksjon som en viktig utfordring. Det som imidlertid var litt overraskende var at justissektoren *ikke* nevnte dette som et problem. Det kan derfor virke som om det er en forskjell i tankegangen mellom private og offentlige virksomheter, hvor de private i større grad er avhengige av å overleve i et stadig tøffere konkurransemarked og dermed også i større grad kan se på sikkerhet som et hinder.

Spesielt innen finanssektoren ble «time to market» (Stian, finanssektoren) tatt frem som en viktig faktor, og dette viser at det å jobbe i et marked som stadig krever mer effektivitet og raske løsninger gjør arbeidet med sikkerhet mer krevende. Sikre løsninger som skal forhindre angrep og uønskede hendelser blir sett på som tungvinte og unødvendige, og ansatte tar heller snarveier utenom disse fordi det går raskere. I tillegg vil det være en medvirkende faktor at dette er ansatte som ikke jobber med sikkerhet og dermed heller ikke måles på det, noe som også bidrar til at de ikke prioriterer det. Dette er noe som også vises i

forskning på området, og det å finne en balanse mellom sikkerhet og brukervennlighet som sikrer fortsatt effektivitet, er derfor avgjørende for å bidra til mer etterlevelse blant de ansatte (Bada, Sasse & Nurse, 2019). En løsning på dette kan derfor være å involvere brukerne av systemene i utviklingen av de sikre løsningene, noe som samtidig også kanskje bidrar til en økt forståelse for hvorfor man er nødt til å ha dem.

Det kan altså være stor variasjon i holdningene til sikkerhet, også innenfor én og samme virksomhet. Ulik bakgrunn, ulike arbeidsoppgaver og ulikt fokus er alle faktorer som gjør at det dannes ulike subkulturer innad i en organisasjon, og som igjen påvirker holdningene våre (Bang, 2011; Jacobsen & Thorsvik, 2013). Videre vil holdninger til sikkerhet og det å ha en korrekt risikoforståelse påvirke hverandre gjensidig; har man en negativ holdning til sikkerhet, vil man høyst sannsynlig heller ikke ha en korrekt risikoforståelse. Det at enkelte miljøer i virksomheten har slike negative holdninger til sikkerhet som nevnt over kan sies å bære preg av såkalt «gruppetenkning». Dette er en konsekvens av utviklingen av subkulturer fordi det fører med seg en selektiv og skjev informasjonstilgang som fører til at ansatte tror at det de selv jobber med er viktigere enn andre oppgaver i organisasjonen (Jacobsen & Thorsvik, 2013). Dette bidrar til at mange av informantene opplever at det er vanskelig å nå ut til alle, og at det er noen miljø man «aldri vil nå frem til» (Trine, finanssektoren). Det er derfor ikke så rart at mange hevder at mennesket alltid vil være en stor risikofaktor når det kommer til digital sikkerhet, fordi bevisstheten rundt digital sikkerhet vil avhenge av hvorvidt man oppfatter digitale angrep som en reell trussel eller ikke.

Ser man på definisjonen av begrepet «sikkerhetskultur» ser man imidlertid at dette omfatter en *kollektiv forståelse* for hvilke trusler og farer man står overfor, samt en *felles oppfatning* om betydningen av sikkerhet (Aven et al., 2004; Turner, 1978; Reason, 1997). Det samme gjelder for digital sikkerhetskultur, hvor blant annet *felles* verdier, holdninger og risikooppfattelse er det som bidrar til at man unngår å bli rammet av digitale angrep (NorSIS, 2020). *Kollektiv bevissthet* og såkalt «sensemaking» er også helt sentralt innenfor teorier om høypålitelige organisasjoner (Weick & Sutcliffe, 2015), og dette viser at arbeidet med å skape en god digital sikkerhetskultur rokker ved noen grunnleggende utfordringer når det kommer til kultur generelt, nemlig hvordan man kan skape en god sikkerhetskultur på tvers av alle subkulturene som utvikler seg i en organisasjon. Kanskje er det dette som er noe av grunnen til at flere av informantene stilte spørsmålstegn ved hvorvidt det å bruke ressurser på å øke bevisstheten og forståelsen av digital sikkerhet er verdt det eller ei.

Men til tross for at det kan oppleves som vanskelig å nå ut til alle og man sitter igjen med en følelse av at det er grupper i virksomheten som ikke tar innover seg risikoen man står overfor, er det faktisk også sånn at ulikhet kan være bra og en god kilde til læring og utvikling. For selv om fokuset innen sikkerhetskultur er en *kollektiv* forståelse og bevissthet, påpeker Weick & Sutcliffe (2015, s. 130) at man også risikerer å skape en såkalt «kollektiv blindhet» hvor viktige faktorer blir oversett på grunn av en *for* homogen oppfatning av risikoen og farene. Dette samsvarer også med det Turner (1978) så på som selve grunnlaget for utviklingen av ulykker, nemlig at de kulturelle oppfatningene ikke lenger stemte overens med de faktiske forholdene. Det å stå overfor grupper i virksomheten som utfordrer og kanskje også vanskeliggjør sikkerhetsarbeidet kan derfor på sin måte være en god utfordring og bidra til at man ikke blir hengende bakpå, men at man heller ser på det som et kontinuerlig arbeid som krever innsats over tid.

5.1.3 Ledelsens rolle i arbeidet med å skape en god digital sikkerhetskultur

Ledere skal sette retning og utarbeide mål og visjoner for virksomheten, og ut fra dette legges det strategier for hvilke områder som skal prioriteres med penger og ressurser (Jacobsen & Thorsvik, 2013). Dette vil i sin tur påvirke de ansattes holdninger til ulike områder i organisasjonen da ledelsens prioriteringer i stor grad kan sies å være et uttrykk for deres, og dermed organisasjonens, verdier og syn på hva som er viktig (Bang, 2011). Innenfor teorier om sikkerhetskultur trekker flere frem viktigheten av ledelsens forpliktelse når det kommer til sikkerhet og sikkerhetsarbeid – uten den er det nemlig stor sannsynlighet for at arbeidet blir nedprioritert til fordel for andre områder (Reason, 1997; Turner, 1978; Weick & Sutcliffe, 2015; Kvalnes, 2010; NorSIS, 2020; Alshaikh, 2020; Wiley et al., 2019). Dette fremkommer også som en utfordring blant informantene, og alle sektorene forteller om fragmenterte og til dels uklare ansvarsområder når det kommer til digital sikkerhet. Informantene fra kraftsektoren opplever at det har vært noe manglende fokus og strategi fra ledelsen på akkurat dette, og Mads (kraftsektoren) forteller at han har måttet jobbe målrettet for å løfte IKT-sikkerhet opp til å bli en viktig del av organisasjonens oppgaver. Selv i finanssektoren hvor de anser seg selv for å være langt fremme når det kommer til digitalisering, opplever de at det er en del oppdelte miljøer som sitter med ansvar for hver sine ting, og at dette fører til en uklar ansvarsfordeling. Dette rammer nok spesielt arbeidet med bevisstgjøring og opplæring, da dette er noe som har fått mer fokus de senere årene og dermed ikke har vært en del av den tradisjonelle IKT-sikkerheten tidligere. Flere av informantene påpeker at digital sikkerhet har

fått et løft de siste par årene, hvor de har fått økt bemanning og økte bevilgninger. Det kan likevel virke som om det mangler noen overordnede strategier for arbeidet med digital sikkerhet, og at dette bør komme på plass for å sørge for et godt og enhetlig arbeid på veien mot å øke den generelle forståelsen og bevisstheten i virksomhetene.

Bergsjø et al. (2020, s. 43) påpeker at arbeidet med digital sikkerhetskultur er ledelsens ansvar, og at de derfor må sette klare mål for hva de ønsker å oppnå. Han understreker viktigheten av å jobbe målrettet og helhetlig med dette over tid, og dette har nok kanskje vært noe av problemet for flere av virksomhetene. Jeg skrev innledningsvis om hvordan digital sikkerhet ofte oppleves som noe nytt og fremmed for mange, og dette kan nok også til en viss grad gjelde for ledelsen. Jeg var tidligere i oppgaven inne på hvordan risikoforståelsen vår blir påvirket av flere forhold, og Reason (1997, s. 4) trekker frem det faktum at ledelsen selv sjelden er utdannet eller har noen spesiell kompetanse innen sikkerhet, og at dette igjen påvirker deres holdninger til sikkerhetsarbeidet. Dette krever at de som jobber med sikkerhet evner å formidle den risikoen og de truslene man står overfor på en god og hensiktsmessig måte, men dette er ikke alltid like enkelt. Det å kommunisere risiko og sikkerhet kan være utfordrende fordi informasjonen man har ofte kan være ganske vag og indirekte, i motsetning til andre områder hvor man kan vise til tall og statistikk. Denne kommunikasjonsutfordringen er også noe av det Turner (1978) trekker frem i sin ulykkesteori, og Thomas fra finanssektoren påpeker at han mener at man i større grad må evne å kvantifisere risiko, slik at det blir mer håndfast og direkte for de man skal nå frem til. Dette krever riktignok at man får tilgang til ledelsen på en måte som gjør denne kommunikasjonen mulig, og Daniel (justissektoren) forteller at dette ofte kan være en utfordring i deres virksomhet som er en tradisjonell byråkratisk organisasjon. «For hvert nivå du går opp i en organisasjon så er det et filter. Og jo flere nivåer du har, desto mer filtreres kommunikasjonen og jo mindre kommer frem». Dette viser en grunnleggende utfordring med kommunikasjon på tvers av nivåer i en virksomhet, og kan ofte føre til at viktig informasjon ikke kommer frem til de som bør ha den, noe som i sin tur kan forårsake en uønsket hendelse lenger frem i tid (Turner, 1978; Pidgeon & O'Leary, 2000).

Trine (finanssektoren) forteller om ledere som ikke gidder å gjennomføre opplæring, og dette kan igjen påvirke de ansatte da de kan få et inntrykk av at dette ikke er noe som prioriteres og som de ikke trenger å bruke tid på. Det å nå gjennom og få anerkjennelse fra ledelsen er svært viktig for det holdningsskapende arbeidet, men det kan være vanskelig når man opplever at de stopper opplæringsprogram fordi de selv ikke vil gjøre feil og tabbe seg

ut. Knut (justissektoren) kom med et eksempel på dette når han fortalte om ledere som han mistenkte satte en stopper for en phishing-kampanje fordi de selv hadde gått på det året før. Han stilte derfor spørsmålstegn ved hvor godt disse lederne forstår det faktiske problemet og hensikten med slik opplæring. Bang (2011, s. 81) påpeker at ledelsens synlige atferd og hva de gjør og ikke gjør påvirker alle de andre ansatte, både positivt og negativt. En negativ innstilling til sikkerhetsarbeid og opplæring vil derfor lett kunne smitte over på de andre, og føre til dårligere oppslutning og deltakelse på slike tiltak. En negativ holdning til det å innrømme feil kan i tillegg bygge opp under en fryktkultur, hvor det å innrømme feil blir sett ned på (Kvalnes, 2010). Innenfor sikkerhetsarbeid og opplæring er dette overhodet ikke en effektiv strategi, og vil i stor grad kun føre til dårligere oppslutning og deltakelse (Bada et al., 2019).

Mads fra kraftsektoren forteller derimot om en leder som stod frem og turte å si ifra når hun hadde klikket på en falsk e-post, og dette bruker de som et foregangseksempel for de andre ansatte. Thomas sier også at de bevisst prøver å bruke ledelsen som «bjellesauer», fordi de vet hvor stor påvirkningskraft lederne har og hvor viktige de er i arbeidet med sikkerhet. Disse eksemplene er helt i tråd med det flere påpeker som en svært viktig faktor når det kommer til sikkerhet og ledelse, nettopp det at ledelsen er villige til å gå foran som gode eksempler og ikke lar frykt for å tape ansikt eller dumme seg ut styre hvorvidt de står frem med egne feil eller ikke (Bergsjø et al., 2020; NorSIS, 2020,; Kvalnes, 2010). NorSIS (2020) omtaler dette som en fellesskapskultur, hvor hensynet til fellesskapet går foran det faktum at det føles ubehagelig og flaut å fortelle om egne feil. De ovenstående eksemplene viser hvor mye ledelsens forpliktelse til sikkerhetsarbeidet har å si, og det legger videre til rette for en kultur preget av åpenhet og et ønske om læring og forbedring, noe som er helt essensielt for å få en god sikkerhetskultur (Reason, 1997; Turner, 1978; Pidgeon & O'Leary, 2000; Kvalnes, 2010; NorSIS, 2020).

5.1.4 Lærende organisasjoner – et resultat av åpenhet, varsling og refleksjon

Det å være en lærende organisasjon inneholder flere ulike faktorer, og informantene ble stilt spørsmål om hvorvidt de hadde et system for varsling og rapportering, hvorvidt det var kultur for å varsle, og til slutt om informasjonen man fikk inn ble brukt som en kilde til læring. Både innenfor teorier om organisasjonskultur og sikkerhetskultur står læring sentralt, og Jacobsen & Thorsvik (2013) hevder at en organisasjonskultur er basert på læring og hvordan man

tilpasser seg til nye erfaringer og forandringer. Pidgeon & O'Leary (2000) hevder videre at organisatorisk læring er kritisk for en god sikkerhetskultur. For at erfaringer og opplevelser skal kunne bidra til *systematisk organisatorisk læring*, må det imidlertid settes i et system som både muliggjør deling av informasjonen og ikke minst være en arena hvor de ansatte føler at det er greit å dele personlige erfaringer og hvor det skapes muligheter for refleksjon og diskusjon (Pidgeon & O'Leary, 2000; Jacobsen & Thorsvik, 2013; Irgens, 2011).

Flere av informantene trekker frem viktigheten av at det må være enkelt å varsle, slik at terskelen for å si ifra blir lav. Camilla (kraftsektoren) påpeker at de aller fleste har travle arbeidsdager, og at det derfor ikke må oppleves som merarbeid å varsle om feil eller uønskede hendelser. Samtidig er det varierende i hvor stor grad virksomhetene har utarbeidet et godt system for dette, men felles for dem alle er at dette er noe som er på agendaen og som de har satt fokus på. Det hjelper imidlertid ikke å ha et godt system for varsling og rapportering dersom de ansatte ikke føler at det er greit å melde ifra. Dette betyr at de ansatte må føle trygghet og ha en viss garanti for at de ikke blir straffet dersom de melder fra om feil, og dette er igjen avhengig av tillit mellom de ansatte og ledelsen (Pidgeon & O'Leary, 2000; Reason, 1997; Kvalnes, 2010; NorSIS, 2020). Flere av informantene sier at de aktivt går ut og forsøker å predikere at alle kan gjøre feil, men at det viktigste er at de sier ifra om det slik at det blir fanget opp. De prøver dermed å få bukt med at frykt og flauhet skal stå i veien for å si ifra om egne feil, men spesielt innen finanssektoren virker det å være utfordringer med å nå gjennom til alle med denne holdningen. Både Trine og Stian (finanssektoren) forteller igjen om sterke profesjonskulturer hvor det å gjøre feil ikke blir akseptert og hvor det også kan gi konsekvenser i form av tapte bonuser og andre belønninger. Dette er altså stikk i strid med det teorien fremhever som viktig for å fremme læring i organisasjonen. Her kan man videre se sammenhengen med ledernes rolle i arbeidet med å bygge en god sikkerhetskultur – de er også en del av de ulike profesjonskulturene, og hvis ikke man får de med seg på laget vil det skape ytterligere utfordringer med å nå gjennom til disse miljøene og skape en god varslings- og læringskultur.

Har man et system som gjør det enkelt å varsle og rapportere om hendelser, samt får de ansatte til å faktisk gjøre dette til tross for at det er ubehagelig å innrømme egne feil, er man langt på vei mot å bli en lærende organisasjon. Det krever imidlertid at man faktisk har et fokus på at innrapportering og varsler skal *føre til læring*, og at det ikke bare ender opp som masse informasjon som ligger i systemet uten å bli brukt på en hensiktsmessig måte (Jacobsen & Thorsvik, 2013; Irgens, 2011). For selv om virksomhetene virker å være gode på å dele

informasjon både internt og eksternt, er det likevel ikke et uttalt fokus på læring, og dermed heller ikke noe system for å ivareta dette. Læring krever at man ikke bare tilegner seg ny kunnskap, men at man også evner å reflektere rundt hvorvidt denne informasjonen endrer på de grunnleggende målene og verdiene man har, og i sin tur bidrar til å endre den faktiske atferden, såkalt dobbelkretslæring (Jacobsen & Thorsvik, 2013; Irgens, 2011). Dette kan også sees i sammenheng med Weick & Sutcliffes (2015) prinsipper om å både være opptatt av feil og uønskede hendelser, og om å ha respekt for ekspertise og kompetanse. Hvis man ikke har et system for rapportering som sørger for god informasjons- og erfaringsdeling, vil heller ikke de ansattes ekspertise bli godt nok brukt og ivaretatt som en viktig del av organisasjonens samlede kompetanse.

Digitale angrep er som tidligere nevnt komplekse og uoversiktlige, og de kan ramme på tvers av både organisasjoner og sektorer. For å være best mulig forberedt og klare å forhindre disse type truslene og angrepene må man derfor være i stand til å bidra til en såkalt grenseoverskridende «sensemaking» noe som betyr at man må legge til rette for informasjonsdeling (Ansell, Boin & Keller, 2010; Boin, 2019). En utfordring som kanskje er mer fremtredende for samfunnskritiske funksjoner enn det er i andre sektorer, er riktignok dette med taushetsbelagt informasjon, som blir trukket frem av kraft- og justissektoren. De forteller at dette gjør dem mer restriktive med tanke på hvilken informasjon de deler, og med hvem. Dette kan på sikt bidra til det som Turner (1978) mente var kjernen til mange ulykker, nemlig problemer med informasjonsdeling og kjennskap til konteksten krisen foregår i for å tolke informasjonen riktig og viderebringe dette til riktige personer. Thomas fra finanssektoren påpeker på sin side at andre, både i samme bransje og utenfor, i all hovedsak blir utsatt for de samme trusselaktørene og -angrepsmetodene innenfor det digitale domenet, og at det derfor er svært viktig at de deler erfaringer rundt dette for å forhindre fremtidige angrep. De har derfor valgt å være relativt åpne om både antall angrep og ulike trusselaktører.

Dette viser at det å sørge for god informasjons- og erfaringsdeling kan være utfordrende på grunn av faktorer som gjelder spesielt for samfunnskritiske funksjoner. Når man imidlertid ser hvor viktig denne prosessen er for å sikre organisatorisk læring og dermed også øker mulighetene til å forhindre fremtidige digitale angrep, er det likevel avgjørende at man ser på ulike løsninger som både ivaretar behovet for å beskytte kritisk informasjon samtidig som man deler det man kan. Dette kan løses gjennom et forslag som også Steinar fra kraftsektoren la frem, nemlig å ha lukkede forum hvor alle er innforstått med at informasjonen ikke deles ytterligere. Samtidig må man som en samfunnskritisk funksjon også ha i bakhodet

at slike forum kan utnyttes til å innhente informasjon om ulike virksomheters svakheter og sårbarheter (Lars, justissektoren). Det kan altså være en krevende balansegang i dette, men så lenge man har fokus på læring og det å stadig bli bedre, kan man tilstrebe å gjøre de tilpasningene som må til for å gjøre dette på en sikker måte.

5.1.5 Bevisstgjøring – er det verdt det?

Daniel (justissektoren) påpekte at mennesker aldri vil slutte å gjøre feil, og at det derfor er bedre å investere i sikre teknologiske systemer fremfor tiltak for å øke forståelsen og bevisstheten. Mange kilder innen informasjons- og datasikkerhet påpeker imidlertid at tekniske systemer aldri vil være nok for å forhindre digitale angrep, og at den menneskelige faktoren alltid vil være et risikomoment som kan sette de sikre systemene ut av spill (Bergsjø et al., 2020; Nätt & Heide, 2015; Krombholz, Hobel, Huber & Weippl, 2014; Khan, Alghatbar, Nabi & Khan, 2011; Smith & Ali, 2019). Ser man på menneskelige feil som en isolert hendelse hvor årsaken ene og alene tilskrives individet selv, kan det å heller satse på teknologiske løsninger fremstå som hensiktsmessig. Ser man derimot på menneskelig svikt som en konsekvens av latente forhold i organisasjonen og systemet, er det ingen tvil om at det er organisatoriske tiltak som må til for å forhindre disse feilene. Tar man utgangspunkt i definisjonene og beskrivelsene av sikkerhetskultur er det tydelig at man også her legger vekt på forhold ved organisasjonen, hvor det å skape et felles verdigrunnlag og en kollektiv bevissthet og forståelse er det som står i fokus. Og som Reason (1997) sier: «You cannot change the human condition, but you can change the conditions under which people work» (Reason, 1997, s. 223). Dette innebærer at man må se på feilhandlinger som en del av et større bilde, hvor det er forhold utenfor individets kontroll som i stor grad kan lede til disse feilhandlingene.

Som nevnt fra teorien er det altså samspillet mellom menneske, teknologi og organisasjon som sammen kan bidra til å forhindre digitale angrep. Mennesker vil aldri slutte å gjøre feil, men nettopp derfor er de også en så stor og viktig del av sikkerhetsarbeidet. Ved å sette inn tiltak på organisatorisk nivå opp mot bevisstgjøring og økt forståelse, gir man de ansatte muligheten til å beholde en viss grad av autonomi og en følelse av at de betyr noe, og dette kan i sin tur føre til en opplevelse av større eierskap og mer forutsigbarhet (Wiley, McCormac & Calic, 2019) – noe som ut fra informantenes forklaringer ofte har vist seg å være en mangelvare når det kommer til digital sikkerhet. Med en slik «aktør-kultur» er det

større sjanse for at de ansatte evner å håndtere uforutsette hendelser, nettopp fordi de har blitt tillagt større grad av selvstendighet og handlingsrom fremfor å kun være vant til å følge detaljerte instrukser (Kvalnes, 2010, s. 139). Digitale angrep kan være svært komplekse og uoversiktlige, hvor man ikke kan lage slike detaljerte instrukser for ethvert scenario. Man bør derfor vise en tillit til de ansatte som gjør at de stoler mer på egen kunnskap når det kommer til digitale hendelser, og dermed også sier ifra dersom de opplever unormale eller uønskede situasjoner. Det vil riktignok alltid være ulike behov i ulike virksomheter og etater, og byggingen av en god sikkerhetskultur må derfor også tilpasses lokale forhold for å ivareta de krav og interesser som virksomheten har (Kvalnes, 2010; Bada et al., 2019). Men det å legge til rette for en digital sikkerhetskultur hvor de ansatte er bevisste på deres egen rolle for å forhindre digitale angrep, vil uten tvil være av stor betydning for den digitale sikkerheten, nettopp fordi teknologiske løsninger aldri vil kunne forhindre at mennesker gjør en feil og klikker på noe som i ytterste konsekvens kan omgå så å si alle sikkerhetsbarrierer.

5.1.6 Sikker digital atferd – selve målet med en god digital sikkerhetskultur

Organisasjonsteori dreier seg i stor grad om atferdsvitenskap, og det sentrale er dermed menneskers atferd og hvordan man kan påvirke den (Jacobsen & Thorsvik, 2013). Kulturen kan altså benyttes som et styringsmiddel for å angi hva som er passende atferd, og når det kommer til det å bygge en god sikkerhetskultur er målet å påvirke de ansattes holdninger og verdier slik at de til syvende og sist også utøver en *sikker atferd* (Weick & Sutcliffe, 2015; Kvalnes, 2010). Dette binder dermed alle funnene sammen – sikker atferd er selve «finalen» i sikkerhetsarbeidet, hvor hele prosessen med bevissthet og risikoforståelse, holdninger, ledelse og læring knyttes sammen og har betydning for om man lykkes med å oppnå dette eller ei. En god sikkerhetskultur betyr dermed at man har klart å få sikkerhet til å bli en del av den overordnede kulturen i organisasjonen, og på den måten har fått det til å bli en del av de dagligdagse prosessene (Gjertsen et al., 2017).

Knyttet opp mot digital sikkerhetskultur innebærer en sikker atferd blant annet i hvor stor grad de ansatte evner å identifisere phishing e-poster og håndterer dem riktig, om de klarer å skille mellom sikre og usikre linker og nettsider, og om de har en god passord-forståelse (NorSIS, 2020; Krombholz et al., 2014). Man ønsker altså at de ansatte jobber *med* teknologien og de sikre systemene, og ikke mot dem gjennom å ta usikre snarveier, slik at de bidrar til det samspillet som fører til færre digitale angrep og uønskede hendelser. Kunnskap

og kompetanse er viktig for å øke forståelsen, og forståelsen er igjen avgjørende for å bidra til bedre holdninger og mer sikker atferd gjennom for eksempel å følge de sikkerhetskrav og -rutiner som er satt. Som tidligere nevnt mente imidlertid mange av informantene mine at det manglet en grunnleggende forståelse for digital sikkerhet blant de ansatte, og at dette var en av årsakene til at man også kunne se en mangel på sikker digital atferd. Flere mente derfor at det å forklare hvorfor man har disse sikkerhetskravene og -rutinene og hva de bidrar til, ville øke sjansene for at de ansatte fulgte dem.

Økt bevissthet og forståelse vil dermed utvilsomt bidra til en sikrere atferd, men i tillegg til dette er det imidlertid også en annen viktig faktor som kan spille inn, nemlig mangel på sikker atferd *på tross av* at kunnskapen øker (Bergsjø et al., 2020; Bada et al., 2019; Khan et al., 2011). Både Stian og Thomas fra finanssektoren trekker frem dette som en utfordring. Stian påpeker at det er én ting å ha masse sikkerhetskrav og -rutiner, men det er noe helt annet å få folk til å faktisk følge dem. Thomas har på sin side erfaringer med ledere som bevisst tar mer risiko enn de burde gjøre, fordi de opplever at sannsynligheten for at noe skal skje er så lav at det er verdt å omgå sikkerhetstiltakene for å være mer effektiv. Dette trekker meg tilbake til utfordringen med sikkerhet versus produksjon, hvor det å også ha fokus på brukervennlighet er et sentralt poeng når det kommer til utviklingen av sikre systemer og det å få ansatte til å faktisk etterleve sikkerhetskravene (Bada et al., 2019).

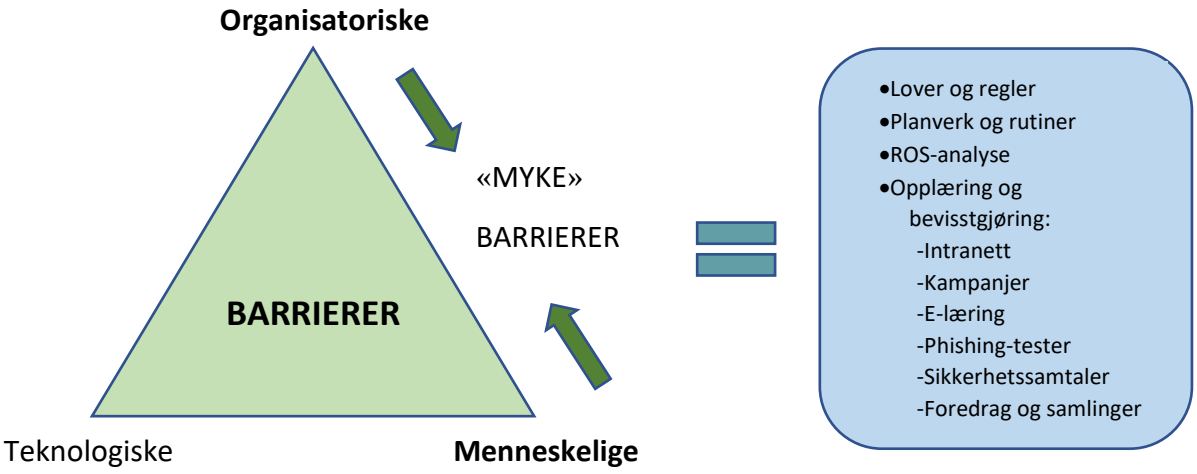
I tillegg opplever også mange at digital sikkerhet er noe fremmed og noe som er utenfor deres kontroll, og som dermed påvirker deres risikoforståelse og atferd i negativ retning (Kvalnes, 2010; Cone et al., 2007). Knut (justissektoren) trekker frem et eksempel på dette når han opplever at folk har et greit nivå med tanke på bevisstheten og bekymringene rundt digitale angrep, men at de er usikre på om de kan gjøre noe med det og dermed fortsatt bruker enkle passord og andre ting som er i strid med anbefalingene og reglene. Denne opplevde mangelen på kontroll og en følelse av at man kun er en brikke i det store systemet, kan medføre en passivitet i atferden (Kvalnes, 2010). Et tiltak som kan være med på å løse disse utfordringene er å involvere de ansatte i prosessen med å utarbeide rutiner, tiltak og systemer for digital sikkerhet. Dette kan bidra til å gi dem både økt forståelse og et slags eierskap til feltet, samtidig som man kanskje i større grad kan ivareta balansen mellom sikkerhet og brukervennlighet for de som skal bruke systemene. Dette kan i sin tur være med på å øke motivasjonen til å følge de kravene som blir satt (Wiley et al., 2019; Bada et al., 2019; Khan et al., 2011).

5.2 Barrierer

Under denne kategorien viderefører jeg overskriftene fra funnkapittelet, og vil derfor drøfte følgende temaer:

- Forebyggende arbeid og «myke» barrierer
- Spesifikke tiltak for opplæring og bevisstgjøring

Som tidligere nevnt er jeg opptatt av å få frem hvor viktig det forebyggende arbeidet er, og at et godt arbeid i forkant kan spare virksomheter for både tid, penger og omdømme ved å unngå alvorlige digitale hendelser. Barrierer og tiltak deles gjerne inn i tre ulike kategorier; teknologiske, organisatoriske og menneskelige (Reason, 1997, s. 2; NorSIS, 2020; NSM referert i Bergsjø, Windvik & Øverlier, 2020). Innenfor dette har fokuset mitt vært på organisatoriske og menneskelige tiltak som fremmer en sikker digital atferd, og tiltakene jeg har valgt å se på er derfor knyttet opp mot bevisstgjøring og opplæring. Dette er såkalte «myke» barrierer som ifølge Reason (1997, s. 8) dreier seg om en kombinasjon av papir og mennesker. Selv om både rutiner og planverk også er en viktig del av det forebyggende arbeidet opp mot å forhindre digitale angrep, mener jeg at det er bevisstgjøringen av de ansatte som ligger i bunn for alt dette og som i sin tur avgjør om krav og rutiner blir fulgt eller ikke. Reason (1997) understreker også at barrierer på laveste nivå skal sørge for å skape forståelse og bevissthet rundt de truslene virksomheten står overfor, noe som er selve målet med tiltakene innen opplæring og bevisstgjøring.



Figur 5.2. En oversikt over de tre ulike formene for barrierer, samt eksempel på tiltak som er nevnt både fra informantene og fra teorien inn under kategorien «myke» barrierer.

5.2.1 Forebyggende arbeid og «myke» barrierer

Jeg har til nå sett på hvordan den digitale sikkerhetskulturen i virksomhetene oppleves av de som jobber med feltet, og hvilke faktorer som har stor betydning for dette arbeidet og som derfor bør prioriteres. Når man har fått på plass dette burde man også være innforstått med at forebyggende tiltak er avgjørende for å unngå uønskede hendelser og digitale kriser. Noe av problemet med forebyggende arbeid er imidlertid at det ofte blir nedprioritert til fordel for hendelseshåndtering, noe også flere av informantene påpekte. Daniel (justissektoren) poengterte at forebyggende arbeid er mindre synlig og vanskelig å måle effektene av, og dette samsvarer med det Reason (1997, s. 4) hevdet om utfordringene med sikkerhetsarbeid, nemlig at det ofte bare er rett etter en hendelse eller nesten-ulykke man har fokus på det, og at man deretter faller bakpå igjen. Noen kan også tenke at fordi de ikke opplever eller har opplevd mange digitale angrep så er de gode på å forebygge det. Men dette kan være langt fra sant; det kan rett og slett skyldes flaks eller andre forhold som gjør at man har vært heldig å unngå en uønsket hendelse. Dårlige handlinger kan føre til gode resultat, og riktige handlinger kan også lede til et uønsket resultat. Man må derfor skille mellom handling og konsekvens, og ikke tro at alt er bra selv om man tilsynelatende har klart å unngå en alvorlig hendelse (Kvalnes, 2010).

Digitale angrep kan ta mange ulike former, men felles for mange av dem er at de benytter seg av såkalt sosial manipulasjon. Angriperne spiller på følelser som frykt, skam, nysgjerrighet og økonomi for å nevne noen, og tiltak for å øke bevisstheten rundt slike angrep må derfor i stor grad baseres på teori innen både psykologi og læring så vel som innen sikkerhet (Nätt & Heide, 2015; Gjertsen et al., 2017; Khan et al., 2011). Dette fordi kunnskap og overføring av informasjon alene ikke er nok for å endre atferd, man må i tillegg også forstå bakgrunnen for menneskers handlinger, blant annet oppfatning av risiko og motivasjon for å endre atferd (Krombholz et al., 2014; Nyeste & Mayhorn, 2010; Bada et al., 2019; Khan et al., 2011; Smith & Ali, 2019). Dette gjør at det stilles høyere krav til opplæringsprogrammer enn det kanskje mange har tatt innover seg, og dette kan vises gjennom uttalelser fra mange av informantene hvor de forteller at virksomheten ikke har noen strategi eller system for bevisstgjøring og opplæring. Det blir dermed ikke noe kontinuerlig og fastsatt opplegg på det, men det blir mer sporadisk og tilfeldig.

I likhet med manglende strategi og system for opplæring og bevisstgjøring, er en av de største utfordringene også å nå ut til ulike miljøer i virksomhetene. Disse miljøene har utviklet sine egne subkulturer, hvor synet på sikkerhet og risiko kan variere i stor grad. Bada et al.,

(2019) understreker derfor at kulturelle ulikheter er en av de viktigste faktorene man må ta i betraktning når man designer og utvikler trenings- og bevisstgjøringsprogrammer. Dette innebærer at man må tilpasse opplæringen til ulike målgrupper slik at det passer overens med både nåværende kunnskaps- og kompetansenivå og risikoen de faktisk står overfor, slik at det fremstår som relevant og dermed mer motiverende å gjennomføre (Smith & Ali, 2019; Bada et al., 2019; Gjertsen et al., 2017; Digdir, 2021). Dette er noe både Trine og Stian (begge finanssektoren) påpeker, og Trine viste også hvordan ledere kan være med på å undergrave et opplæringsprogram dersom de selv ikke har en forståelse av hvor viktig det er. Hun påpeker derfor at det å kjenne de ulike kulturene i virksomheten er veldig viktig når man skal utarbeide slike programmer, og mangel på dette er mye av grunnen til at mange bevisstgjøringsprogrammer har vist seg å være lite effektive og feiler i å oppnå målet om en sikrere atferd (Gjertsen et al., 2017;

En måte å løse dette på er å gjennomføre målinger eller undersøkelser som gir en viss formening om det nåværende kompetansenivået slik at man både kan avdekke eventuelle gap mellom nåværende situasjon og ønsket situasjon, samt gjøre det lettere å tilpasse opplæringen ut fra dette (Laumann, 2011; Gjertsen et al., 2017). I finanssektoren har de gjennomført det de kaller holdningsundersøkelser og sikkerhetskulturundersøkelser, nettopp for å kunne få en pekepinn på hvordan «ståa» er. Samtidig vil det å måle holdninger i større grad kunne si noe om fremtidig atferd, og det er det man i hovedsak ønsker å kartlegge (Bergsjø, Windvik & Øverlier, 2020; NorSIS, 2018). Det blir imidlertid også påpekt at det er vanskelig å måle holdninger, og dette viser at noe av utfordringen med slike undersøkelser er at man ikke med 100 % sikkerhet kan si at de svarene folk gir samsvarer med deres faktiske holdninger, da mange kan svare på en måte som de tror er best eller mest riktig. Det å kombinere ulike metoder fremfor å kun bruke for eksempel spørreskjema, som er det de fleste benytter seg av når de gjennomfører slike undersøkelser, vil derfor gi et bedre bilde av hvordan sikkerhetskulturen i organisasjonen er. Dette kan man oppnå gjennom å kombinere spørreundersøkelser, intervju og observasjon, benytte longitudinelle studier fremfor tverrsnittundersøkelser, dele beste praksis, samt læring fra erfaring og forskningsfunn. (Patankar og Sabin,referert i Laumann, 2011, s. 285; Bang, 2011). Dette er imidlertid metoder som krever mye tid og ressurser, og det er dermed ikke noe man kan forvente at spesielt små og mellomstore virksomheter skal gjennomføre. En spørreundersøkelse alene vil kanskje ikke gi et fullverdig svar på hvordan tilstanden er, men den vil uansett gi et svar som er godt nok til å bruke som utgangspunkt for videre opplærings- og bevisstgjøringstiltak.

5.2.2 Spesifikke tiltak for opplæring og bevisstgjøring

Det var kun Trine fra finanssektoren som fortalte at de i hennes virksomhet har et innarbeidet system for opplæring og bevisstgjøring. Der har de imidlertid også egne ansatte som jobber med «awareness», noe som viser at det er satt fokus på det fra ledelsens side og at det dermed også blir prioritert og jobbet kontinuerlig med over tid. Dette er noen av suksessfaktorene for å lykkes med dette arbeidet, men i tillegg er det også noen fallgruver å gå i når det kommer til de spesifikke tiltakene man kan iverksette. Jeg vil derfor ta for meg de ulike tiltakene som ble nevnt av informantene i deres arbeid med bevisstgjøring og opplæring, og se på hvilke styrker og svakheter de har slik at det kan bli lettere å sette opp et slik program for andre som også jobber med dette. Jeg har valgt å drøfte de i en rekkefølge ut fra antatt effektivitet og oppnådd læringsutbytte, med de tiltakene som fremstår å være minst effektive til å begynne med, til de som virker å være mest effektive til slutt.

5.2.2.1 Intranett

Det å legge ut informasjon på intranettet er ett av to tiltak som virker å være mest brukt for å nå ut til de ansatte med informasjon om digital sikkerhet. Det legges ut informasjon om både hendelser som har skjedd, ting de bør være oppmerksomme på, samt tips og triks om hvordan de ansatte skal opptre for å ivareta den digitale sikkerheten i virksomheten. Det er altså mye god informasjon som legges ut, men problemet er at dette er noe de ansatte selv aktivt må oppsøke og klikke seg inn på. Dette ble også påpekt av flere av informantene, og sett på som en åpenbar svakhet med dette tiltaket. Som jeg var inne på tidligere i oppgaven er det i stor grad vår egen interesse som styrer hva vi søker informasjon om og hva vi ønsker å lære mer om, og de som da klikker seg inn og leser denne informasjonen er dermed gjerne de som allerede er interessert i feltet og mest sannsynlig allerede har en del kunnskap om det (NorSIS, 2020; Bada et al., 2019; Khan et al., 2011). Samtidig er det en veldig god mulighet for å nå ut til mange, men det bør ikke brukes som eneste tiltak innen opplæring da det ikke nødvendigvis treffer de som trenger det mest.

5.2.2.2 Kampanjer

Sammen med informasjon på intranett, er kampanjer noe alle virksomhetene trekker frem som et viktig tiltak for å øke bevisstheten rundt digital sikkerhet. Det er i all hovedsak Nasjonal sikkerhetsmåned i regi av NorSIS som blir brukt i dette arbeidet, og her understreker flere at

de har full støtte fra toppledelsen og nedover, og at dette er noe som blir satset på. Mange kombinerer de ferdige opplæringsmodulene fra NorSIS med egne tilleggsmoduler for å utnytte denne måneden maksimalt. Kampanjer av denne typen er bra i den forstand at de åpenbart kan få bred oppslutning og støtte i hele organisasjonen, og at man har mulighet til å gå gjennom mange ulike temaer og utfordringer i løpet av kampanjeperioden. Utfordringen ligger imidlertid i at dette ofte kun blir en enkeltstående greie man gjør én gang i året, for så å legge det helt dødt til neste kampanje året etter (Gjertsen et al., 2017). Da risikerer man at mye av det man har lært er glemt innen man får neste påfyll.

I tillegg vil en slik kampanje som dette, som er lagd for å kunne brukes på tvers av både virksomheter og sektorer, være såpass generell at den ikke nødvendigvis treffer den aktuelle virksomheten med tanke på hvilke trusler og farer de står overfor. Den vil dermed ikke være tilpasset den enkelte virksomhet eller organisasjon, og kan dermed oppleves som mindre relevant (Bada et al., 2019; Smith & Ali, 2019; Departementene, 2019b; Digdir, 2021). Samtidig er det, som Thomas fra finanssektoren påpekte, stort sett de samme angrepsmetodene man står overfor både i og utenfor egen sektor, slik at en generell kampanje burde likevel treffe de fleste med noen overordnede mål og prinsipper for digital sikkerhet. Kampanjer blir også som regel lagt opp kun som overføring av kunnskap, noe som i sin tur kan bidra til at det ikke resulterer i noen faktisk endring i atferd og bevissthet (Smith & Ali, 2019; Bada et al., 2019). Det er derfor bedre å bruke det som en del av et bredere opplegg hvor man også kan legge til rette for mer tilpasset opplæring, samt muligheter for diskusjon og refleksjon.

5.2.2.3 E-læring

Databasert trening, eller såkalt e-læring, er en veldig enkel og kostnadseffektiv læringsmetode med tanke på hvor mange man når ut til og hvor lite tid og ressurser som kreves for å gjennomføre det, både for de som er ansvarlig og for de som skal utføre det. Det finnes mange ferdiglagde programmer som virksomheter kan benytte seg av, og det er fleksibelt i den forstand at de ansatte kan gjennomføre det når det måtte passe dem i og med at det alltid er tilgjengelig (Khan et al., 2011). Det er i tillegg en enkel metode som kan benyttes til jevnlig opplæring, noe som Trine (finanssektoren) forteller at de benytter seg av ved å sende ut månedlige e-læringsprogrammer gjennom hele året, og skreddersyr team for hver gang.

Det er imidlertid ikke nok å bare sende ut slike e-læringsmoduler og forvente at læringsutbyttet blir høyt bare av den grunn. For det første krever det at de ansatte faktisk gjennomfører det, noe som i seg selv kan være utfordrende nok i en travel arbeidshverdag. For det andre er det ofte ferdiglagde programmer som ikke er spesifikt tilpasset den enkelte virksomheten, noe som kan ha en demotiverende effekt (Bada et al., 2019; Khan et al., 2011). For det tredje er det en relativt passiv form for trening som ikke legger opp til noen videre dialog for å utfordre brukeren og øke forståelsen (Cone et al., 2007; Khan et al., 2011). Alle disse faktorene gjør at det dermed ofte kan ende opp som noe man bare «klikker seg gjennom» uten å reflektere noe videre rundt det, noe også Camilla (kraftsektoren) påpekte som en svakhet med disse programmene. Man kan riktignok gjøre ulike tilpasninger på disse e-læringsprogrammene for å få de til å bli mer relevante for egen virksomhet, men de blir i likhet med kampanjene likevel kun en måte å formidle informasjon på og dermed ikke en veldig effektiv treningsform i seg selv, og bør derfor også kombineres med andre tiltak.

5.2.2.4 Phishing-tester

Det å sende ut phishing-tester er en konkret måte for å teste brukernes bevissthet rundt digital sikkerhet og deres rolle i dette. Prosessen går ut på at man sender ut falske e-poster med «infiserte» vedlegg eller linker, hvor formålet er at brukerne skal oppdage at dette ikke er en sikker avsender og dermed avstår fra å åpne vedlegg eller klikke på linken, og varsler videre om mottaket av e-posten. Deretter kan man blant annet hente ut statistikk og se hvor mange som faktisk klikket på noe de ikke skulle, og se hvor mange som varslet videre. Man kan dermed få et helt konkret tall på hvordan det står til med den digitale bevisstheten blant de ansatte og hvilken sårbarhet virksomheten står overfor når det kommer til de ansattes atferd på nett.

Det er imidlertid ikke nok å bare sende ut disse e-postene og gi brukerne et helt enkelt svar på om de gikk på svindelen eller ikke. For å sikre et bedre læringsutbytte av både e-læringsprogrammer og phishing-tester er det derfor en god løsning å legge inn mulighet for direkte tilbakemeldinger. Dette kan for eksempel gjøres gjennom å sende en e-post til brukeren umiddelbart etter at vedkommende har klikket på en phishing-link hvor han eller hun får beskjed om hva vedkommende har gjort feil og hvilke konsekvenser det kan ha (Nyeste & Mayhorn, 2010). Dette kan både føre til en økt bevissthet rundt det å oppdage fremtidige phishing-angrep, samtidig som det kan gi en bedre risikoforståelse med tanke på de

truslene man faktisk står overfor. Dette var også noe Trine (finanssektoren) fortalte om, hvor de prøver å lage slike opplegg hvor brukeren blir sendt direkte videre til en opplæringsmodul dersom vedkommende har klikket på et vedlegg eller link.

Dette ser altså tilsynelatende ut til å være en grei måte å både teste og øke bevisstheten til de ansatte på, men overraskende nok var det bare to av informantene som fortalte at de hadde gjennomført slike tester. Både de og flere av de andre trakk frem en viktig grunn til at mange kanskje avstår fra akkurat dette, nemlig det faktum at mange opplever det som en «utdritningskampanje» hvor målet er å henge ut de som trykker på noe feil. Knut (justissektoren) fortalte at deres phishing-kampanje ble stoppet av for han ukjente grunner, men at han mistenkte at dette var fordi flere ledere hadde gått på forsøket og dermed følte seg uthengt. I likhet med informasjons- og erfaringsdeling ellers er det altså også her problemer med at frykt og flauhet hindrer gjennomføringen av slike tester, noe som til syvende og sist kan gå utover læringen i sin helhet (Kvanles, 2010). Både Trine og Stian (begge fra finanssektoren) påpekte derfor at dataene fra slike kampanjer må brukes på en saklig måte hvor man ikke nødvendigvis publiserer resultatene, men heller benytter det til intern bruk opp mot videre opplæring og bevisstgjøring.

5.2.2.5 Sikkerhetssamtaler

Både Trine (finanssektoren) og Steinar (kraftsektoren) forteller at de gjennomfører såkalte sikkerhetssamtaler med nyansatte i virksomheten. Her går de gjennom og forklarer litt rundt sikkerheten i virksomheten, og hvilke regler og rutiner som gjelder. Av erfaring vet jeg at også justissektoren har slike samtaler med personell som skal jobbe med sikkerhetsgradert informasjon. Dette er en god mulighet til å forklare og begrunne hvorfor det er viktig at alle ansatte er bevisst sin egen rolle i arbeidet med sikkerhet, og samtidig kunne svare på spørsmål de måtte ha rundt dette. Det legger altså til rette for en viss dialog og mulighet for diskusjon. Når det kun gjennomføres samtaler med nyansatte er det imidlertid en viss fare for at informasjonen som blir gitt bærer preg av å være ganske monoton og kjedelig, og at det blir en enveis-dialog fra den som sitter og har samtalen. Det kan bli mye oppramsing av lover og regler, og for en nyansatt som allerede har mye annet å sette seg inn i, kan det dermed fort bli noe som er glemt i det man går ut døren. I tillegg er det ikke alltid så lett å være ny og skulle stille spørsmåltegn ved hvorvidt de rutinene og reglene man blir presentert er fornuftige og fungerer etter hensikten. Det kan derfor være en bedre løsning å gjøre slik som Steinar

(kraftsektoren) forteller at de nå er i gang med, nemlig å gjennomføre disse samtalene med *alle* ansatte som har tilgang til sensitiv informasjon. Ved å gjøre dette vil disse samtalene i større grad kunne føre til en dialog og diskusjon rundt det som blir presentert, både fordi eldre ansatte har gjort seg noen erfaringer i løpet av tiden de har vært der, og at de i større grad tør å komme med det. Likevel vil det også her være et spørsmål om tid og ressurser, da det å gjennomføre en slik samtale med alle ansatte vil kreve mye arbeid fra de som skal gjennomføre det. Det kan derfor være en mulighet å se på om det er noen utvalgte miljøer man heller burde fokusere på, og gjennomføre slike samtaler med disse fremfor alle i hele virksomheten.

5.2.2.6 Foredrag og samlinger

Foredrag og samlinger blir nevnt av flere av informantene som noe de prøver å gjennomføre med ulike deler av virksomheten. Dette tiltaket er i motsetning til mange av de andre tiltakene noe som i mye større grad tilrettelegger for både mer tilpasning og diskusjon blant både deltakerne og mellom deltakerne og instruktørene. Det er dermed større muligheter for å dele erfaringer og opplevelser, noe som jeg tidligere har vist er avgjørende for å bli en lærende organisasjon som evner å forbedre seg. Denne formen for opplæring har mange gode kvaliteter, og anses derfor som et effektivt tiltak for å øke bevisstheten blant de ansatte. Det scorer derfor høyt på effektivitet og læringsutbytte, og er noe alle virksomheter burde benytte seg av, gjerne i kombinasjon med andre opplæringsformer for å danne et enda bedre diskusjonsgrunnlag (Khan et al., 2011).

Det krever imidlertid en del mer tid og ressurser enn det for eksempel e-læring gjør, noe som kanskje bidrar til at det ikke blir brukt i like stor grad. I tillegg påpeker Lars fra justissektoren at det er veldig viktig at de som holder foredragene er gode på å formidle budskapet slik at de ansatte faktisk forstår det, og ikke bare er sikkerhetseksperter som snakker i vei om avansert teknologi og bruker kompliserte faguttrykk og illustrasjoner (Bada et al., 2019). Camilla (kraftsektoren) var riktignok inne på noe veldig viktig når hun sa at hun trodde at det å bli fortalt og vist litt av de truslene og sårbarhetene man står overfor, gjorde et mye større inntrykk enn å bare klikke seg gjennom en e-læringsmodul eller lese informasjon på intranett. Hun sa at man da kan få gjort noe litt mer spennende ut av det, og at det da kanskje ligger litt mer i bakhodet når man skal gjennomføre en e-læringskampanje senere. Det å holde foredrag og presentasjoner er derfor noe som i likhet med de andre tiltakene gjerne

kan kombineres med andre former for opplæring, både for å skape et bedre diskusjonsgrunnlag og en viss progresjon, men også for å spare noe tid og ressurser på gjennomføringen av opplæringsprogrammet

5.2.2.7 Oppsummering

Jeg har nå gått gjennom de ulike tiltakene som ble nevnt av informantene i arbeidet deres med digital sikkerhet. Noen viser seg som mindre effektive enn andre, men i all hovedsak dreier det seg om at et opplærings- og bevisstgjøringsprogram må være godt forberedt og organisert, noe som krever et fokus fra både ledelsen og ansatte som jobber med digital sikkerhet. Digitaliseringsdirektoratet påpekte i sin rapport fra 2018 at mange virksomheter arbeider med kompetanseheving, men at det ofte er lite målrettet og ikke tilpasset virksomheten og de ulike målgruppene, og en tilrettelegging ut fra trusler og behov er derfor viktig for å skape et engasjement (Digdir, 2018). Man bør også kombinere ulike tiltak, sørge for jevnlig gjennomføring og opplæringen bør i hovedsak være basert på frivillighet. I tillegg må det, i henhold til teorier om læring, legges til rette for refleksjon og diskusjon slik at man faktisk oppnår en dypere forståelse for risikoen man står overfor. På denne måten vil man i større grad kunne øke den kollektive bevisstheten rundt digital sikkerhet, og dermed også gi de ansatte mer motivasjon til å endre sin egen digitale atferd (Weick & Sutcliffe, 2015; Krombholz et al., 2014; Nyeste & Mayhorn, 2010; Bada et al., 2019; Khan et al., 2011; Smith & Ali, 2019).

Som jeg har vist gjennom drøftingen av de ulike tiltakene er det riktignok ingen av dem som alene kan sies å være effektiv nok til å bedre den digitale bevisstheten blant de ansatte. Den beste løsningen for et effektivt opplærings- og bevisstgjøringsprogram er derfor å kjøre en hybrid læringsmodell som kombinerer ulike tiltak. På denne måten har man mulighet til å utnytte det beste i hvert enkelt tiltak og få til en løsning som også fungerer over tid fordi man i større grad forhindrer at mottakerne går lei (Bada et al., 2019; Gjertsen et al., 2017). Men et opplæringsløp innen digital sikkerhet kan ikke bare rulle og gå uten noen form for evaluering eller endring; den teknologiske utviklingen skjer i rekordfart, og likeså utviklingen av nye trusler og sårbarheter. I tillegg er kan man ikke sette seg ned og tro at opplæringen fungerer etter hensikten uten å foreta noen form for evaluering eller tilbakemelding fra de som faktisk gjennomfører den. Opplæringen må derfor endres og utvikles i takt med dette, og

samtidig gjentas slik at de ansatte hele tiden er oppdatert på det siste som gjelder av trusler og konsekvenser (Bergsjø et al., 2020; Gjertsen et al., 2017).

6 Konklusjon

Digital sikkerhet er et felt det blir stadig mer fokus på etter hvert som den teknologiske utviklingen for alvor preger både drift og produksjon innenfor samfunnskritiske funksjoner. Digital sikkerhetskultur er dermed et høyaktuelt tema, og gjennom denne oppgaven har jeg sett på hva som kjennetegner denne kulturen innen samfunnskritiske funksjoner. Ut fra dette har jeg kartlagt fire områder som har stor betydning for arbeidet med å skape en god digital sikkerhetskultur: 1) risikoforståelse, bevissthet og holdninger, 2) ledelsens rolle, 3) varsling og læring, og 4) sikker atferd. I tillegg har jeg sett på hvilke forebyggende tiltak virksomhetene har når det kommer til opplæring og bevisstgjøring av de ansatte og hvordan man på best mulig måte kan lage et opplæringsprogram som fungerer etter hensikten og bidrar til en sikrere digital atferd blant alle ansatte.

Lengst fremme med dette arbeidet ligger finanssektoren, som i flere år har ansett seg selv for å være en heldigital virksomhet og derfor også har hatt større fokus på digitale angrep fremfor andre typer krisehendelser. Kraft- og justissektoren henger litt etter, men også de har innsett at digitale hendelser i stadig økende grad preger risikobildet, samtidig som de fortsatt er nødt til å forholde seg til de mer tradisjonelle krisehendelsene utløst at natur- og værkatastrofer, brann, og andre typer ulykker. Fagpersonell som jobber med digital sikkerhet har en god forståelse for hvilke trusler og sårbarheter virksomheten står overfor, men det kan være utfordrende å nå ut til alle ansatte i virksomheten med dette. Sikkerhet og sikkerhetstiltak blir av mange sett på som tungvint og noe som hindrer effektiviteten i arbeidet deres, og de som ikke jobber med eller måles på sikkerhet har også ofte en manglende forståelse for de truslene man står overfor og hvilke konsekvenser de kan ha for virksomheten. I tillegg vektlegger de produksjon fremfor sikkerhet, noe som fører til at usikre snarveier fremstår som mer effektivt og positivt både for dem selv og virksomheten enn å følge de sikre løsningene. Selv om finanssektoren ligger lengst fremme med tanke på fokus på digital sikkerhet, er det også her man ser ut til å møte mest utfordringer når det kommer til det å nå ut til de ansatte om viktigheten av å tenke på sikkerhet. Et tøft konkurransemarked hvor kravet om effektivitet og produktivitet kanskje er større enn i offentlig sektor, kan dermed være én av årsakene til at det oppleves som mer vanskelig å skape gode holdninger til sikkerhet og nødvendige sikkerhetstiltak.

Ledere vil alltid være en nøkkelbrikke når det kommer til dette arbeidet, og manglende strategier og fokus på sikkerhet kan føre til uklare ansvarsforhold, spesielt innen digital

sikkerhet da dette er et relativt nytt felt. Ledelsen må derfor sørge for at arbeidet med digital sikkerhet er forankret helt på toppen, og de må utarbeide policyer og rutiner som blir kommunisert ut til ansatte og ledere på alle nivå. For å klare dette er de imidlertid avhengige av å få viktig og riktig informasjon om trusselbildet, og god kommunikasjon med ledelsen er derfor avgjørende for å skape en god forståelse for sikkerhetsarbeidet. Videre vil en ledelse som går foran som gode eksempler og innrømmer egne feil, fremme åpenhet og legge til rette for en god varslings- og rapporteringskultur. Dette er viktig dersom man ønsker å lære av tidligere hendelser og være bedre i stand til å forhindre fremtidige digitale angrep. De ansatte er en verdifull informasjonskilde i dette arbeidet, men det krever et system som gjør det enkelt og lite tidkrevende å varsle og rapportere om feil og uønskede hendelser.

For å øke de ansattes bevissthet når det kommer til digital sikkerhet er det viktig med et ordentlig opplærings- og bevisstgjøringsprogram. Det er mange ulike tiltak som kan benyttes i dette arbeidet, men det beste er å velge en hybrid læringsmodell som kombinerer de «enkle» tiltakene med de som er ansett å være mer effektive, men også mer tidkrevende. E-læring kan for eksempel kombineres med foredrag og presentasjoner som legger til rette for dialog og diskusjon slik at læringen kan tilpasses og bidra til mer refleksjon rundt temaet. På denne måten vil man i større grad kunne lykkes med å øke de ansattes forståelse for sin egen rolle innen arbeidet med digital sikkerhet, samt deres motivasjon til å etterleve sikkerhetstiltak, noe som vil bidra til at de får en sikrere digital atferd.

6.1 Praktiske og teoretiske implikasjoner

I denne oppgaven har jeg intervjuet informanter fra tre ulike sektorer innen samfunnskritiske funksjoner, og tanken bak dette var å få frem både likheter og ulikheter mellom virksomhetene for på den måten å kunne sammenligne og trekke konklusjoner på bakgrunn av mer variasjon. Dette har bidratt til å gi en bredde som gjør at resultatene i større grad kan brukes i arbeidet med digital sikkerhetskultur også for andre virksomheter. Veldig mye av informasjonen som fremkom viste seg imidlertid å være gjeldende for alle virksomhetene, noe som viser at arbeidet med digital sikkerhetskultur i stor grad vil være ganske likt uavhengig av hvilken bedrift eller sektor man tilhører.

Jeg valgte å ta utgangspunkt i teori innenfor sikkerhetskultur generelt da det ikke finnes noen konkrete teorier knyttet til begrepet digital sikkerhetskultur. Det er imidlertid gjennomført en del nyere forskning på dette området hvor det stadig blir påpekt at mennesker

er det svakeste leddet i dette arbeidet, og at det derfor er avgjørende å skape bevisste ansatte som har en sikker digital atferd og som unngår å bli brukt i digitale angrep. Det har imidlertid manglet en kobling opp mot mer anerkjente teorier innen sikkerhet, og jeg har derfor med denne oppgaven fylt et tomrom som viser denne problematikken fra et systemperspektiv. Dette er i sin tur med på å beskrive hvilke faktorer som påvirker den digitale sikkerhetskulturen og hvilken betydning de har for det praktiske arbeidet.

Gjennom mine undersøkelser fant jeg en stor grad av samsvar mellom mine empiriske funn og teorien på området, og mine fire hovedkategorier innen digital sikkerhetskultur går igjen i flere ulike teorier om sikkerhetskultur. Funnene mine viser imidlertid også at enkelte faktorer spiller en viktigere rolle innen arbeidet med digital sikkerhetskultur enn innenfor de mer tradisjonelle teoriene, dette gjelder spesielt funn knyttet opp mot risikoforståelse, bevissthet og motivasjon. Det kan synes som om digital sikkerhet og digitale hendelser i større grad oppleves som mer fremmed, mindre personlig og utenfor individenes kontroll, noe som fører til en dårligere risikoforståelse. I tillegg vil en innføring av sikre digitale løsninger føre til mer arbeid og en mindre opplevd effektivitet blant de ansatte, noe som igjen gjør at motivasjonen til å følge dem kan bli lavere. Totalt sett viser imidlertid mine empiriske funn at arbeidet med å skape en god digital sikkerhetskultur ikke krever noe «spesielt» i forhold til mer tradisjonelle sikkerhetshendelser; selv om det kan virke mer komplekst og ukjent må man bare bryte det ned til de enkle og kjente faktorene som har betydning for det meste av sikkerhetsarbeid og -kultur.

Jeg ønsket også med denne oppgaven å få frem noen konkrete suksessfaktorer knyttet til arbeidet med digital sikkerhetskultur, slik at andre organisasjoner kan benytte seg av dette i deres eget arbeid på området. Hovedfunnene i oppgaven beskriver de faktorene det er viktig å ta hensyn til, og gjennom analysen og drøftingen har jeg kommet med mer konkrete forslag til hvordan man kan implementere disse i egen virksomhet. Videre har jeg også drøftet hvilke tiltak som er mest hensiktsmessige i opplæringsøyemed, og dermed forespeilet en opplæringsmodell som med stor grad av sannsynlighet kan bidra til at man lykkes med å skape bevisste og motiverte ansatte som er med på å forhindre alvorlige digitale angrep. Mine funn og analyser vil dermed være svært nyttig for andre som skal utarbeide strategier og policyer for arbeidet med å skape en god digital sikkerhetskultur, da de er basert på resultater fra virksomheter som er spesielt utsatt for denne type trusler og angrep, og igjen drøftet og sett i lys av anerkjente teorier innenfor sikkerhetskultur.

Tabell 6.1 viser en oversiktlig og lettfattelig kobling mellom forskningsspørsmål og hovedfunn fra empirien, samt hva de betyr både for det teoretiske arbeidet med digital sikkerhetskultur og for alle de som skal utarbeide konkrete policyer og strategier for digital sikkerhet innenfor sin egen virksomhet. Den er en videreføring av tabell 5.1 og oppsummerer forskningsspørsmålene og de empiriske funnene under «Hovedfunn» og «Detaljer». I tillegg settes dette i en større sammenheng ved å vise de teoretiske og praktiske implikasjonene oppgaven bidrar med.

Hovedfunn	Detaljer	Teoretiske implikasjoner	Praktiske implikasjoner
Bevissthet og risikoforståelse	• Digital sikkerhet oppfattes som fremmed og skummelt. • Mange ansatte har et naivt syn på truslene og hvordan en selv kan være interessant for trusselaktører.	• Risiko oppfattes subjektivt, og dersom digitale angrep oppleves fjernt i både rom og betydning kan risikoen oppleves som mindre enn det den faktisk er. • Ansatte som tror de er «uviktige» bidrar til økt sårbarhet for hele virksomheten.	• Gode risikovurderinger må brukes aktivt og basere seg på det faktiske trusselbildet. • Dette må kommuniseres ut i virksomheten slik at risikoforståelsen øker.
Holdninger	• Forretning og produksjon går foran sikkerhet. • Ulike holdninger hos ulike avdelinger i virksomhetene – mange ser på sikkerhet som en hindring for effektivt arbeid. • Mennesker vil aldri slutte å gjøre feil.	• Utfordrende å danne én felles sikkerhetskultur på tvers av ulike subkulturer i virksomheten. • Digitale feilhandlinger bør sees som en konsekvens heller enn en årsak – årsakene ligger gjerne i systemet i form av manglende opplæring og bevisstgjøring.	• Å endre holdninger tar lang tid og krever kontinuerlig arbeid. • Prioriter bevisstgjøring for å øke den grunnleggende forståelsen for sikkerhet og tiltak, og ivareta de ansattes autonomi. • Se på ulikhet som en kilde til utvikling.
Ledelse	• Uklare ansvarsforhold, manglende fokus og strategi. • Holdningene varierer, men det er en positiv utvikling mtp økt bemanning og økte bevilgninger. • Ledelsen må brukes aktivt som «bjellesauer».	• Ledelsen er sjelden utdannet innenfor sikkerhet, dette påvirker deres holdninger. • Ledelsen har også en subjektiv risikooppfattelse – dersom digital sikkerhet oppleves som fremmed gir det mindre fokus. • Lederes digitale atferd påvirker alle ansatte.	• Kommunikasjon er svært viktig – sørg for at ledelsen får viktig og riktig informasjon om risiko man står overfor. • Ledere er rollemodeller, de må gå foran som gode eksempler.
Varsling og læring	• Noe manglende system for effektiv og enkel varsling. • Det jobbes for å få bukt med frykt, flauhet og manglende aksept for å innrømme feil. • Informasjon deles, men taushetsbelagt informasjon gjør det vanskeligere. • Manglende system for læring.	• Erfaringer og opplevelser må settes i et system for at de skal kunne bidra til organisatorisk læring. • Tillit og trygghet er viktig for å skape en god arena for deling av informasjon og erfaringer. • Informasjons- og erfaringsdeling + *refleksjon* er avgjørende for å forhindre uønskede hendelser og bidra til læring.	• Enkelt og intuitivt system for varsling av feil/uønskede hendelser. • Bygge en god varslings- og rapporteringskultur – ledelsen er viktig! • Følg opp varsler og legg til rette for dialog og refleksjon.
Sikker atferd	• Naive holdninger og manglende forståelse sees i sammenheng med mindre sikker atferd. • Ansatte tar snarveier forbi de sikre løsningene – dårlig brukervennlighet.. • Usikker atferd på tross av økt bevissthet og kunnskap.	• Usikker digital atferd skyldes manglende forståelse for trusler og egen rolle/betydning. • Opplevd mangel på kontroll kan påvirke atferden negativt – ser seg selv som en passiv brikke og tror ikke man kan gjøre noe fra eller til. • Opplevd positiv gevinst av å omgå sikkerhetstiltak.	• Involver ansatte i prosessen med å utarbeide rutiner og tiltak for digital sikkerhet – kan øke forståelsen. • Ivareta balanse mellom sikkerhet og brukervennlighet – kan øke motivasjonen til å følge tiltak.
Forebyggende arbeid og tiltak for opplæring og bevisstgjøring	• Forebyggende arbeid kan ofte bli nedprioritert til fordel for hendelseshåndtering. • Manglende strategi og system for opplæring. • Vanskelig å nå frem til alle miljøer. • Sikkerhetskulturunders. • Kampanjer, e-læring, intranett, foredrag og samlinger, phishing-tester og sikkerhetssamtaler.	• Fravær av hendelser er ikke ensbetydende med god sikkerhet. • Psykologiske faktorer må tas i betraktning når det gjelder opplæringsprogrammer. • Opplæring som kommer jevnlig + legger til rette for diskusjon/refleksjon fører til økt forståelse og motivasjon. • Tiltakene må skape forståelse og bevissthet rundt de truslene virksomhetene står overfor.	• Forebyggende arbeid må prioriteres ut fra et trusselbasert perspektiv. • Opplæringen må tilpasses ulike deler av virksomheten – kulturelle ulikheter må tas i betraktning. • Kartlegg sikkerhetskulturen for å få et grunnlag for videre opplæringsløp. • Gå for en hybrid læringsmodell med jevnlige moduler.

Tabell 6.1. Oversikt og kobling mellom empiriske funn, teoretiske og praktiske implikasjoner.

6.2 Videre forskning

I denne oppgaven har jeg kun snakket med fagpersonell innen digital sikkerhet, og det var forventet at de hadde god kunnskap og kompetanse innen feltet. Som en videreføring av prosjektet hadde det derfor vært av stor interesse å utvide dette slik at man også hadde intervjuet «vanlige» ansatte og ledere, for på den måten å kunne undersøke hvorvidt påstandene som fremkom i min oppgave samsvarte med resultater man hadde fått fra disse. Jeg har allerede tidligere i oppgaven nevnt at det å måle sikkerhetskultur kan være vanskelig og derfor bør inneholde flere ulike måleparametre, og en slik videreføring ville derfor ivaretatt dette og gitt et enda bedre svar på hvordan den digitale sikkerhetskulturen faktisk er i de ulike virksomhetene, samt hvilke tiltak som fungerer best for å skape bevisste ansatte.

Referanser

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Elsevier, Computers & Security 98* (2020). https://doi.org/10.1016/j.cose.2020.102003

Ansell, C., Boin, A. & Keller, A. (2010). Managing Tranboundary Crisis: Identifying the Building Blocks of an Effective Response System. *Journal of Contingencies and Crisis Management*, Vol. 18, No. 4. DOI: 10.1111/j.1468-5973.2010.00620.x

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

Bada, M., Sasse, A. M. & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society, 2015.* DOI: arXiv:1901.02672

Bang, H. (2011). *Organisasjonskultur*. (4.utg.) Oslo: Universitetsforlaget.

Bergsjø, H., Windvik, R. & Øverlier, L. (red). (2020). *Digital sikkerhet. En innføring.* Oslo: Universitetsforlaget.

Blumer, H. (1954). What is wrong with social theory? *American Sociological Review*, Feb. 1954, Vol. 19, No. 1 (Feb., 1954), pp. 3-10. What is Wrong with Social Theory? (nord.no)

Boin, A. (2019). The Transboundary Crisis: Why we are unprepared and the road ahead. *Journal of Contingencies and Crisis Management*, 2019;27:94–99. DOI: 10.1111/1468-5973.12241.

Bowen, G. (2006). Grounded theory and sensitizing concepts. *International Journal of Qualitative Methods.* 2006, 5(3). Grounded Theory and Sensitizing Concepts - Glenn A. Bowen, 2006 (sagepub.com)

Cone, B. D., Irvine, C. E., Thompson, M. F. & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security 26*, (2007), pp. 63-72. DOI: 10.1016/j.cose.2006.10.005

Departementene. (2019a). *Nasjonal strategi for digital sikkerhet.* Hentet fra nasjonal-strategi-for-digital-sikkerhet.pdf (regjeringen.no)

Departementene. (2019b). *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.* Hentet fra Tiltaksoversikt til nasjonal strategi for digital sikkerhet (regjeringen.no)

Digitaliseringsdirektoratet (2018). *Arbeidet med informasjonssikkerhet i statsforvaltningen*. (Difi-rapport 2018:4). Hentet fra Arbeidet med informasjonssikkerhet i statsforvaltningen | Digdir

Digitaliseringsdirektoratet (Digdir). (2021). *Sikkerhetskultur*. Hentet fra PowerPoint-presentasjon (digdir.no)

Digitaliseringsdirektoratet (u.å.). *Veileder i kompetanse- og kulturutvikling innen digital sikkerhet.* Hentet 30.04.21 fra Veileder i kompetanse- og kulturutvikling innen digital sikkerhet | Digdir

Direktoratet for samfunnssikkerhet og beredskap (DSB) (2012). *Nasjonalt risikobilde 2012.* Hentet fra Nasjonalt risikobilde (NRB) 2012—side 76 (dsbinfo.no)

Direktoratet for samfunnssikkerhet og beredskap (DSB) (2016). *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid? Versjon 1.0.* Hentet fra Samfunnets kritiske funksjoner | Direktoratet for samfunnssikkerhet og beredskap (dsb.no)

Direktoratet for samfunnssikkerhet og beredskap (DSB) (2019). *Analyser av krisescenarioer 2019*. Hentet fra https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

Eid, J., & Johnsen, B.H. (2005) *Operativ psykologi.* Bergen: Fagbokforlaget.

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

Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., & Flores, W. R. (2017). Gamification of Information Security Awareness and Training. *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, pp. 59-70. DOI: 10.5220/000612850059007

Fimreite, A. L., Lango, P. Lægreid, P. & Rykkja, L.H. (2011). *Organisering, samfunnssikkerhet og krisehåndtering*. Oslo: Universitetsforlaget.

Irgens, E. J. (2011). *Dynamiske og lærende organisasjoner. Ledelse og utvikling i et arbeidsliv i endring*. Bergen: Fagbokforlaget.

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. (3.utg.) Oslo: Cappelen Damm.

Jacobsen, D. I., & Thorsvik, J. (2013). *Hvordan organisasjoner fungerer* (4. utg.). Bergen: Fagbokforlaget.

Johannessen, A., Tufte, P.A. & Christoffersen, L. (2016). *Introduksjon til samfunnsvitenskapelig metode*. (5.utg.) Oslo: Abstrakt forlag.

Johannessen, A., Christoffersen, L. & Tufte, P.A. (2011). *Forskningsmetode for økonomisk-administrative fag*. (3.utg.) Oslo: Abstrakt forlag.

Justis- og beredskapsdepartementet. (2017). *IKT-sikkerhet – Et felles ansvar*. (Meld. St. 38 (2016-2017)). Hentet fra https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/?ch=1

Justis- og beredskapsdepartementet (2019). *Nasjonal strategi for digital sikkerhet*. Hentet fra *nasjonal-strategi-for-digital-sikkerhet.pdf (regjeringen.no)

Khan, B., Alghathbar, K. S., Nabi, S. I. & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management, Vol. 5*(26), pp. 10862-10868. DOI: 10.5897/AJBM11.067

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. (2014). Advanced Social Engineering Attacks. *Journal of Information Security and Applications, October 2014*, pp. 1-11. DOI: https://doi.org/10.1016/j.jisa.2014.09.005

Kvalnes, Ø. (2010). *Det feilbarlige menneske. Risiko og læring i arbeidslivet*. Oslo: Universitetsforlaget.

Laumann, K. (2011). Perspektiver på menneskelige og organisatoriske årsaker til feil, ulykker og sikkerhet. I P. Ø. Saksvik (Red.) *Arbeids- og organisasjonspsykologi*. (s. 267-298). Oslo: Cappelen Damm.

Justis- og beredskapsdepartementet. (2017). *Risiko i et trygt samfunn – Samfunnssikkerhet*. (Meld. St. 10 (2016-2017). Hentet fra Meld. St. 10 (2016–2017) - regjeringen.no

Moldjord, C., Arntzen, A., Firing, K., Solberg, O.A., & Laberg, J. C. (2007) *Liv og lære i operative miljøer - «Tøffe menn gråter»*. Bergen: Fagbokforlaget.

Nasjonal Sikkerhetsmyndighet (NSM) (2021). *Risiko 2021 – helhetlig sikring mot sammensatte trusler*. Hentet fra Det digitale risikobildet - Nasjonal sikkerhetsmyndighet (nsm.no)

Nasjonal Sikkerhetsmyndighet (NSM) (2019). *Helhetlig digitalt risikobilde 2019*. Hentet fra https://www.nsm.stat.no/globalassets/rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf

Nätt, T.H. & Heide, C.F. (2015). *Datasikkerhet. Ikke bli svindlerens neste offer.* Oslo: Gyldendal.

Norsk senter for informasjonssikring (NorSIS) (2018). *Nordmenn og digital sikkerhetskultur 2018.* Hentet fra Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf (norsis.no)

Norsk senter for informasjonssikring (NorSIS). (2020). *Nordmenn og digital sikkerhetskultur 2020. Kommentar til årets befolkningsundersøkelse av Bjarte Malmendal*. Hentet fra Nordmenn-og-digital-sikkerhetskultur-2020-web.pdf (norsis.no)

NOU 2015: 13. *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Justis- og beredskapsdepartementet. Hentet fra NOU 2015: 13 - regjeringen.no

Nyeste, P. G. & Mayhorn, C. B. (2010). Training Users to Counteract Phishing. *Proceedings of the Human Factors and Ergonomics Society 54th Annual Meeting*, pp. 1956-1960. DOI: https://doi.org/10.1177/154193121005402311

Politiets Sikkerhetstjeneste (PST) (2020). *Nasjonal trusselvurdering 2021*. Hentet fra Nasjonal trusselvurdering 2021 (pst.no)

Pedersen, K. S. & Gaupseth, M. O. (2019). *Digital sikkerhetskultur i Norge – en studie av dokumenter utgitt av nasjonale aktører*. (Masteroppgave, Universitetet i Stavanger). Hentet fra UiS Brage: Digital sikkerhetskultur i Norge - En studie av dokumenter utarbeidet av nasjonale aktører. (unit.no).

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate

Sikkerhetsloven. (2019). *Lov om nasjonal sikkerhet*. (LOV-2018-06-01-24). Hentet fra Lov om nasjonal sikkerhet (sikkerhetsloven) - Lovdata

Smith, D. T. & Ali, A. I. (2019). You've been hacked: A technique for raising cyber security awareness. *Issues in Information Systems, Vol. 20, Issue 1, 2019*, pp. 186-194. Hentet fra https://iacis.org/iis/2019/1_iis_2019_186-194.pdf

Telenor (u.å.). *Én enkelt e-post kan koste bedriften din millioner – slik kan du stoppe den*. Hentet 04.05.21 fra (Én enkelt e-post kan koste bedriften din millioner - slik kan du stoppe den (telenor.no)

Tjora, A. (2012). *Kvalitative forskningsmetoder i praksis*. (2.utg.) Oslo: Gyldendal Norsk Forlag AS.

Weick, K. E. & Sutcliffe, K. M. (2015). *Managing the unexpected: sustained performance in a complex world* (3rd ed.). Hoboken, New Jersey: Wiley.

Wiley, A., McCormac, A. & Calic, D. (2019). More than the individual: Examining the relationship between culture and Information Security Awareness. *Elsevier, Computers & Security 88*, January 2020. https://doi.org/10.1016/j.cose.2019.101640

Vedlegg

Vedlegg 1 – Informasjonsskriv og samtykkeskjema

Vil du delta i forskningsprosjektet

"Digital beredskap innen samfunnskritiske funksjoner"?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å kunne vise suksessfaktorer knyttet til forebygging og forhindring av kriser som følge av digitale sårbarheter, slik at organisasjoner kan nyttiggjøre seg dette i deres arbeid med kriseledelse opp mot digital beredskap. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Prosjektet er en masteroppgave gjennom studiet Beredskap og kriseledelse ved Nord Universitet. Oppgaven skal leveres mai 2021. Tema for oppgaven er digital beredskap innen samfunnskritiske funksjoner, og jeg vil intervjue informanter i ulike etater innenfor disse kategoriene.

I og med at samfunnet vi lever vi blir stadig mer digitalisert, ser vi også en økende sårbarhet knyttet til digitale trusler og angrep. Vi har i stor grad gjort oss avhengige av avanserte datasystemer både i den daglige driften og til bruk i krisesituasjoner, og mange påpeker at den største utfordringen når det gjelder cybertrusler er den menneskelige faktoren. Det er derfor sannsynlig at mange vil rammes av kriser relatert til cybersikkerheten dersom man ikke øker bevisstheten rundt dette og arbeider aktivt for at organisasjonen som helhet skal bli mer robust mot denne typen hendelser. Jeg ønsker derfor å kartlegge holdninger til og bevissthet rundt temaet digital beredskap innen samfunnskritiske funksjoner da disse har en særskilt viktig rolle i å ivareta sikker drift og service både under kriser og i hverdagen.

I og med at dette er en masteroppgave innen samfunnsvitenskapelige fag, vil det ikke bli drøftet hvilke teknologiske løsninger som vil kunne forhindre digitale angrep. Fokuset vil derimot ligge på organisasjonsforståelse og kriseledelse, og knyttes opp mot bevisstgjøring og sikkerhetskultur innad i organisasjonen. Jeg vil altså ikke gå inn på hvilken teknologi ulike etater benytter seg av, men kartlegge holdninger til og bevissthet rundt temaet digital beredskap. Jeg vil derfor ikke gå inn på sensitive opplysninger som er taushetsbelagt med tanke på sikkerhetsteknologiske løsninger.

Opplysningene som fremkommer vil kun bli brukt i dette prosjektet.

Hvem er ansvarlig for forskningsprosjektet?
Nord Universitet er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Fokuset mitt for oppgaven er som tidligere nevnt digital beredskap innen samfunnskritiske funksjoner, og jeg har derfor valgt ut tre ulike etater innen disse kategoriene for å få et så bredt spekter som mulig innenfor de begrensningene oppgavene setter. Jeg har henvendt meg til ulike etater med forespørsel om deltakelse til prosjektet, og din etat har takket ja til dette. Jeg har videre fått opplysninger fra mine kontaktpersoner i din etat på at du vil være en god informant fordi du jobber opp mot dette feltet og vil kunne bidra med nyttig informasjon.

Hva innebærer det for deg å delta?
Datainnsamlingen vil foregå gjennom personlige intervju. Intervjuene vil bli gjennomført i løpet av høsten, fortrinnsvis september/oktober. Jeg har foreløpig ikke satt noe spesifikt antall på informanter, men det vil trolig ligge på mellom 2-3 personer per etat.

Hvis du velger å delta i prosjektet innebærer det at du stiller opp til et intervju, fortrinnsvis personlig, men med mulighet for å ta det over telefon. Intervjuet vil ta ca. 1 – 1 ½ time. Jeg vil be om følgende personlige opplysninger om deg i intervjuet:

- Navn og stilling
- Antall år du har jobbet i etaten/stillingen

Jeg vil i tillegg ta lydopptak og notater fra intervjuet. Lydopptaket blir primært gjort for å kunne sikre en best mulig gjengivelse av det informanten sier. Det vil derfor bli brukt til transkribering av intervjuene og vil dermed bli lagret elektronisk frem til sensur av prosjektet foreligger.

Det vil bli gitt grundig informasjon om samtykke og behandling av opplysninger i forkant av eventuelle intervju. Opplysningene som fremkommer gjennom intervjuene vil kun bli brukt i dette prosjektet.

Som tidligere nevnt vil jeg i utgangspunktet ikke gå inn på taushetsbelagte opplysninger, men jeg ønsker likevel å understreke at ingen av deltakerne er løst fra sin taushetsplikt.

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

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

Det vil kun være student og veileder som har tilgang til opplysningene.

Transkribering av intervjuene vil bli gjort ved bruk av systemet Nvivo.

I den ferdigstilte oppgaven vil deltakerne anonymiseres og vil ikke kunne gjenkjennes.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er ca. juni 2021. Personopplysninger og eventuelle opptak slettes når prosjektet er godkjent.

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

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

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

På oppdrag fra Nord Universitet har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Nord Universitet, v/ Jan-Oddvar Sørnes (veileder)
- Tone Gunnes (student)

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Jan-Oddvar Sørnes
(Forsker/veileder)

Tone Gunnes
(student)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «Digital beredskap innen samfunnskritiske funksjoner», og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju
- ☐ at det blir tatt lydopptak under intervjuet

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet.

(Signert av prosjektdeltaker, dato)

Vedlegg 2 – Godkjenning fra NSD

NSD sin vurdering

Prosjekttittel
Digital beredskap innen samfunnskritiske funksjoner

Referansenummer
436020

Registrert
09.09.2020 av Tone Gunnes - tone.gunnes@student.nord.no

Behandlingsansvarlig institusjon
Nord Universitet / Handelshøgskolen / Marked, organisasjon og ledelse

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)
Jan-Oddvar Sørnes, jan-oddvar.sornes@nord.no, tlf: 90839821

Type prosjekt
Studentprosjekt, masterstudium

Kontaktinformasjon, student
Tone Gunnes, tone-gunnes@hotmail.com, tlf: 47618343

Prosjektperiode
03.08.2020 - 26.05.2021

Status
11.09.2020 - Vurdert

Vurdering (1)

11.09.2020 - Vurdert
Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 11.09.2020, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du

melder inn en endring, oppfordrer vi deg til å lese om hvilke typer endringer det er nødvendig å melde:
https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html Du må vente på svar fra NSD før endringen gjennomføres.
TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 26.05.2021.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

• lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen

• formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål

• dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet

• lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

NSD vurderer at informasjonen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Tlf. Personverntjenester: 55 58 21 17 (tast 1)

Vedlegg 3 – Intervjuguide

INTERVJUGUIDE

Innledning

- Info om prosjektet – hvorfor deres organisasjon er valgt ut – takk for bidrag!
- Info om innhenting av personopplysninger og lydopptak.
- Samtykkeerklæring
- Forklar gjennomføringen av intervjuet (fri forklaring, tema og spørsmål, avslutning).
- Tidsbruk ca. 1 – 1 ½ time.

Bakgrunnsinformasjon:

- Hvilken stilling har du?
- Hvor lenge har du hatt denne? Tidligere erfaring?

Digital sikkerhet / cybersikkerhet

- **Begrepet**
  - Hva legger du i begrepet digital sikkerhet / cybersikkerhet?
  - Hva betyr det for din arbeidsplass?
  - Hvilket syn har dere på den menneskelige faktoren opp mot dette begrepet?

- **Trusler**
  - Hvilke utfordringer/trusler står dere overfor?
  - Har dere hatt tilfeller av dette? Hvilke typer, hvor mange?

- **Håndtering**
  - Hvordan har dere håndtert denne typen trusler? (både før og etter det skjer)

Stikkord: informasjonssikkerhet, social engineering, løsepengevirus

Organisering og ansvar

- **Beredskapsorganisasjonen**
  - Hvordan er beredskapsorganisasjonen deres bygd opp? (likhetsprinsippet?)

- **Ansvar for digital sikkerhet**
  - Hvordan er dere organisert med tanke på cybersikkerhet vs. tradisjonell sikkerhet?
  - Hvem har ansvaret for cybersikkerheten på din arbeidsplass?
  - Hvem har beslutningsmyndighet ved cyberhendelser/-kriser?

- **Samarbeid**
    - Har dere samarbeid med andre organisasjoner/etater når det kommer til cybersikkerhet? Hvordan?

Stikkord: krisehåndteringsprinsippene, samarbeid/samvirke.

Organisasjons- og sikkerhetskultur

- **Feil og avvik**
    - Hvordan oppdages feil, avvik og uønskede hendelser i deres organisasjon?
    - Hvordan håndteres dette?
    - Hvem følger opp uønskede hendelser og hvordan gjøres dette? (System for rapportering, læring og tilbakemeldinger?)
- **Kollektiv bevissthet**
    - Hvordan sikrer dere at ansatte er bevisst egen og andres rolle innen cybersikkerhet?
    - Hvordan evalueres sikkerhetstiltakene?

Stikkord: sikkerhetsbevissthet, desentralisert beslutningsmyndighet, perspektiv på feil (syndebukk vs systemfeil), lærende organisasjon, åpenhet.

Risiko- og sikkerhetsstyring

- **Beredskapsplaner og instrukser**
    - Har dere beredskapsplaner for cybersikkerhet? Hvorfor / hvorfor ikke? Evnt hvilke?
    - Har dere instrukser som omfatter cybersikkerhet?
    - Hvem har ansvaret for å utarbeide planer og instrukser for dette?
    - Har dere utført såkalte gap-analyser?
- **Tiltak og barrierer**
    - Hvilke ikke-teknologiske tiltak og barrierer har dere mot digitale trusler?
    - Hvordan evalueres tiltakene?
- **Opplæring og øvelser**
    - Gjennomføres det opplæring innen cybersikkerhet på din arbeidsplass? På hvilken måte? (holdningsskapende og bevisstgjøring?)
    - Gjennomføres det øvelser innenfor dette feltet? Hvilke?
    - Hvem har deltatt på denne typen øvelser?

- **Systemutvikling og verdikjeder**
    - Hvem utvikler systemene og teknologien som brukes? Kjenner man disse? (verdikjeder - sårbarhet)
    - Blir denne testet opp mot brukerne av systemene?

Stikkord: kunnskapsarbeid, risikoforståelse, sikkerhetsbevissthet, sikkerhetsatferd, MTO

Avslutning

- Hva fungerer spesielt bra når det kommer til cybersikkerhet i deres organisasjon?
    - Hvorfor?
- Er det noe dere kunne/ville gjort annerledes? Hvorfor?
    - Hvor godt forberedt er dere på digitale trusler og angrep?
- Hva mener du er spesielt viktig for å utvikle og vedlikeholde en god cybersikkerhet i en organisasjon?
- Ut fra det vi har snakket om, er det andre ting du ønsker å føye til / andre synspunkter du vil dele?
- Er det greit om jeg kontakter deg ved en senere anledning dersom jeg har flere spørsmål?