Høgskolen
i Innlandet

Fakultet for økonomi og samfunnsvitenskap

Leiv Andreas Krohn og Stian Singsaas

Masteroppgave

Digital sikkerhetskultur i kraftsektoren

En studie av kjennetegn ved den digitale sikkerhetskulturen i kraftbransjen

Master i offentlig ledelse og styring

2023

Abstract

Our modern society is characterized by a large degree of digitalisation. Digitization is simply about using technology to improve and renew our businesses in society, while ensuring good security. Norwegian businesses experience digital attacks on a daily basis, and there have been several examples of serious data attacks in Norway in recent years. This places new demands on how businesses conduct their security and preparedness work. The digital security work must be in line with the digital risk the businesses are exposed to. National risk assessments point in particular to humans as a favorite target for those who try to penetrate digital systems. As the person will always be the user of the digital solutions, this means that they can also be influenced in different directions to make mistakes or share sensitive information about the business. Our businesses critical to the function of our society, such as the power sector, will always be exposed to greater digital risk since they work with our fundamental services. Based on this, we have chosen to address the human and organizational factors that play a role in the work to create a good digital safety culture in businesses in the power sector. We arrived at the following problem: *What characterizes Norwegian power companies work with digital safety culture, seen from the perspective of professional employees and management?*

We have used literature in the study from traditional theories around man-made and highly reliable organizations and safety culture. Digital security culture is a relatively new term and thus the traditional theories are important to describe the phenomenon. We have also made use of recent national and international research on digital security culture. In addition, we have included public documents which describes how national authorities approach digital security culture. Norwegian power companies are mainly owned by the public sector, and they must comply with national guidelines and are subject to Norwegian laws and regulations.

Our research project was carried out as a descriptive multiple case study, with participation from two different power companies. The data collection was carried out using a qualitative method inspired by Grounded theory and a step-by-step deductive inductive method, and we conducted a total of 11 interviews of specialist employees and managers in two different power companies. Furthermore, we transcribed all the interviews, coded them and categorized them using the analysis program NVivo. After an extensive process of coding, we were left with broad data material that formed the basis for three main categories

of empirical findings: "digital security", "digital security culture" and "barriers". These categories formed the basis for our discussion and conclusion in the study.

The purpose of the research project is to contribute to insight into what characterizes the digital safety culture from the perspective of management and specialist employees in the power sector. Through our analysis and discussion, we have found direct connections between the thesis' empirical findings and existing literature on the subject. Risk understanding, management's influence and preventive work mutually influence each other and play an important role in developing a good digital security culture.

Our conclusion is that in order to create a good digital security culture in the power industry, a good awareness of digital security is required among employees through an understanding of risk and knowledge. The management plays a central role in the organization and in the anchoring of digital security work in the businesses. They themselves should act as good role models to increase trust in the employees. Preventive work through soft barriers must be prioritized in order to change employees' attitudes and knowledge of digital security.

Sammendrag

Vårt moderne samfunn preges av i stor grad av digitalisering. Digitalisering handler enkelt sagt om å bruke teknologi til å forbedre og fornye våre virksomheter i samfunnet, samtidig som man ivaretar god sikkerhet. Norske virksomheter opplever digitale angrep tett på kroppen daglig, og det har vært flere eksempler på alvorlige dataangrep i Norge de siste årene. Dette stiller nye krav til hvordan virksomhetene driver sitt sikkerhets- og beredskaps arbeid. Det digitale sikkerhetsarbeidet må stå i stil til hvilken digital risiko virksomhetene blir utsatt for. Nasjonale risikovurderinger peker spesielt mot mennesket som et yndet mål for dem som prøver å trenge igjennom digitale systemer. Ettersom mennesket alltid vil være brukeren av de digitale løsningene, betyr det at de også kan påvirkes i ulik retning til å gjøre feil eller dele sensitiv informasjon om virksomheten. Våre samfunnskritiske virksomheter, som kraftsektoren, vil alltid være utsatt for større digital risiko siden de arbeider med våre grunnleggende verdier. På bakgrunn av dette har vi valgt å ta for oss de menneskelige og organisatoriske faktorene som spiller inn på arbeidet med å skape en god digital sikkerhetskultur i virksomhetene i kraftsektoren. Vi kom frem til følgende problemstilling: *Hva kjennetegner norske kraftvirksomheter sitt arbeid med digital sikkerhetskultur, sett fra fagansatte og ledelsen sitt perspektiv?*

Litteraturen i studien har vi hentet fra tradisjonelle teorier rundt menneskeskapte og høypålitelige organisasjoner og sikkerhetskultur. Digital sikkerhetskultur er et relativt nytt begrep og dermed er de tradisjonelle teoriene viktige for å beskrive fenomenet. Vi har også benyttet oss av nyere nasjonal og internasjonal forskning på digital sikkerhetskultur. I tillegg har vi trukket inn offentlige dokumenter som beskriver hvordan nasjonale myndigheter tilnærmer seg digital sikkerhetskultur. Norske kraftselskaper er i all hovedsak eid av offentlig sektor, og dermed må de forholde seg til nasjonale føringer på området og er underlagt norske lover og regler.

Forskningsprosjektet vårt ble gjennomført som en deskriptiv flercasestudie, med deltakelse fra to ulike kraftvirksomheter. Datainnsamlingen ble gjennomført ved bruk av kvalitativ metode inspirert av Grounded Theory og stegvis-deduktiv induktiv metode, og vi gjennomførte totalt 11 intervjuer av fagansatte og ledere i to forskjellige kraftvirksomheter. Videre transkriberte vi alle intervjuene, kodet dem og kategoriserte dem med bruk av analyseprogrammet NVivo. Etter en omfattende prosess med koding satt vi igjen med bredt datamaterialet som dannet grunnlaget for tre hovedkategorier av empiriske funn: «digital

sikkerhet», «digital sikkerhetskultur» og «barrierer». Disse kategoriene dannet grunnlaget for vår drøftelse og konklusjon i studien.

Forskningsprosjektet har som formål å bidra til innsikt i hva som kjennetegner den digitale sikkerhetskulturen sett fra ledelse og fagansatte i kraftsektoren. Gjennom vår analyse og drøfting har vi funnet direkte knytninger mellom oppgavens empiriske funn og eksisterende litteratur på området. Risikoforståelse, ledelsens påvirkning og forebyggende arbeid påvirker hverandre gjensidig og spiller en viktig rolle for å utvikle en god digital sikkerhetskultur.

Vår konklusjon er at for å skape en god digital sikkerhetskultur i kraftbransjen kreves det god bevissthet rundt digital sikkerhet hos de ansatte gjennom kunnskap og risikoforståelse. Ledelsen spiller en sentral rolle i organiseringen og forankringen av digitalt sikkerhetsarbeid i virksomhetene. De bør selv gå frem som gode rollemodeller for å øke tilliten til de ansatte. Forebyggende arbeid gjennom myke barrierer må prioriteres for å endre holdninger og kunnskap de ansatte har til digital sikkerhet.

Forord

Denne masteroppgaven markerer avslutningen på vår erfaringsbaserte master i offentlig ledelse og styring ved Høgskolen i Innlandet. Oppgaven tar for seg hva som kjennetegner den digitale sikkerhetskulturen i kraftsektoren. Bakgrunnen for valg av tema var vår interesse for sikkerhetskultur og på bakgrunn av økende digitalisering av samfunnet ønsket vi å lære mer om dette i en digital kontekst. Selve prosessen med å skape oppgaven har for oss vært interessant og lærerikt. Den har gitt oss inngående kunnskaper om digital sikkerhetskultur. Vi håper dette arbeidet kan komme andre til gode.

Vi ønsker å takke vår veileder, Mass Soldal Lund, for god veiledning gjennom konstruktive tilbakemeldinger under hele prosessen. Han har ved sin brede kunnskap på området ledet oss trygt igjennom arbeidet. Vi vil også rette en stor takk til alle som stilte til intervju og bidro gjennom å dele egne erfaringer, refleksjoner og kunnskap om teamet. Alle dere har vært avgjørende for gjennomføringen av studie. Vi vil også takke våre nåværende og tidligere arbeidsgivere som har lagt til rette og gitt oss muligheten til å gjennomføre studiet.

Å skrive en masteroppgave har krevd mye av vår oppmerksomhet i en lengre periode, og det har til tider vært krevende å kombinere studier med to fulltidsjobber og privatliv. Takket være våre fantastiske samboere har vi kommet i mål med oppgaven, Tusen takk for tålmodigheten Linn, Martine og Hugo.

Figur og tabelloversikt

Tabelloversikt

Figuroversikt

Vedleggsoversikt

Begrepsordliste

Samfunnskritisk funksjoner: Funksjoner som samfunnet ikke kan klare seg uten i syv døgn eller kortere uten at det truer befolkningens sikkerhet og/eller trygghet

PST: Politiets sikkerhetstjeneste

DSB: Direktoratet for samfunnssikkerhet og beredskap

NSM: Nasjonale sikkerhetsmyndighet

IKT: Informasjons- og kommunikasjonsteknologi

NVE: Norges vassdrag- og energidirektorat

NSR: Næringslivets sikkerhetsråd

NorSIS: Norsk senter for informasjonssikkerhet

Innhold

1 Innledning

Vi lever i et samfunn der stadig ny teknologi tas i bruk. Norge er et av de fremste landene på å benytte seg av teknologi, og teknologiske løsninger preger hverdagen til alle i samfunnet. De nye digitale tjenester gjør at det skapes avhengigheter på tvers av ansvarsområder, sektorer og nasjoner. Uten de digitale tjenestene står vi nakne og sårbare, og dermed er kravet at disse tjenestene til enhver tid opprettholdes og er tilgjengelige for brukeren. Digitaliseringen av samfunnet har påført digitale sårbarheter, som trusselaktørene kan utnytte seg av for å ramme vår digitale sikkerhet (Departementene, 2019). For at vi som samfunn skal lykkes med digitaliseringen må kravet om sikkerhet til nye teknologiske løsninger ivaretas. Her peker flere sikkerhetsvurderinger fra E-tjenesten (FOKUS), Nasjonal risikovurdering fra PST og NSM (Risiko) mot at sårbarhetene ikke i tilstrekkelig grad blir erkjent og håndtert på en god nok måte (Departementet, 2019). Da Norske Hydro i 2019 ble rammet av et omfattende digitalt angrep lammet det selskapet fullstendig. Angrepet førte til total nedstenging og kostnadene ved angrepet var på 800 mill. kroner (Meld. St. 9 (2022-2023). Denne hendelsen er en påminnelse til alle som driver med digitalt sikkerhetsarbeid om viktigheten av å ha et effektivt og tilstrekkelig forsvar mot digitale trusler.

Allerede i 2003 ble den første nasjonale strategien for digital sikkerhet lansert i Norge. Dette gjorde Norge til et av få land i verden med en slik nasjonal strategi på digital sikkerhet. I takt med utviklingen av trusselbildet i Norge og verden har arbeidet med strategien blitt revidert fire ganger med siste utgave i 2019. Norge fikk sin første stortingsmelding som utelukkende omhandler digital sikkerhet i 2017 med tittelen «IKT- sikkerhet – et felles ansvar» (Meld. St. 38 (2016-2017). Digital sikkerhet gikk altså fra å være et tema for spesielt interesserte, til noe som angår oss alle (Departementet, 2019). Nasjonal sikkerhetsmyndighet (NSM), Etterretningstjenesten og politiets sikkerhetstjeneste (PST) er alle offentlige etater som utgir trussel- og risikovurderinger hvert år i Norge. Alle disse rapportene har et stort fokus på digitale trusler og risikoer.

Ifølge NSM sin trussel og risikovurdering fra 2023 har det de siste årene vært flere alvorlige cyberangrep globalt, og trenden er økende. I Norge har vi fra 2019 til 2021 sett en tredobling i alvorlige cyberoperasjoner mot norske myndigheter og virksomheter. Vedvarende phishing og kartleggingsaktivitet mot norske aktører understreker at disse er attraktive mål, og at denne kartleggingen kan peke mot framtidige cyberangrep som kan ramme oss hardt. NSM

(2023) understreker at det er mennesker som er mest utsatt for slik aktivitet, og de har derfor laget ulike digitale sikkerhetstiltak som virksomhetene bør iverksette for å sikre seg mot uønskede digitale angrep. Dette er tiltak som retter seg mot ledelsen, sikkerhetskultur og oppdatering av tekniske sikkerhetssystemer. I rapporten til NSM (2023) trekkes spesielt arbeid med god sikkerhetskultur frem. Hvilke kunnskaper og holdninger de ansatte har om digital sikkerhet og betydningen av å ha ledere som setter klare mål og tar tydelige beslutninger, trekkes frem som viktige faktorer for et godt digitalt sikkerhetsarbeid. De setter også et spesielt fokus på personellsikkerhet og økt forståelse av sikkerhetsregler og rutiner. På den måten vil det føre til mer årvåkenhet blant de ansatte som igjen kan føre til at sårbarheter fanges opp (NSM, 2023, s. 9-23).

Med vår bakgrunn fra nødetat og andre arbeidsforhold med samfunnssikkerhet som fokus, har vi utviklet en interesse for organisasjonskultur og mer spesifikt sikkerhetskultur. Gjennom våre arbeidsforhold i samfunnskritiske etater har vi gjort noen antakelser om at digital sikkerhet er noe mange opplever som skummelt og at flertallet av ansatte ikke innehar tilstrekkelig kompetanse om hvordan man skal forholde seg til det digitale rom. Basert på interessen for sikkerhetskultur og nysgjerrigheten knyttet til digital sikkerhet ønsker vi å se nærmere på sikkerhetskultur, i digital kontekst.

1.1 Aktualisering

PST og NSM frykter sabotasje innenfor kraftforsyningen i Norge. Frem til invasjonen av Ukraina var Russland den største gassleverandærer til Europa – nå er det Norge. Droneobservasjoner og sabotasje mot Nord Stream- ledningen viser oss viktigheten av å beskytte infrastrukturen knyttet til kraftinstallasjoner, for å opprettholde Norges grunnleggende samfunnsfunksjoner. For å sikre vår evne til å beskytte våre verdier i krise og krig, må vi sikre våre viktigste verdier i fredstid (NSM, 2023, s. 11).

Digitaliseringen fører med seg mange positive effekter for virksomhetene, men den fører også med seg mange sårbarheter (NSM, 2019, s 5). Vi ønsker med denne oppgaven å belyse hvordan tilstanden er når det kommer til digital sikkerhetskultur i kraftsektoren. Vi har valgt oss ut kraftsektoren basert på trussel og risikovurderingene som nasjonale myndigheter vektlegger i sine rapporter. Vi ønsker å se nærmere på hva som kjennetegner arbeidet med digital sikkerhetskultur i kraftsektoren, og hva virksomhetene i sektoren selv opplever av digitale sårbarheter og utfordringer.

I mars 2021 offentliggjorde Riksrevisjonen sin rapport om NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Rapporten pekte på flere sårbarheter, herunder manglende oversikt over IKT- sikkerhetstilstanden til kraftselskapene og at tilsynet til NVE ute hos kraftselskapene var mangelfullt (Riksrevisjonen, 2021). NVE gjennomførte i 2021 en spørreundersøkelse om IKT- sikkerhetstilstanden i kraftforsyningen. Et av funnene var at 60% av de fagansatte på digital sikkerhet mente at virksomheten mangler styringssystemer for informasjonssikkerhet. Dette funnet tyder på en avstand mellom beredskapsledelsen og de fagansatte på digital sikkerhet i hvordan de oppfatter arbeidet med digital sikkerhet i virksomhetene (NVE, 2021).

I mørketallsundersøkelsen til Næringslivets sikkerhetsråd fra 2022 oppgis menneskelige feil og sikkerhetsbevissthet hos de ansatte som årsaken til henholdsvis 37% og 28% av informasjonssikkerhetshendelser. Dette er en nedgang fra 2020, men det er fortsatt urovekkende tall. Hadde det vært gjort tilsvarende funn ved HMS-arbeidet i virksomhetene, hadde det etter Næringslivets sikkerhetsråd sitt syn, blitt utløst omfattende organisatoriske og teknologiske tiltak for å avlaste menneske og tilfeldigheten som feilkilde (NSR, 2022).

Både trusselvurderingene nasjonalt og kjente beredskapsteorier trekker frem mennesket som den største sårbarheten i sikkerhetsarbeidet. Det kreves bevisstgjøring av alle ansatte for at virksomhetene skal kunne forhindre kriser og uønskede cyberhendelser (Bergsjø et al., 2020, s. 40). Trussel og risikorapporten til NSM (2023) sier at myndighetene og virksomhetene bør redusere sine digitale sårbarheter for å gjøre trusselaktørenes jobb vanskeligere. For å imøtegå dagens digitale risikoer kreves det et omforent situasjonsbilde og et effektivt samarbeid. Det stilles større krav til ivaretakelse av sikkerheten nasjonalt, hos virksomhetene og blant enkeltindivider. NSM ser også at ondsinnede cyberoperasjoner mot norske virksomheter har blitt gjort gjennom utnyttelse av menneskelige, organisatoriske og teknologiske sårbarheter. Ved bruk av velutprøvde metoder og varianter av sosial manipulasjon, som blant annet phising eposter, har trusselutøvere forsøkt å ta seg inn i norske virksomheter datasystemer (NSM, 2023, s. 4 og s. 18)

Bergsjø (2020) forteller at mange av studiene som er gjennomført rundt digital sikkerhetskultur har fokusert på enkeltindividets adferd. Ved å utelukkende se på adferd og ikke ta med verdier og holdninger, avdekkes ofte funn som sier noe om hva enkeltindividene gjør eller har gjort, og lite funn rundt hva folk kommer til å gjøre i fremtiden. Dette stemmer dårlig med hva den digitale sikkerhetsbransjen forsøker å få til, som er å forutse hva som vil komme til å skje. Sikkerheten må være forebyggende, altså i forkant (Bergsjø et al., 2020, s.

36). Derfor så Norsk senter for informasjonssikring (NorSIS) i sin rapport The Norwegian Cybersecurity Culture fra 2016 mer på holdninger, verdier og følelser. Det var første gang digital sikkerhetskultur ble beskrevet og kartlagt i Norge, og det ble utarbeidet åtte kjerneområder for å beskrive digital sikkerhetskultur på en helhetlig og relevant måte. Disse åtte punktene er felleskap, styring og kontroll, tillit, risikooppfattelse, optimisme for teknologi og digitalisering, kompetanse, interesse for teknologi og IT, samt adferdsmønstre (NorSIS, 2020, sitert i Bergsjø et al., 2020, s. 36). I denne oppgaven velger vi å benytte oss av NorSIS sin definisjon på digital sikkerhetskultur som er de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til digitale verdier (Bergsjø et al., 2020, s. 36)

Økningen av alvorlige cyberangrep og et økende behov for digitalisering utgjør til sammen en stor digital risiko mot Norge. NSM (2023) er helt tydelige på i sine risikoanalyser at digitale angrep mot samfunnskritiske funksjoner, som kraftsektoren, er det som kan påføre samfunnet vårt størst skade. Vi ønsker med denne oppgaven å belyse hvordan forholdene i kraftsektoren er når det kommer til arbeidet med digital sikkerhetskultur. Som nevnt spiller mennesket en stor rolle i dette sikkerhetsarbeidet, og vi vil derfor ta for oss menneskelig og organisatoriske forhold i kraftvirksomhetene vi undersøker.

1.2 Problemstilling

Med bakgrunn i vår interesse for sikkerhetskultur og antakelser om det finnes utfordringer knyttet til arbeidet med digital sikkerhetskultur i kraftsektoren, utarbeidet vi en problemstilling som kunne være med på å belyse bakenforliggende årsaker til hvorfor arbeidet med digital sikkerhetskultur oppleves ulikt i kraftsektoren, spesielt mellom ledelsen og de fagansatte på digital sikkerhet. Problemstillingen vil forhåpentligvis kunne gi noen svar på hva som fungerer i arbeidet og hva som kan forbedres. På bakgrunn av dette kom vi frem til følgende problemstilling:

Hva kjennetegner norske kraftselskaper sitt arbeid med digital sikkerhetskultur, sett fra fagansattes og ledelsen sitt perspektiv?

For å besvare problemstillingen har vi utarbeidet følgende forskningsspørsmål:

- Hvilken digital risiko opplever kraftselskapene at de står overfor?
- Hvordan påvirker de ansattes holdninger og bevissthet arbeidet med digital sikkerhetskultur?
- Hvordan påvirker ledelsen arbeidet med digital sikkerhetskultur?

- Hvordan ivaretas arbeidet med varsling og læring av digital sikkerhet i virksomheten?
- Hvilke forebyggende arbeid og tiltak gjøres i virksomhetene for å styrke den digitale sikkerhetskulturen?

Vi har ikke funnet lignende forskningsprosjekter som omhandler spesifikt kraftsektoren, men vi er kjent med at det er gjennomført lignende prosjekter knyttet til samfunnskritiske funksjoner. I Norge finnes det undersøkelser gjennomført av private og offentlige aktører som gir noe innsikt i denne spesifikke tematikken. Vi ønsker gjennom to ulike perspektiver, herunder fra fagansatte på digital sikkerhet og fra ansatte som har en ledende rolle når det kommer til digital sikkerhet, å belyse og beskrive kjennetegnene på den digitale sikkerhetskulturen i kraftsektoren på en best mulig måte.

1.3 Operasjonalisering og avgrensning

1.3.1 Samfunnskritisk funksjon

I 2016 definerte Direktoratet for samfunnssikkerhet (DSB) hvilke funksjoner som skal regnes som samfunnskritiske. De la til grunn at dette må være funksjoner som kjennetegnes ved at svikt i disse funksjonene raskt medfører tap og skade. Begrepet forbeholdes videre de funksjoner som samfunnet ikke klarer seg uten i syv døgn eller kortere uten at dette truer befolkningens sikkerhet og/eller trygghet (DSB, 2016, s. 26)

Grunnleggende samfunnsfunksjoner og viktige samfunnsoppgaver er helt avhengig av en pålitelig energiforsyning. Det stilles store krav til forsyningssikkerheten i Norge fordi vi i stor grad benytter oss av elektrisk energi. Elektrisk energi går i hovedsak fra vannkraftanlegg og ut til forbrukerne i Norge. DSB sier i sin rapport om samfunnets kritiske funksjoner (2016) at kraftforsyningen omfatter de systemer og leveranser som er nødvendige for å ivareta samfunnets behov og dermed regnes kraftforsyningen som en samfunnskritisk funksjon (DSB, 2016). Kraftselskapene er dermed underlagt energiloven og blant annet kraftberedskapsforskriften (DSB, 2016, s. 86).

Norges vassdrag- og energidirektorat (NVE) har ansvaret for å forvalte de innenlandske energiressursene og er nasjonal reguleringsmyndighet for elektrisitetsektoren som kraftsektoren er en del av. (DSB, 2016, s. 89). Det blir også henvist til KraftCERT i oppgaven. KraftCERT er et ISAC (Information Sharing and Analysis Center) og et IRT (Incident Respons Team) for sin målgruppe, og jobber for god, sikker og effektiv hendelseshåndtering og informasjonsdeling mellom relevante selskaper nasjonalt og internasjonalt.

I dette forskningsstudiet vil vi se på de ulike miljøene internt i virksomhetene. Dette er operasjonell teknologi (OT) og informasjonsteknologi (IT). Vi vil se på samspillet mellom OT, IT og markedsmiljøene i virksomhetene. Dette for å vise hvordan kraftsektoren fungerer og hvilke prosesser som skaper positive eller negative friksjoner som fremmer eller hemmer utviklingen i den digitale sikkerhetskulturen.

1.3.2 Sikkerhet

Begrepet sikkerhet kan defineres som en tilstand ved nesten totalt fravær av uønskede hendelser, frykt og fare (Norske Standard, sitert i Bergsjø et al., 2020, s. 19). Det kan også omtales som forebyggende tiltak som har til hensikt å redusere sannsynligheten for at noe uønsket skjer eller minimere skaden av en allerede inntruffet uønsket hendelse. Altså evnen en virksomhet har til å unngå skader og tap. Sikkerhet kan også deles inn i flere fasetter. Fysisk sikkerhet, som teknologiske og omgivelser generelt, eller som menneskelige og sosiale sikkerhetsfaktorer. Dette omhandlerom sosial atferd, organisasjonens struktur og virkemåte (Aven et al, 2019, s. 17). Dette viser oss at sikkerhet som begrep kan omtales på ulike nivåer i samfunnet vårt. Videre er sikkerhet noe alle er en del av enten som enkeltindivid, organisasjon eller samfunn. Dermed kan vi si at alle påvirke sikkerheten ved sine handlinger og valg (Aven et al., 2019). På engelsk har man to ord for sikkerhet. Det ene er «security» som henviser til risikoen og usikkerheten tilknyttet tilsiktede uønskede hendelser som kriminalitet eller terror. Det andre ordet er «safety» og henviser til usikkerheten og risikoen tilknyttet ikke tilsiktede hendelser som industriulykker eller naturkatastrofer (Engen et al., 2021, s. 101). I denne studien innbefatter begrepet sikkerhet både tilsiktede hendelser og utilsiktede hendelser.

Samfunnssikkerhet er en videre utvikling av sikkerhetsbegrepet og beskrives som «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). Dette begrepet er ment å dekke et bredt spekter av utfordringer, både det på engelsk som omtales som «safety» og begrepet «security».

En uønsket hendelse kan defineres som en hendelse som har forårsaket eller kunne forårsaket ulike typer skader på verdier som mennesker, materiell eller miljø. Definisjonen sier ikke noe om omfanget av selve hendelsen. Derfor skille vi gjerne de uønskede hendelser inn i ulykker, kriser og katastrofer. Ulykker er en hendelse av mindre omfang som lokale responsstrukturer kan håndtere selv. En krise har et større omfang enn en ulykke og krever en

mer omfattende respons både lokalt og regionalt. Den mest alvorlig uønskede hendelsen kalles katastrofer. En katastrofe innebærer en større ødeleggelse på infrastruktur som krever mobilisering av omfattende nasjonale responskapasiteter og i noen tilfeller internasjonalt (Engen et al., 2021, s. 302).

1.3.3 Digital sikkerhet

Begrepene datasikkerhet, IKT- sikkerhet, informasjonssikkerhet, cybersikkerhet og digital sikkerhet er alle begreper som blir brukt om hverandre når man snakker om digital sikkerhetskultur. Siden mange av begrepene har samme betydning, ser vi det som ryddig og nødvendig å rydde opp i begrepsbruken og hva vi legger i den. Historisk sett var datasikkerhet populært å bruke på 1980-tallet, så dukket cybersikkerhet opp i 2010, mens i 2019 tok norske myndigheter i bruk digital sikkerhet (Jøsang, 2021, s. 13).

En definisjon av digital sikkerhet er gitt i Departementet sin nasjonale strategi for digital sikkerhet: «Digital sikkerhet handler om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjon- og kommunikasjonsteori» (Departementene, 2019, s. 6). Digital sikkerhet blir i denne oppgaven sett på som tiltak som kan forebygge og begrense uønskede hendelser når det gjelder digitale sårbarheter og angrep (Bergsjø et al., 2020, s. 35).

1.4 Oppgavens oppbygging:

Kapittel 1 gir en innføring i og aktualisering av tematikken for studien. Videre har problemstillingen blitt presentert, sammen med forskningsspørsmålene våre. Vi har operasjonalisert begreper og avgrenset oppgaven. I oppgavens kapittel 2 vil vi presentere sentral internasjonal litteratur og teori på området samfunnssikkerhet og beredskap. Teoriene om menneskeskapte ulykker, organisatoriske ulykker og høypålitelige organisasjoner blir trukket frem her. Det vil også bli vist til sentral litteratur som treffer digital sikkerhetskultur i norske forhold. I kapittel 3 presenteres studiens metodiske momenter. Her beskrives våre valg av forskningsdesign, metode for gjennomføring av studien og besvarelse av problemstillingen vår. I kapittel 4 tar vi for oss resultatene av intervjuene. Her presenterer vi våre empiriske funn i 3 hovedkategorier som er «digital sikkerhet», «digital sikkerhetskultur» og «barrierer». I kapittel 5 vil de empiriske hovedfunnene bli analysert og drøftet opp mot vårt teoretiske rammeverk, og vil bli presentert i analysen i to hovedkategorier, herunder «digital sikkerhetskultur» og «barrierer». Til slutt i oppgaven blir konklusjonene presentert i kapittel 6, sammen med refleksjoner rundt videre forskning.

2 Teori

I dette kapitlet vil vi gjøre rede for grunnleggende teori som er relevant for oppgavens problemstilling. Dette vil danne det teoretiske rammeverket i oppgaven. Hensikten med det teoretiske rammeverket er å danne et utgangspunkt for videre drøfting av de empiriske funnene våre i analysedelen av oppgaven. Det vil bli presentert relevant litteratur innen sikkerhet- og beredskapsarbeid, også med tilknytning til nasjonale forhold, samt kjente internasjonale teorier som treffer vårt fagfelt. Dette er teoriene om høypålitelige organisasjoner og menneskeskapte- og organisatoriske ulykker.

2.1 Risiko og digital risiko

Risiko kan uttrykkes på mange ulike måter. Aven og Renn (2010) beskriver risikobegrepet som usikkerheten utover en tallfestet sannsynlig, basert på usikkerheten om og alvorligheten av en uønsket hendelse og resultatet av en aktivitet med hensyn til det mennesker verdsetter (Aven & Renn, 2010, referert i Engen et al., 2021, s. 94). En annen velkjent definisjon omtales i Engen (2021), at risiko er produktet av sannsynlighet og konsekvens. Her legges det også stor vekt på at vårt digitaliserte samfunn skaper store utfordringer knyttet til å beregne risiko. Samfunnsvitenskapelige syn på risiko vektlegger hvordan vi som kollektiv og individer tolker og forstår risiko. Risiko blir dermed noe vi mennesker skaper selv og sammen. Hvordan vi som mennesker oppfatter og håndterer risiko omtaler vi som risikoforståelse. Alle mennesker på alle samfunnsnivåer må forholde seg til risiko. Spørsmålet blir dermed hvordan risikoen blir opplevd og forstått. Og igjen hvordan dette utspiller seg i samspillet mellom enkeltindivider, grupper, organisasjoner og institusjoner. (Engen et al., 2021 , s. 92; Aven et al., 2019, s. 40)

Den tyske sosiologen Ulrich Beck (1992) skriver om dagens risikosamfunn, som kjennetegnes ved samspillet mellom komplisert teknologi, komplekse organisasjoner og individuelle handlinger i omgivelser som stadig er i endring. Dette har ført det internasjonale og nasjonale samfunnet tettere sammen. Det har ført til effektiviseringsfordeler i prosesser og økt tempoet på informasjons- og beslutningsprosesser (Aven et al., 2019, s. 21-22; Engen et al., 2021, s. 128-129). I denne oppgaven knyttes risiko til digitalisering og digital sikkerhet. Derfor vil det i det følgende blir redegjort for digital risiko.

2.1.2 Digital risiko

Det moderne menneske omgir seg i stadig større grad med moderne teknisk utstyr. Det tekniske utstyret har gjort hverdagen vår mye enklere og åpnet for muligheter som bare for få

år siden var utenkelige. Gjennom økt brukt av teknologi har trusselbildet og den digitale risikoen økt i samfunnet. At vi alle er blitt databrukere, uten nødvendig kunnskap om digital risiko, er uheldig. (Daler et al., 2019, s. 172-173). Risikoen vil dermed være knyttet til aktivitetene ved bruk av ny digital teknologi, teknologiske systemer og komplekse digitale løsninger. For å kunne håndtere digital risiko må vi forstå hvordan digitale risikoer oppstår og hvordan de kan identifiseres. Når vi knytter risikoen til digitalisering, er det altså på grunn av all informasjonen som det er mulig å lagre og kople, selve kompleksiteten og egenskapene til digitaliseringsteknologien og de konsekvensene implementeringen og bruk av digitaliseringsteknologier får for menneske, organisasjoner og samfunnet. Teknologier og samfunnet kan ikke sees på som to distinkte sfærer, det må ses på som komponenter i et komplett system, som gjensidig påvirker og konstruerer hverandre. Samspillet mellom menneske og teknologi er blitt så tett koblet sammen at man vanskelig kan tenkte seg det ene uten det andre (Jasanoff (2014) sitert i Engen et al., 2021, s. 247-249).

2.2 Digital sikkerhetskultur – Mennesker, teknologier og organisasjon

Kultur defineres i samfunnsvitenskapen som det felleskapet av ideer, verdier og normer som en gruppe mennesker deler (Bergsjø et al., 2020, s. 34). For å få den fulle forståelse av hva en digital sikkerhetskultur innebærer, må vi se på organisasjonskulturen. Kultur i organisasjoner kan ikke reduseres til kun å handle om observerbar atferd og individuelle opplevelser. Kultur omhandler komplekse systemer av symboler og meninger, bestående av historier, myter, ritualer og andre verdimessige uttrykk som gjennomsyrer sikkerheten i organisasjonen (Turner 1997; Antonsen, 2019, referert i Engen et al., 2021, s.175). Bang (2011) oppsummerer flere ulike definisjoner av organisasjonskultur til en samlet definisjon: «Organisasjonskultur er de sett av felles verdier, normer og virkelighetsoppfatning somutvikler seg i en organisasjon når medlemmene samhandler med hverandre og omgivelsene» (Bang, 2011, s. 23)

Før vi tar for oss den digitale sikkerhetskulturen må vi innom hva sikkerhetskultur er og hva som kjennetegner denne kulturen. Sikkerhetskulturen handler om den kollektive forståelsen av hva som er farlig og hvordan man kan bidra til å redusere farene som truer organisasjonen. I en organisasjon vil det som alltids bli en avveiing mot tidsmessige og økonomiske hensyn ved valg av sikkerhetstiltak som skal iverksettes. I denne prosessen om hvilke beslutninger som tas vil sikkerhetskulturen kunne virke avgjørende for de valgene som tas. Er sikkerhetskulturen god vil organisasjonen mest sannsynlig ikke ta snarveier og heller velge de tiltak som opprettholder sikkerhetsmålene til bedriften. Sikkerhetskulturen handler

om ulike særtrekk som bidrar til fokus på sikkerhet. Disse særtrekkene kan for eksempel være sanksjonsmekanismer, verdier, organisasjonsstruktur og normer for adferd (Aven et al, 2019, s.33-34)

Norsk senter for informasjonssikkerhet (NorSIS) beskrev konseptet digital sikkerhetskultur for første gang i 2016. Mange sentrale aktører innen digital sikkerhet var bidragsytere i denne rapporten som ble laget på oppdrag fra Justis- og beredskapsdepartementet. Digital sikkerhetskultur har tradisjonelt blitt regnet som en del av organisasjonskulturen, altså noe som bedrifter og virksomheter har drevet med. På bakgrunn av dette synet har digital sikkerhetskultur blitt regnet som et verktøy for effektivitet og etterlevelse av regler og krav. Historisk er konseptet relativt nytt, men det handler om å beskytte digitale verdier fra ulike former for trusler som rettes mot innebygde sårbarheter (NorSIS, 2016)

De fleste studier til nå om digital sikkerhetskultur har dreid seg om enkeltindividets adferd. Det betyr å se på hva individet gjør eller har gjort. Dette fokuset er reaktivt og lite forebyggende som sikkert burde være. Nå fokuseres det mindre på adferd og mer på holdninger, verdier og følelser som kan si noe mer om hvordan enkeltindividet vil reagere på en trussel. Digital sikkerhetskultur må ses med et mer kollektivt perspektiv. Derfor må vi se hvordan enkeltindividene sammen med virksomheten som et kollektiv forholder seg til sikkerhet. For å finne ut hva som kjennetegner verdier, holdninger og følelser i digital sikkerhetskultur lagde NorSIS åtte kjerneområder de mener beskriver dette på en relevant og helhetlig måte (Bergsjø et al., 2020, s.36-42).

(1) Fellesskap – Hvordan forholder enkeltindivider seg til felleskapet og i hvilken grad den enkelte ser seg selv som en del av det «digitale fellesskapet»

(2) Styring – Synet på overvåkning er sentralt her. Hvor går grensen for hva fellesskapet skal kunne kontrollere av enkeltindividers digitale oppførsel.

(3) Tillit – Betydningen av digital tillit for å opprettholde demokratiske prosesser.

(4) Risikooppfattelse – Hvordan individet oppfatter risiko gjennom fakta og subjektive faktorer. Studier viser en urealistisk optimisme til risiko.

(5) Optimisme for teknologi og digitalisering – Holdningen din til digitalisering påvirker måten du forholder deg til teknologi på. Trygghet til teknologi er avgjørende og mistillit er direkte ødeleggende for å lykkes med digitaliseringen.

(6) Kompetanse – Implementering av kunnskaper hos de ansatte.

(7) Interesse for teknologi og IT – Interessen vår former våre holdninger, ferdigheter og kunnskaper.

(8) Adferdsmønstre – Råd fra eksperter og myndigheter om sikker adferd på nett.

En god digital sikkerhetskultur som er å tråd med de åtte kjerneområdene til NorSIS vil være med å fange opp de menneskelige, teknologiske og organisatoriske sårbarhetene som ligger i en virksomhet. Kontinuerlige prosesser som øker bevissthet og kunnskap er avgjørende for å skape god digital sikkerhetskultur i virksomheten. Jevnlige påfyll av digital sikkert kunnskaper vil gi gode verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til digitale verdier (NSM, 2021)

2.3 Organisatoriske ulykker og informerende kultur

James Reason (1997) mener i sin teori om organisatoriske ulykker at det foreligger underliggende årsaker til hvorfor organisatoriske ulykker inntreffer. Han syn på årsak til ulykker kalles gjerne for systemperspektiv. Han mener i all hovedsak at menneskelig feil skyldes forhold ved organisasjonen og ikke skyldes individet selv. Han utelukker ikke betydning menneske i seg selv har, men vektlegger forhold ved organisasjonen i mye større grad. Ved å ha et slik syn på årsak til ulykker blir menneskelige feil en konsekvens av organisatoriske forhold. Latente forhold i organisasjonen er noe Reason spesielt trekker frem. Latente forhold dreier seg om forhold ved organisasjonen som kan skape ulykker. Disse forholdene kan for eksempel være ledelsen, uoppdagede feil eller rutiner for å nevne noen (Reason, 1997)

Reason (1997) forklarer at en ideell sikkerhetskultur ikke er avhengig av ledernes personlige egenskaper eller virksomhetens økonomiske interesser. Han er opptatt av at det jobbes hele tiden i virksomheten mot en forbedret sikkerhet, og at det fokuseres på forebygging av organisatoriske ulykker gjennom å forandre forholdene de ansatte jobber under, fremfor å forandre de ansatte (Reason, 1997).

En effektiv sikkerhetskultur er ifølge Reason en informerende sikkerhetskultur. For at en virksomhet skal oppnå dette, må fire komponenter være til stedet og interagere sammen, herunder rapportering, rettferdighet, fleksibilitet og læring. Disse komponentene påvirker hverandre, noe som betyr at dersom det ikke er en rettferdig kultur i virksomheten, vil det kunne påvirke den ansattes vilje til å rapportere (Reason, 1997).

En rapporterende kultur innebærer at man skaper en arena for rapportering, slik at det legges til rette for at data som nesten-ulykker, ulykker og feil kommer inn. På den måten kan virksomheten skaffe seg en oversikt over risikoer, og legge til rette for å forebygge uønskede hendelser gjennom beredskap og tiltak. Dette avhenger av at medarbeiderne i virksomheten bidrar til rapportering av denne type data. Frykt for sanksjoner ved rapportering der man selv har vært involvert i ulykken, at man føler det som lite viktig eller ikke tar seg tid til å gjøre det, samt opplevelse av rapportering som ekstra arbeid eller som fokus på feil, er momenter som hindrer en god rapporterende kultur. Derfor er det viktig at tillit og oppmuntring preger arbeidsmiljøet, og Reason nevner anonym rapportering, raske tilbakemeldinger, enkel rapportering og amnesti for represalier som viktige faktorer for å skape motivasjon, mengde og kvalitet på rapportering (Reason, 1997).

En rettferdig kultur innebærer at det foreligger rettferdighet og tillit i virksomheten, og at avvik og ulykker ikke skal tillegges skyld på involvert personell, og at man skal oppmuntres til å rapportere om ting som er sikkerhetsrelatert. Det skal være klare retningslinjer på hva som forventes av oppførsel, skyld og prosedyrer på håndtering av disiplinære tiltak, men straff for uforskyldte handlinger er ikke hensiktsmessig (Reason, 1997).

En fleksibel kultur handler om hvordan virksomheter klarer å tilpasse seg endringer dersom dette trengs. Reason mener at virksomhetene må anerkjenne og respektere de ansattes kompetanse, og gi dem god opplæring slik at beslutninger i en krisesituasjon kan gå til de som har den beste kompetanse og erfaring på området. Dette kan innebære at man raskt skifter fra en hierarkisk organisasjonsstruktur til en flat struktur for å håndtere en krisesituasjon best mulig.

En lærende kultur handler om at virksomhetenes evne til å lære, slik at sikkerheten kan forbedres. Observering, analysering, planlegging og utføring er viktige elementer som inngår i en lærende kultur, og Reason hevder elementet om utføring ofte er det som er vanskeligst, fordi virksomheter kan velge å nedprioritere dette. I arbeidet med å utvikle en sikkerhetskultur, hvor virksomheten vil ha ansatte med de rette holdningene og atferd, krever det at begge sider forstår at feil er umulig å unngå og er en viktig del av læringsprosessen (Reason, 1997).

For å oppsummere, er en informerende kultur avhengig av at de ansatte rapporterer om feil, ulykker og nesten-ulykker for å lære. Kvaliteten og viljen til å rapportere krever at det

foreligger tillit og oppmuntring, men det skal være klart hva som er akseptabel og uakseptabel atferd, og hvor disiplinære tiltak skal håndteres rettferdig. Virksomheter må ha en fleksibilitet, hvor man anerkjenner spisskompetansen til de ansatte og har vilje til å gjøre endringer i strukturen når dette trengs. Dette krever at man har respekt for de ansattes kompetanse og gir dem nødvendig og god opplæring. Læring skjer i en kollektiv læreprosess, hvor man anerkjenner at det vil bli gjort feil, men at man lærer av feilene som har blir gjort (Reason, 1997).

2.4 Menneskeskapte ulykker

Turner (1978) mener små og ubetydelig beslutninger i en virksomhet er starten på veien til en ulykke. Det betyr at han ser på hverdagslige mønstre i virksomhetene når han skal lete etter årsaken til at en ulykke inntreffer. Ulykker er et resultat av sosiale, tekniske, institusjonelle og administrative faktorer i en kombinasjon (Turner, 1978).

Kulturelle antakelser og normer i virksomhetene er det som er avgjørende i hvordan den kollektive oppmerksomheten og atferden er i møte med risiko. Han mener prosedyrer og prosesser i stor grad preges av hvilken sosial kontekst som eksisterer i virksomheten. Kulturelt akseptert risiko kan være første steg mot en ulykke. «Informasjonsgap» er navnet Turner bruker om dette fenomenet og beskriver fenomenet om at det innebærer ofte elementer av selvsikkerhet, forbigåelse av regler og rutiner, flere ulike kilder til informasjon og en generell arroganse blant de ansatte i virksomheten. Virksomheter som blir oppfattet som sikre og profesjonelle av samfunnet at størst sjanse for å bli utsatt for ulykker (Turner, 1978)

I sin teori legger Turner stor vekt på risikoforståelse fordi risiko er noe subjektivt og alle personer opplever risiko ulikt. Skapes en kultur der den kollektive oppfatningen av risiko er veldig sterk, kan det Turner omtaler som inkubasjonstid inntreffe. Turner forklarer i sin teori at inkubasjonstiden preges av at den kollektive feiloppfattelsen av risikoen virksomheten står ovenfor er så sterk at den overkjører individets risikooppfattelse. Dette fører til at de ansatte i virksomheten håndterer risikoen feil og det fører virksomheten nærmere en ulykke. Derfor mener Turner at sikkerhetskulturen og risikoforståelsen er viktig for virksomhetene sin evne til å forebygge seg bort fra ulykker (Turner, 1978).

For å skape en god sikkerhetskultur trekker Turner frem ledelsen sin rolle i dette arbeidet. Han mener ledelsen må legge til rette for strukturerte prosesser som ivaretar informasjonsdeling på en god og sikker måte ved behandling av informasjon. Turner setter også et sterkt søkelys på hvordan kommunikasjonen i virksomheten foregår. Kjennetegnes

kommunikasjonen av for eksempel ignorering av eksisterende informasjon og for store mengder informasjon til feil person, kan dette i seg selv føre til ulykker. Mennesker vil som regel gå for løsninger som er «godt nok» mener Turner, og derfor trekken han frem menneskets begrensende kapasitet til å håndtere komplekse problemer som en årsak til ulykker (Turner, 1978).

2.5 Høypålitelige organisasjoner

Teorien om High-Reliability Organizations (HRO), på norsk høypålitelige organisasjoner, skiller seg ut fra de andre beredskapsteoriene. Der de andre teoriene i stor grad ser på årsaken til at en ulykke inntreffer, tar HRO teorien utgangspunkt i at enkelte virksomheter har en unik evne til å unngå ulykker og har så gode forebyggende tiltak at virksomhetene ikke blir utsatt for ulykker. Den ble utviklet på 1980- tallet av forskere fra Berkeley, og har senere blitt omtalt og utviklet av flere anerkjente forskere, som for eksempel Weick og Sutcliffe (2015). Teorien kjennetegnes ved at den har ett positivt syn på styring og kontroll. Dette innebærer at virksomhetene gjennom sitt unike organisasjonsdesign selv kan forebygge seg bort fra ulykker og hindre at menneskelige feil får oppstå og føre til ulykker (Aven et al., 2019, s. 59).

Hovedfokuset til HRO teorien er prosessen «mindful organizing». Denne prosessen kjennetegnes ved at virksomhetene er tilpasningsdyktige og svært sensitive for hint og tegn på farer. Prosessen har som hensikt å forhindre at små feil utvikler seg og spres videre i organisasjonen og på den måten skaper større sammensatte ulykker. Gjennom å skape et system for persepsjon, erfaringer og forventinger er hensikten til teorien å skape en meningsdannende prosess. Det betyr at prosessen oppfatter farer og reagerer med riktig mottiltak og delvis klarer å forutsi hvilke farer som lurer rundt neste sving. Denne prosessen har til hensikt å skape en helhetlig tilnærming til sikkerhet og skape en motstandsdyktig organisasjon (Weick & Sutcliffe, 2015, s.21-22, s.32). For å oppnå høy pålitelighet i virksomheten fremheves fem overordnede kognitive prinsipper (Weick & Sutcliffe, 2015, s. 7-14).

(1) Opptatthet av mindre feil – Prinsippet tar for seg de ansatte sin overvåkenhet rundt symptomer og indikasjoner på feil som kan spre seg videre. Det handler om å identifisere feilene og håndtere dem fortløpende for å unngå utvikling til større uønskede hendelser.

(2) Motvilje til å overforenkle årsaker – De ansatte må inneha en motvilje til å akseptere forenklede forklaringer på komplekse kontekster og hendelser. Denne motviljen vil bidra med å se detaljene i feilene som oppstår og lukke feilen raskere.
(3) Sensitivitet for operasjoner – Prinsippet fokuserer på den operasjonelle delen av organisasjonen. Punktet har til hensikt å øke bevisstheten til risiko og årvåkenheten til de ansatte rundt det som faktisk skjer foran dem operasjonelt. Slik kan de ansatte håndtere avvik tidlig og på riktig måte.
(4) Forpliktelse til motstandsdyktighet – Ingen er immune mot feil, ingen organisasjoner er uten feil og mangler. Derfor må organisasjoner lære av sine feil, utfordre sine oppfatninger og opprettholde sin sensitivitet mot arbeidet som gjøres daglig. Evnen en organisasjon har til å opprettholde eller gjenoppta en dynamisk og stabil situasjon etter en uønsket hendelse eller stort press kan defineres som motstandsdyktigheten til organisasjonen.
(5) Anerkjennelse av kompetanse – For å kunne håndtere usikkerhet i ulike miljøer og tilpasse seg komplekse settinger, ønsker HRO-ene er bredt utvalg av kompetanse og eksperter i sin organisasjon. For å kunne utnytte denne kompetanse på best mulig måte burde beslutningsmyndigheten senkes ned fra toppledelsen, siden de ikke nødvendigvis innehar riktig kompetanse og erfaring. Gjennom denne desentraliseringen av beslutninger vil dette prinsippet bli opprettholdt og feil effektivt bli løst på riktig nivå.

2.6 Oppsummering av teori

Vårt forskningsprosjekt baserer seg i hovedsak på sentrale og kjente teorier innen beredskap og samfunnssikkerhet. Teoriene er menneskeskapte ulykker, høypålitelige organisasjoner og informerende kultur. Menneskeskapte ulykker setter søkelyset på å finne årsaken bak en ulykke som har inntruffet, mens den høypålitelige teorien setter søkelyset på å forebygge ulykker gjennom organisering og konstant meningsdannende kognitive prosesser i virksomhetene. Den informerende kulturen handler også i stor grad om å forebygge seg bort fra ulykker gjennom å ha en god rapporterende, rettferdig, fleksibel og lærende kultur. For å skape et bredere teorigrunnlag har vi også valgt å ta med litteratur som omhandler risiko og digital risiko. Siden oppgaven handler om menneskelige og organisatoriske forhold har vi plukket ut teori som kultur, sikkerhetskultur, menneskelige, teknologiske og organisatoriske forhold.

Kjerneelement	Risiko, digital risiko og risikoforståelse	Digital Sikkerhetskultur-MTO	Menneskeskapte kulturer	Informerende kultur	Høypålitelige organisasjoner	Organisatoriske ulykker
Risikoforståelse	Risiko konstrueres av mennesket og er dermed subjektivt.	Hvordan mennesker forholder seg til digitale verdier og deres sikkerhetsadferd	Alle oppfatter risiko ulikt. Risikoforståelse avgjørende ved god sikkerhetskultur	Den kollektive evnen organisasjonen har til å forstå risiko. Kulturen påvirker risikoforståelsen til den ansatte	Motvilje til å akseptere forenklede forklaringer på komplekse hendelser	Delt bekymring for farer og deres innvirkning. Forståelse for hva som kan bryte gjennom i dybden.
Kunnskap og kompetanse	Kunnskap om trusler, sårbarheter og verdier påvirker vår risikoforståelse.	Kunnskap om datasikkerhet er avgjørende for total sikkerhet.	Manglende kunnskap og kompetanse kan føre til ulykker.	Informasjonsgap kan føre til ulykker. Store mengder digital informasjon er utfordrende.	Anerkjennelse av intern og ekstern kompetanse.	Kunnskap kan bidra til å
Ledelse	Avgjørende for å se den totale risikoen og ta gode velbegrunnede beslutninger	Viktig for god risikostyring og sikkerhetskultur	Toppledelsen må sette gode strukturer og prosesser for behandling av informasjon	Legger til rette for en rapporterende kultur gjennom.	Forpliktelse til sikkerhetsarbeidet og anerkjennelse av kompetanse. Overføre beslutningsmyndigh et til riktig nivå i organisasjonen.	Unngå latente forhold i organisasjonen. Ledelsen må prioritere sikkerhet og allokere ressurser.
Rapportering og varsling		Fokus på felleskap-tørre å si ifra om egne feil-opplevelse av tillit.	Rapporterings kultur. Tillit til at personvern ivaretas og gode tilbakmedlinger	Tillit og oppmuntring	Opptatt av feil. Tidlig identifisering og håndtering av små feil.	Rapporteringskultur - tillit
Forebygging	Viktig for å kunne spå fremtiden. Må ha kunnskap om tall og mennesker.	Tekniske tiltak ikke tilstrekkelig. Vektlegger sikkerhetskulturen i virksomhet.	Fokus på latente forhold.	Forebygge gjennom å ha en lærende kultur der feil kommer frem i lyset.	Mindful organizing og sensemaking. Bruk av persepsjon og erfaring til å unngå uønskede hendelser.	Unngå latente forhold i organisasjonen som kan skape ulykker
Øving og læring	Kompleks samspill mellom teknologi og menneske	Jobbe opp mot mennesket, organisasjon og teknologi.	Læringskultur	Kontinuerlig refleksjon og organisatorisk læring	Utfordre sine oppfatninger og lære av feil.	Organisatorisk læring/kontinuerlig refleksjon
Bevissthet	Viktig for å ha en hensiktsmessig forhold til risiko.	Bevissthet rundt at verdier kobles til nett.	Menneskelige feil er et resultat av organisatoriske forhold.	Stor tillit de at riktig kompetanse kommer sammen i kriser.	Meningsskapende prosess. Kollektiv bevissthet.	Realistiske og fleksible normer og regler for farer

Tabell 2.1 Oversikt over hovedpunkter fra det teoretiske rammeverket

3 Metodiske momenter

For at vi mennesker skal fungere i hverdagen trenger vi forutsigbarhet. Dette lager vi ut ifra egne erfaringer og opplevelser som danner teorier og oppfatninger om hvordan virkeligheten er (Johannessen et al., 2020, s. 19-20). Vitenskapelig metode er ikke helt forskjellig fra dette, men forskjellen er at man følger en fremgangsmåte (Oppen et al., 2020, s. 23). Det handler om systematikk, grundighet og åpenhet, for å se om våre oppfatninger og teorier om virkeligheten stemmer med virkeligheten eller ikke (Johannesen et al., 2020, s. 21)

Samfunnsvitenskapelig metode er en kontrollert undersøkelse for å finne, beskrive, forstå, forklare, evaluere og forandre mønstre og regelmessigheter i den sosiale virkeligheten (Blaike, 2010, s. 36). Metoden gir oss altså en fremgangsmåte på hvordan man skal gå frem for å samle, analysere og tolke informasjonen, slik at informasjonen sier noe om den sosiale virkeligheten på en korrekt måte.

En forskning begynner som oftest med søken etter kunnskap om en virkelighet, og man utformer en problemstilling. Problemstillingen skal vise til hva forskningen ønsker å gi svar på, altså formålet, og den legger grunnlag for teorivalg, forskningsdesign og metode (Johannessen et al., 2020 s. 23). Vår problemstilling er følgende: *Hva kjennetegner norske kraftselskaper sitt arbeid med digital sikkerhetskultur, sett fra fagansatte og ledelsen sitt perspektiv?*

For å kunne besvare problemstillingen vår, har vi utarbeidet flere forskningsspørsmål som vi mener vil bidra til å svare på problemstillingen i sin helhet. Disse forskningsspørsmålene går på opplevelse av digital risiko, ledelsens påvirkning, holdninger hos ansatte og ledelsen, forebyggende tiltak, samt tiltak for tilsyn og læring. Det er mange måter å gå frem på, og vi vil i det følgende vise hvordan vi har tenkt i forhold til design og metode, innsamling av data, og analyse. Vi vil også vise til betraktninger rundt kvaliteten på forskningen, herunder validitet, pålitelighet og generalisering, samt refleksjon over vår egen rolle som forskere, kritisk refleksjon over forskningsdesign og metode, samt etiske betraktninger rundt det å drive et forskningsprosjekt.

3.1 Forskningsdesign og metode

I den første fasen, skal man lage et forskningsdesign som viser hvordan man har tenkt å besvare problemstillingen. Man må finne ut av hvem og hva undersøkelsen skal sette søkelys på, og hvor og hvordan undersøkelsen skal utføres (Oppen et al., 2020, s. 32).

Vi ville å få en dypere forståelse av hvordan den digitale sikkerhetskulturen i kraftbransjen er. Digital sikkerhetskultur ble derfor et konkret fenomen som vi ville beskrive, og vi ønsket å innhente detaljert informasjon omkring dette fenomenet, gjennom opplevelsen til de fagansatte og ledelsen som jobber eller som har en sentral rolle når det kommer til digital sikkerhetskultur i kraftvirksomheten sin.

En case blir sett på som et studieobjekt, og ett studieobjekt kan være en aktør, for eksempel en enkeltperson eller en gruppe mennesker (Johannessen et al., 2020, s. 211). Vi vil argumentere for at vårt studie er et deskriptivt flercasestudie, gjennom at ledelsen og de fagansatte er hver sin case, da de kan bli sett på som to ulike grupper. Det er videre normalt at casestudier brukes innen organisasjonsforskning, som de to kraftvirksomhetene vi undersøker klart må regnes som. Vi underbygger videre at vi har et flercasestudie gjennom at vi har hentet inn mye informasjon gjennom dybdeintervjuer som må regnes som detaljert og omfattende datainnsamling over en viss tidsperiode, og at vi åpner for en sammenlikning av casene gjennom å fremheve de to ulike casenes sine perspektiver på digital sikkerhetskultur (Johannessen et al., 2020, s. 212).

Det har ikke vært gjort så mye spesifikk forskning på akkurat denne tematikken i kraftbransjen, men vi vet at det er gjort noe. Derfor vil vi påstå at forskningen også er til dels eksplorerende (Blaike, 2010, s. 70). Den informasjonen som ble innhentet av oss ble gjennomført i perioden 15 januar til 20 februar 2023. Det ble derfor gjort på et bestemt tidspunkt, og det ga ett øyeblikksbilde som viste hvordan fenomenet opplevdes her og nå, noe som gjorde det til en tverrundersøkelse (Johannessen et al., 2020, s. 259-260).

Man skiller gjerne mellom kvalitativ og kvantitativ metode i samfunnsvitenskapen. Den kvantitative metoden er som regel mer lineær og hvor man bruker metoder som spørreundersøkelser og statistiske analyser for å få en forståelse av bredde og spørsmål som hvor mange og hvor ofte. Dette muliggjør at man kan studere store populasjoner, og hvor forskeren gjennom statistiske generaliseringer kan si noe om den kunnskapen han besitter er representativ for virkeligheten. Den kvalitative metoden handler på sin side mer om spørsmål som hvordan og hvorfor, og hvor man gjennom bruk av datainnsamlingsmetoder forsøker å få en dybdeforståelse av personers erfaringer og opplevelser for å forstå og forklare sosiale fenomener. Det handler mer om å forstå enn å forklare, og bruken av tekst fremfor tall (Oppen et al., 2020, s. 31-33; Tjora, 2012, s. 18). Vi har valgt en kvalitativ tilnærming, da vi ønsket å få en dypere forståelse av fenomenet vi studerte gjennom å hente inn detaljert og utfyllende informasjon fra et færre antall informanter.

Når man har bestemt seg for kvalitativ metode, finnes det flere metoder å arbeide videre etter. En metode er deduksjon, hvor man tar utgangspunkt i en etablert teori, og tester denne ut i praksis, for å forklare fenomenet. Motsetningen til denne tilnærmingen er induksjo*n*, hvor man går fra empiri til teori, og hvor man ut ifra funnene finner teorier og forklaringer. Når man har elementer fra begge tilnærmingene, kalles det *abduksjon*. Da kan man for eksempel starte fra ett induktiv perspektiv, men samtidig ha en teoretisk forforståelse (Oppen et al., 2020, s. 29 og 378).

Glaser og Strauss utviklet på 1960-tallet noe som heter *Grounded Theory*, som er en induktiv tilnærming hvor man i stedet for teoriverifisering, var mer opptatt av teorigenerering gjennom å la datagrunnlaget utvikle nye teoretiske ideer (Nilssen, 2012, s. 79). De mente at teorigenerering og teoriverifisering er begge en del av samme prosess og foregår på en fleksibel måte (Blaike, 2010, s. 141). Koding er en sentral prosess i Grounded Theory, hvor man gir koder på innsamlet data som ser ut til å være av mulig teoretisk betydning, eller som ser ut til å være spesielt fremtredende i den sosiale verden til de som studeres (Bryman, 2016, s. 573). Derfor kan den metoden være et godt alternativ å jobbe etter, når man studerer noe man ikke har mye kunnskap om fra før, og man ønsker å forstå og kartlegge fenomenet.

En lignende metode, er noe som heter stegvis-deduktiv induktiv metode. Idealet til denne metoden er å gjøre det man kan med den empirien man har frembrakt, og ikke være avhengig av å hente inn mer data dersom man har behov for dette. Man jobber i en trinnvis modell, hvor det foregår en induktiv prosess der man etappevis jobber fra rådata til konsepter og teorier, samtidig som det foregår en deduktiv prosess, der man ofte sjekker fra det teoretiske til det empiriske. Kritikken Grounded Theory har fått er at den baserer seg på utvikling av teori gjennom en systematisk sirkulær vandring mellom datagenerering og konseptutvikling. Dette kan ofte oppleves som vanskelig i praksis som følge av tidsbruk. I stegvis-deduktiv induktiv-modellen kan man alltid gå tilbake i stegene. Har man ikke nok empiri til å lage tilstrekkelige kategorier, kan man gå tilbake til det første steget, og begynne på nytt. Den skal tilrettelegge for systematikk og fremdrift i ett kvalitativ forskningsprosjekt. (Tjora, 2012, s. 26 og 174 – 176).

Fenomenet vi studerer hadde vi ikke mye kjennskap til fra før, og som det heller ikke finnes så mye spesifikk og etablert teori på. Derfor valgte vi å ha en abduktiv tilnærming, og bruke Grounded Theory som utgangspunkt for fremgangsmåten vår i å beskrive, forstå og forklare fenomenet. Det å innhente mer empiri underveis i prosessen ville vært vanskelig som følge av tidsplan, og vi var avhengig av å bruke den innsamlede empirien vi fikk. Derfor

valgte vi å benytte oss av stegvis-induktiv deduktiv metode, slik at vi kunne operere i de ulike trinnene samtidig og utforske teori og empiri om hverandre.

Teori skal ikke være det som leder forskningsprosjektet i kvalitativ forskning. På den andre side, så har de fleste som gjør et forskningsprosjekt med seg en forforståelse, som kan ha en innflytelse på hvilke fenomen som man interesser seg for, og hvordan man forsker seg frem (Tjora, 2012, s. 29-30). Man har en teori som omgir studien, kjent som ett teoretisk rammeverk, og dette har en innvirkning på hva vi stiller av spørsmål, hvordan vi utformer intervjuguiden, hvilke teori vi ser på, og hvilke tolkninger vi gjør. Det teoretiske rammeverket fungerer som linsen man ser verden gjennom, og sammen med våre egne verdier, holdninger, kunnskap og forskningsfilosofi, gjør det at vi som forskere kan ha en ulik tilnærming på innsamlet data og teoribruk. (Nilssen, 2012, s 62-68).

Årsaken til at vi valgte å skrive om digital sikkerhetskultur i kraftbransjen, er som følge av en generell interesse for sikkerhetskultur, samt antakelser om at det finnes utfordringer knyttet til arbeidet med digital sikkerhetskultur i kraftbransjen. Disse antakelsene hadde vi fått gjennom å lese offentlige dokumenter, rapporter og artikler som var tilgjengelig, og som sammen skapte vår forforståelse som vi tok med inn i forskningsprosjektet. Vi hadde ingen kjennskap eller erfaringer til den digitale sikkerhetskulturen i kraftbransjen fra før, og vi ønsket å skrive om dette da vi så at det var dagsaktuelt, samt at vi ønsket å tilegne oss nye kunnskaper gjennom å kunne forske på temaet.

3.2 Datainnsamling og utvalg

Med en kvalitativ metode er målsetningen vår å kunne forklare sosiale fenomener gjennom en nær kontakt med de vi studerer, og på den måte oppnå en forståelse av fenomenet. Når det kommer til datainnsamling, er det viktig at man tenker gjennom hva som er best egnet til å belyse problemstillingen (Oppen et al., 2020, s. 342-343). Hvem og hvor mange skal delta i forskningsprosjektet, hvordan skal man rekruttere informanter og utvalgsstrategi, er vurderinger man må gjøre i forhold til dette (Johannesen et al., 2020, s 24).

Vi fant ut at det var intervju vi ønsket å bruke som metode for datainnhenting. Årsaken til dette er fordi vi tenkte at det kunne gi oss den beste forutsetning for å skaffe til veie best mulig informasjon for å forklare fenomenet. Dette krevde at vi måtte formulere en aktuell problemstilling, slik at det kunne bli tydeligere for oss hvem vi ønsket å ha som deltakere og om hva vi skulle prate om. Vi leste oss opp på det vi kunne finne av offentlige dokumenter, rapporter og artikler som omhandlet digital sikkerhet i kraftbransjen eller i andre

samfunnskritiske sektorer. Vi snakket også med kolleger og bekjente som hadde en mening om temaet, og som kunne være med på å gi oss andre perspektiver. På denne måten fikk vi avgrenset og konkretisert vår problemstilling til noe som var forskbart og aktuelt, og som ga oss en pekepinn på hvem vi ønsket å intervjue.

Vi tenkte først å ha flere forskjellige norske kraftvirksomheter i forskjellige størrelser som målgruppe, slik at vi kunne belyse fenomenet bredt. Etter en samtale med veileder og bekjente som har drevet forskningsprosjekter tidligere, forsto vi at dette kom til å bli vanskelig med tanke på rekruttering av informanter innen den tidsrammen vi hadde. Vi landet på at vi skulle intervjue fagansatte og ledere i en liten norsk kraftvirksomhet og det samme i en større norsk kraftvirksomhet. Slik kunne vi fange opp meninger og få informasjon om den digitale sikkerhetskulturen fra fagansatte og ledere som jobber i samme sektor og i virksomheter som varierer i størrelse hva gjelder antall ansatte.

3.2.1 Utvalgsstrategi og utvalgskriterier

Når det kommer til rekruttering av informanter til forskingsprosjektet er det viktig å finne personer som sitter på god informasjon om temaet man studerer. Det er viktig at man finner informanter som kan prate reflektert om temaet man forsker på, noe man kaller for strategisk utvelgelse (Tjora, 2012, s. 145). Samtidig bør antallet informanter ikke være så stort at det ikke er mulig å gjennomføre gode analyser, da forskerens intensjon i kvalitative metoder skal være å forklare, beskrive og tolke et fenomen, fremfor å generalisere fra utvalget til en populasjon (Johannessen, et al., 2020, s 74).

Vi kom frem til at for å belyse vårt fenomen ønsket vi å ha en utvalgsstrategi som baserte seg på et utvalg med to ulike perspektiver. Det ene perspektivet, videre omtalt som ledere, skulle være ansatte i kraftbransjen som hadde en ledende posisjon, mens det andre perspektivet skulle være ansatte i kraftbransjen som var fagansatte, videre omtalt som fagansatte. Årsaken til dette var fordi vi fant det hensiktsmessig å få perspektiver fra begge sider for å beskrive fenomenet på best mulig måte.

I valg av informanter foretok vi en kriteriebasert utvelgelse som handler om å velge informanter ut ifra spesielle kriterier (Johannesen et al., 2020, s. 64). I ledelsesperspektivet, ønsket vi ansatte som hadde en ledende rolle i virksomheten, og som hadde en sentral, eller aktiv rolle i arbeidet med digital sikkerhet. I fagansatte perspektivet, ville vi ha fagansatte som hadde en sentral rolle i arbeidet med digital sikkerhet i virksomheten. Årsaken til dette var at vi ønsket å ha personer med reflekterte meninger rundt temaet. Vi kunne snakket med andre

ansatte i kraftvirksomheten som ikke hadde noe med dette å gjøre i sitt arbeid, men vi landet på at det ikke var hensiktsmessig i forhold til hva vi kunne forvente å få av god informasjon til å belyse fenomenet vårt.

I forhold til valg av virksomhet gjorde vi undersøkelser på ulike kraftvirksomheter som finnes i Norge. Det ga oss en oversikt over store og små virksomheter. Kriteriene vi hadde for valg av virksomhet var at det skulle være en forskjell i størrelse, hva gjelder antall ansatte, på de virksomhetene vi skulle velge. Vi fant frem til to virksomheter som passet til våre kriterier, og som vi tok kontakt med gjennom epost, hvor vi gjennom et informasjonsskriv, beskrev forskningsprosjektet og hvilke informanter fra virksomheten vi ønsket å ha som deltakere. På den måten hadde vi ikke kontroll på hvem som ville ta kontakt med oss, men ettersom vi hadde lagt ved beskrivelse og kriterier for hvem vi ville komme i kontakt med, regnet vi med at virksomhetene ville sette oss i kontakt med de riktige informanter. Vi fikk raskt svar fra virksomhetene, og vi opplevde at de var positive til å delta i forskningsprosjektet, da de mente at temaet var dagsaktuelt og spennende. Vi ble introdusert til en person i hver virksomhet, og gjennom vedkommende ble vi tipset og introdusert til flere aktuelle informanter som vi endte opp med å bruke i vårt forskningsprosjekt. Dette er også kjent som snøballmetoden, som handler om at man spør informanten om anbefalinger om andre personer fra samme miljø som man bør kontakte for intervju (Oppen et al., 2020, s. 348).

Vi opplevde at det var stor interesse for tematikken, og at nesten samtlige informanter ønsket å delta i prosjektet. En mulig utfordring ved verving av informanter, og som man som forskere bør reflektere over, er dette med informantens hensikt med å delta. Dersom en informant har uærlige hensikter, for eksempel deltar for å vinne en premie, kan det svekke studien (Tjora, 2012, s. 153-154). Vår opplevelse av informantene etter å ha pratet med dem før, under og etter intervjuet, var at de fant tematikken interessant, dagsaktuell og viktig for kraftvirksomheten. Samtlige viste entusiasme for at vi ville skrive om dette og vi opplevde at informantene ga oss god informasjon om temaet under intervjuene.

Med tanke på antall informanter skal man intervjue så mange som trengs for å finne ut av det man trenger å vite (Kvale og Brinkmann, 2010, sitert i Oppen et al., 2020, s. 349). Det er altså snakk om et metningspunkt, hvor man etter hvert mottar den samme informasjonen fra informantene. Som nevnt over skal det også gjøres analyser, noe som gjør at antallet ikke bør overskride det man har av tid tilgjengelig (Johannessen et al., 2020, s. 74). Det var vanskelig fra starten å finne ut av hvor mange informanter vi ønsket, men vi var klare på at vi ønsket omtrent like mange informanter fra hvert av perspektivene. Vi endte med fem leder-

informanter og seks fagansatt-informanter, og vi syntes dette antallet var tilstrekkelig i forhold til tiden vi hadde til rådighet og med hensyn til det videre arbeidet med å transkribere og analysere. Hvis vi skulle gjort noe annerledes, kunne det vært aktuelt å legge til enda et utvalg bestående av ansatte i virksomheten som ikke jobber direkte med eller som ikke har en sentral rolle når det kommer til digital sikkerhet i virksomheten. På den måten kunne vi fått belyst den digitale sikkerhetskulturen fra deres perspektiv, og da spesielt i forhold til hvordan de opplever de forebyggende tiltakene.

3.2.2 Intervju

Intervju er den mest fremtredende formen for datainnsamling i kvalitativ forskning og gjør seg godt når man søker dyptgående og gode beskrivelser av en informants totale opplevelse av et fenomen, og for å få frem kompleksiteter og nyanser. (Johannessen et al., 2020, s. 105-106). Et godt gjennomført intervju vil gi rike beskrivelser av hvordan informanten opplever, reflekterer og fortolker sin situasjon, og det kan gi en stor mengde empiri raskt (Oppen et al., 2020, s 344). Vi valgte å bruke intervju som metode for datainnhenting, da vi fant dette mest hensiktsmessig for å innhente best mulig informasjon om fenomenet vi studerte.

Intervjuer har forskjellige strukturingsgrader. Ustrukturerte intervjuer minner mer om en hverdagssamtale, hvor intervjuene har en uformell form for å skape trygghet og rom for at informanten kan snakke om det han er opptatt av, og hvor intervjueren tilpasser seg og spør spørsmål etter hva som kommer frem. Motsatt av dette er strukturerte intervjuer hvor spørsmål er forhåndsformulert og stilles i rekkefølge med det formål å skape en likhet og gjøre det enkelt å organisere. Mellom disse så finnes det semistrukturerte intervjuer (Oppen et al., 2020, s. 350).

Vi gjennomførte semistrukturerte intervjuer, hvor vi på forhånd lagde en intervjuguide med definerte temaer vi ønsket at informanten skulle belyse. En intervjuguide vil hjelpe å holde struktur i samtalen (Oppen et al., 2020, s. 351). Temaene i intervjuguiden er basert på vår problemstilling og forskningsspørsmål, og intervjuguiden ble rammeverket vårt i intervjuene. Fleksibiliteten vi hadde, gjorde at temaer og spørsmål ble stilt etter hvordan intervjuet med informanten utfoldet seg. Dette gjorde at informanten enklere kunne snakke fritt, samtidig som vi var innom alle temaene vi hadde planlagt, bare at vi lot dette skje i en naturlig veksling under intervjuet. Temaer som informanten var opptatt kunne komme først, og vi fikk anledning til å følge opp med spørsmål rundt det som informanten fant viktig. Vi

begynte også hvert intervju med et åpent spørsmål som gikk direkte på problemstillingen vår. Dette gjorde at vi fikk ett upåvirket svar fra informanten, og hvor informanten selv kunne fortelle oss hva han syntes var viktig. Dette gjorde at vi kom inn på temaer som vi ikke hadde tenkt ut på forhånd, og som var viktig for informanten. Slike digresjoner fra informanten er tillatt, og kan vise seg å være relevant for forskingsprosjektet (Tjora, 2012, s. 105).

Før vi begynte med intervjuene gjennomførte vi noen øvelser med intervjuguiden på to bekjente som hadde kunnskap om digital sikkerhet. Årsaken til dette var at vi ønsket å se om det fungerte i praksis, og om den opplevdes som relevant. I tillegg ønsket vi å øve på intervjusituasjonen, og se hvilken teknikk som egnet seg best for å få svar på det vi lurte på (Johannessen et al., 2020, s. 114). Intervjuguiden og måten vi gjennomførte intervjuet på fikk positiv tilbakemelding fra våre bekjente, og vi følte vi behersket intervjusituasjonen godt. Vi foretok noen endringer på formuleringen av enkelte spørsmål under enkelte temaer, samt endret rekkefølgen på et av temaene.

Kvaliteten på intervjuet avhenger av hvilken tillit som er opparbeidet mellom forskeren og informanten (Tjora, 2012, s. 107). Hva man får av informasjon kan påvirkes av blant annet legitimering av forskningsprosjektet, rammen rundt intervjuet og informantens oppfattelse av intervjueren (Johannessen et al, 2020, s. 115-116). I forkant av intervjuene var vi opptatt av å gi informantene rikelig med informasjon om forskningsprosjektet for å skape en legitimering av forskningsprosjektet, og de fikk tilsendt informasjonsskriv med informasjon om formål, rettigheter og personvern. Ved intervjuets begynnelse, begynte vi alltid med å fortelle om forskingsprosjektet og bakgrunnen vår, samt la til rette for spørsmål de hadde om prosjektet, om de hadde forstått rettighetene sine og deres deltakelse inn i dette. Rammene rundt intervjuet avklarte vi på forhånd, herunder lengde, tidspunkt og hvor det skulle bli gjennomført. Intervjuets plassering bør være der hvor informanten føler seg trygg, gjerne på arbeidsplassen hvis det er temaet for oppgaven (Tjora, 2012, s. 120). Vi lot informanten bestemme tid og sted. Vi ønsket helst å ha fysiske intervjuer hvor vi satt ansikt til ansikt, og gjerne på deres arbeidsplass for å få dem til å føle seg tryggere. Ansikt til ansikt intervjuer kan gi en bedre dynamikk mellom partene som følge av økt tillit ved observering av hverandres kroppsspråk (Oppen et al., 2020, s. 345). Vi fikk gjennomført omtrent halvparten av intervjuene ansikt til ansikt, mens resterende gikk digitalt over møteplattformen Microsoft Teams. Hovedårsaken til dette var geografisk avstand, og en større fleksibilitet rundt tidspunktet for intervjuet. Flere av informantene ønsket også selv denne løsningen, og var trygge og godt vante med digitale løsninger for møter. Det at vi så og hørte hverandre

gjennom et kamera, gjorde at vi også fikk sett hverandres kroppsspråk og vi opplevde at dette var en vellykket løsning. En av svakhetene er at man kan bruke lang tid, dersom det tekniske ikke fungerer (Oppen et al., 2020, s. 347). Vi sørget for at det tekniske var i orden før intervjuet og hadde gjort klart back-up løsninger dersom noe skulle skje. Alle intervjuer ble det tatt lydopptak av slik at vi frigjorde egen kapasitet til å kunne fokusere på intervjusettingen. Informantene ble opplyst om bruken av lyd i forkant av intervjuet, hvordan dette skulle bli behandlet og hvor det skulle lagres. Dette for å sørge for at lydopptaket ikke skulle være til hinder for hva informanten valgte å snakke om.

Intervjuet baserer seg i grove trekk på tre faser med ulike typer av spørsmål. (Tjora, 2012, s. 112-114). I oppvarmingsfasen, stilte vi spørsmål som gikk på informantens bakgrunn, arbeidsplass og stilling. Dette for å skape en trygg og myk start hos informanten gjennom uformelle og ufarlige spørsmål, samtidig som vi skaffet oss noen bakgrunnsvariabler. I refleksjonsfasen, introduserte vi informanten for temaer vi ønsket å få belyst gjennom refleksjonsspørsmål eller åpne spørsmål som inviterte informanten til å kunne gå i dybden på aktuelle temaer. I denne fasen opplevde vi en forskjell mellom informantene. Noen kunne ved det første refleksjonsspørsmålet snakke seg gjennom alle temaer vi hadde planlagt i intervjuguiden og på den måte dekket mye av det vi hadde tenkt å stille spørsmål om. Andre kunne gi kortere svar, og var mer avhengig av ytterligere åpne spørsmål eller spørsmål som var mer strukturerte og konkrete, for å snakke videre. Det at vi hadde laget en intervjuguide med åpne spørsmål og underspørsmål viste seg å være veldig til hjelp i slike settinger hvor det stoppet litt opp for informanten, samtidig som vi hadde god nytte av å ha gjort ett par tester på bekjente. Bruk av oppsummering og stillhet var også effektive intervjuteknikker vi benyttet, både for å sørge for at vi hadde forstått riktig, og for å la informanten få muligheten til å utdype seg ytterligere. I avrundingsfasen, var vi opptatt av om informanten hadde noen andre relevante temaer han ønsket å belyse eller om det var noe han savnet og ville ta opp. Vi snakket også om videre gang i forskningsprosjektet, når vi tenkte at det skulle være ferdig og hvordan de kunne få sett det. I tillegg til at vi takket samtlige informanter for deres bidrag, og la til rette for at vi kunne ta kontakt med dem hvis det dukket opp ytterligere spørsmål eller presiseringer av det som hadde blitt sagt i intervjuet.

Vi lærte mye av å gjennomføre intervjuer. Det at vi gjorde en god jobb i planleggingsprosessen med å få tak i gode informanter, lage avtaler, besvare spørsmål som dukket opp, og ikke minst ha en god intervjuguide med oss i intervjuet, var essensielt for at vi klarte å komme i mål med dette. Vi har selv erfaring fra intervjuprosesser gjennom arbeidet vi

til daglig driver med, noe som kom til godt nytte i intervjusamtalen. Likevel, er dette et tema som vi ikke hadde så mye kunnskap om når vi begynte og vi var spent på om informantene fant spørsmålene som relevante. Vi opplevde en god samtaleflyt med informantene, og merket at vi lyktes i å skape en trygg arena for samtale. Dette gjorde at vi opplevde å få gode refleksjoner og perspektiver på tematikken. Etter hvert som vi fikk gjennomført noen intervjuer opplevde vi også en større mestring og trygghet i rollen vår som intervjuer, og vi la merke til at intervjuene ble bedre som følge av dette.

Av refleksjoner rundt hva vi kunne gjort bedre i intervjuene kan vi nevne at vi under transkribering av enkelte intervjuer oppdaget at vi kunne ha fulgt opp noen av svarene som vi fikk med ytterligere spørsmål. Vi løste dette med å ta kontakt med dem på nytt for å avklare det vi lurte på. I tillegg, var vi to stykker som bedrev intervjuene sammen. I de første intervjuene pratet vi som intervjuere litt om hverandre. Dette kan ha blitt opplevd som litt forvirrende for enkelte informanter, og vi endret på dette til at det ble en som intervjuet, mens den andre var bisitter.

3.3 Databehandling

Pseudonym	**Perspektiv**
Petter	Fagansatt
Nils	Fagansatt
Amanda	Fagansatt
Bjørn	Fagansatt
Ivar	Fagansatt
Torgeir	Fagansatt
Arne	Leder
Stian	Leder
Josefine	Leder
Simen	Leder
Espen	Leder

Tabell 3.1 Pseudonym og perspektiv på informantene i utvalget

Hvis personer som er med i forskningsprosjektet kan identifiseres, enten direkte eller indirekte, er dette å anse som personopplysninger, og derfor må vi som forskere være godt kjent med reglene for bruk av dette. Ved bruk av personopplysninger må vi ha en god og

lovlig grunn, ha en tillatelse, ta hensyn til de det gjelder og sørge for en sikker behandling av personopplysningene (Johannessen, et al., 2020, s. 47-48).

Informantene vi brukte i forskningsprosjektet kunne gjennom sine stillinger og arbeidsplass ha blitt identifisert enten direkte eller indirekte, og vi håndterte derfor personopplysninger. Som et forskningsprosjekt ved ett masterstudie i regi av Høgskolen i Innlandet hadde vi en god grunn til å sette i gang med forskningsprosjektet. For å gjøre det lovlig og få tillatelse til å behandle personopplysninger i forhold til personopplysningsloven, søkte vi til Norsk senter for forskningsdata (NSD). Prosjektet ble godkjent den 03.01.2023. Når det gjelder å ta hensyn til informantene sørget vi for at informasjonen som de ga ikke kunne spores tilbake til dem i forskningsprosjektet. Anonymitet var noe vi hadde lovet informantene fra start, og som også er i tråd med taushetsplikten i forvaltningsloven (Johannessen, et al., 2020, s. 50). Informantene fikk hvert sitt et eget pseudonym. Deres arbeidsstilling ble ikke tatt med, men de ble presentert som fagansatt eller leder, alt etter som hvilken rolle de hadde i virksomheten. Navnet på virksomheten de jobbet ved ble ikke tatt med i forskningsprosjektet, og der hvor informantene nevnte virksomheten under intervjuet, ble dette tatt bort fra sitatene vi brukte. Dette gjaldt også annen informasjon som ble sagt av informanten som kunne være identifiserende.

Sammen med informasjonsskrivet benyttet vi oss av et informert samtykke i forkant av intervjuene (Oppen et al., 2020, s. 397). Informantene måtte på forhånd samtykke til å delta på forskningsprosjektet, etter å ha lest om formålet og behandling av personopplysninger. De ble også her opplyst at de når som helst kunne trekke sitt samtykke tilbake uten konsekvenser og begrunnelse. Dette tok vi opp igjen i starten av hvert intervju for å sørge for at alle informantene forsto hva de hadde samtykket til.

3.4 Dataanalyse

En kvalitativ analyseprosess har som hensikt å gjøre våre funn til noe som er meningsfullt og håndterbart (Oppen et al., 2020, s. 378). Dette gjøres gjennom å analysere og tolke datamaterialet, noe som bør gjøres av samme forskere som har innhentet den kvalitative dataen som følge av forforståelser, teorier og hypoteser som forskerne har med seg (Johannessen et al., 2020, s. 155). Analyse og tolkning er noe som går hånd i hånd, men det er noen forskjeller mellom dem. Med analyse så handler det om å finne funn i datamaterialet gjennom at vi som forskere lager oss kategorier, temaer, perspektiver og ser etter mønstre ut ifra det informantene har sagt i intervju. Når dette er gjort, må forskerne fortelle leseren hva

dette betyr i en større mening, og går da over i en tolkningsprosess. Her tolker forskerne funnene opp imot teori for å forklare og ramme dem inn for å gjøre dem forståelige, og vise hvorfor de er viktige (Nilssen, 2012, s. 104-105 og s. 65). Dette er en fase som krever at vi som forskere jobber systematisk (Tjora, 2012, s. 174).

3.4.1 Transkribering

Når man transkriberer gjør man en transformasjon fra muntlig til skriftlig språk, og som et første steg i analyseprosessen handler det om å få skrevet ut empirien ordentlig (Oppen, et al., 2020, s. 378). Når man gjør et intervju om til en tekst kan man miste den ikke-verbale kommunikasjonen som kan ha noe å si for hvordan informasjon kom frem, eksempelvis om informanten svarte usikkert. Dette kalles også visuelle ledetråder (Tjora, 2012, s. 145). For å forsøke å minimere dette er det viktig at vi som forskere foretar transkriberingen selv for å kunne sette oss tilbake til intervjusituasjonen. Det kan være smart å ha et høyt detaljnivå på det som blir sagt og notere ned pauser og uttrykk, slik at man kan se om informanten uttrykker seg usikkert eller må tenke seg om (Tjora, 2012, s. 144; Nilssen, 2012, s. 49).

Vi gjennomførte elleve intervjuer på lyd, og dette måtte gjøres om til tekst som vi kunne bruke videre i forskningsprosjektet. Dette var en tidkrevende oppgave som resulterte i mye tekstmateriale, men som gjorde oss godt kjente med datamaterialet vi hadde innhentet. Vi var veldig opptatt av å få transkribert ferdig hvert enkelt intervju, før vi gikk i gang med neste. Dette fordi det gjorde det enklere for oss å ha atmosfæren i intervjuet til stedet når vi transkriberte. Det at vi transkriberte selv gjorde at vi kunne få ny tanker, spørsmål og ideer underveis, noe som passet bra med vår stegvis-deduktive induktive metode. Vi supplerte også transkriberingen med å føre forskerlogg over interessante perspektiver vi gjorde oss underveis. Når vi var ferdig, satt vi igjen med analysedata som var klare for koding.

3.4.2 Koding og kategorisering

I en kodeprosess handler det om å systematisere den dataen vi har hentet inn, og gi den en mening (Oppen et al., 2020, s. 379). Når man sitter med en større mengde ferdig transkribert intervjumaterialet vil det å se sammenhenger mellom disse være utfordrende. Koding og kategorisering skal hjelpe til med dette. Koder er ord eller uttrykk som beskriver et avsnitt eller et lite utsnitt av datamaterialet, hvor man forsøker å lage tekstnære koder som utvikles ut ifra dataen man har, og ikke ut ifra teori, hypoteser og forskningsspørsmål. Kategorisering handler om å samle koder man har laget i grupper som man finner aktuelle for

sin problemstilling, og slik danne hovedtemaer for videre bruk i analysen. Dette er slik den stegvis-deduktive induktive modellen legger opp til (Tjora, 2012, s. 179 og s. 185).

Måten vi lagde koder på var at vi tok utgangspunkt i et intervju om gangen. I det første intervjuet fant vi koder gjennom begrepsbruk i teksten eller hvordan vi oppfattet det som ble sagt. Kodene noterte vi ned, og vi tok med oss disse kodene inn i neste intervju. Dersom det dukket opp nye koder i dette intervjuet, ble disse lagt til i listen over koder. Dette gjorde vi med alle intervjuene, og vi endte opp en kodeliste på mange forskjellige koder. Vi begynte så arbeidet med kategorisering, hvor vi plasserte kodene i grupper som vi mente var aktuelle for problemstillingen og forskningsspørsmålene våre. Flere koder ble tatt bort som følge av dette. Vi fikk da benyttet et sett med kategorier systematisk og konsekvent på hele datamaterialet (Johannessen, et al., 2020, s. 159).

Vi benyttet oss av Nvivo som analyseverktøy hele denne prosessen. Dette var ett effektivt dataprogram for å systematisere koder og lage kategorier. Ingen av oss hadde tidligere erfaring med dette programmet, men vi hadde fått en grundig opplæring av Høgskolen i Innlandet før vi tok det i bruk.

Vi opplevde denne delen av prosessen som en stor og utfordrende jobb for oss, og det tok tid å finne frem til riktige koder og kategorier som vi ville bruke videre. Vi begge satt med en god følelse etter vi var ferdig med denne delen. Det at vi var to stykker gjorde at vi måtte være godt omforent med de kodene vi skulle bruke, og vi fant ut at den beste måten var at vi kodet intervjuene sammen og diskuterte oss frem til de kodene vi skulle bruke.

Dette arbeidet resulterte i 4 hovedkategorier med 13 underkategorier i første linje. Vi valgte bort den ene hovedkategorien, som følge av at denne inneholdt teknologiske løsninger som dette studiet ikke fokuserer på.

3.4.3 Litteratursøk og teori:

Som tidligere nevnt bruker forskere teorier og litteraturer for å tolke funnene og gi dem mening. Det er gjennom tolkning at forskeren forteller leserne hva som disse funnene handler om (Nilsen, 2012, s. 65).

Når vi begynte med prosjektet gjorde vi en god innledende jobb med å finne ut av hva vi ønsket å forske på, og hvordan vi ønsket å formulere problemstillingen. Vi visste at vi ville skrive om digital sikkerhetskultur, men var noe usikker på hvordan vi skulle formulere problemstillingen, og vi foretok derfor gode søk i eksisterende litteraturer, offentlige

dokumenter, og teorier som omhandlet dette feltet. Gjennom dette masterstudie, samt tidligere fag på Politihøgskolen hadde vi kjennskap til teorier som vi tenkte kunne være relevante i forhold til det vi forsket på. På den andre side, og i tråd med den stegvise-deduktive induktive modellen, ble det foretatt søk etter teori og litteratur underveis i prosjektet. Basert på de funnene vi gjorde viste noe av den teorien vi hadde med fra start å ikke være like aktuelt å bruke i forskningsprosjektet. Teoriene som vi oppdaget og som vi valgte å ta med, fremsto som mer relevant og aktuelt for å besvare problemstillingen vår.

I søken etter teorier og litteratur, benyttet vi oss av Deichmans bibliotek i Oslo og biblioteket i Asker, hvor vi pratet med bibliotekarer som bisto oss med søk. Vi snakket også med informantene våre om de hadde aktuell teori å anbefale, samt brukte søkemotor på internett som Google Scholar. Vi endte opp med relevant litteratur innen sikkerhet- og beredskapsarbeid, også med tilknytning til nasjonale forhold, samt kjente internasjonale teorier som treffer vårt fagfelt

3.5 Forskningsprosjektets kvalitet

For at andre skal kunne stole på forskningen vi har gjort er det viktig at vi som forskere reflekterer over kvaliteten på forskningsprosjektet vårt. Dette er en viktig del av en kvalitativ undersøkelse, og det er tre aspekter som gjør seg gjeldende, herunder pålitelighet, gyldighet og overførbarhet (Oppen et al., 2020, s. 390).

3.5.1 Pålitelighet

Idealet for en forsker i et forskningsprosjekt er å være nøytral og objektiv, men det å være helt nøytral, kan være utfordrende. Valg av tema for oppgaven, og våres egne forforståelser og kunnskaper rundt det tema man forsker på, vil være med oss i forskningsprosessen. Dette er følgelig en ressurs for oss, men det er særs viktig at vi reflekterer over hvordan vår egen posisjon som forskere kan ha noe å si for hvordan vi forsker oss frem (Tjora, 2012, s. 203). Det at vi mennesker kan søke å bekrefte vår egen forforståelse gjennom å lete etter funn som passer inn med hva vi tror på, kan være med på å forhindre at vi for eksempel ikke ser andre funn som er like viktig. På den måten kan påliteligheten på forskningsprosjektet svekkes, og det er derfor av stor viktighet at vi som forskere er bevisste dette og er åpen for å justere våres forforståelser underveis (Nilsen, 2012, s 139) For å sikre en sterk pålitelighet i forskningsprosjektet, er det viktig at man gir en åpen og detaljert beskrivelse av hvordan man har gått frem i forskningsprosjektet (Johannesen et al., 2020, s. 250).

I vårt forskningsprosjekt har vi gitt en detaljert beskrivelse av vår fremgangsmåte, herunder redegjørelser for hvilke valg som er tatt, hvilke metoder som er brukt, hvordan vi jobbet med datainnsamling og hvordan vi har arbeidet med dataen gjennom koding og kategorisering. Vi har sett på vårt eget ståsted som forskere med tanke på tidligere kunnskap og forforståelse, og vært åpne om våre tanker, vurderinger og beslutninger underveis i prosessen.

3.5.2 Validitet

Når man snakker om validitet handler dette om forskerens funn og fremgangsmåte faktisk klarer å svare på det som er forskningsspørsmålet og formålet, og om de i størst grad representerer den virkeligheten som undersøkes (Johannessen et al., 2020, s. 250). Dette omtaltes som indre validitet, og målet er å fortelle at det som kommer frem i forskningsprosjektet ikke er feilaktig ut ifra de faktiske forhold, eller gi rom for misforståelser. Ettersom ett kvalitativt studie ikke kan gjennomføres på nøyaktig samme måte, er det viktig at forskeren beviser at funnene er konsistente og gir mening ut ifra det som er samlet inn av datamaterialet. (Nilsen, 2012, s. 141). Dette kan gjøres gjennom å dokumentere forskningsprosessen, slik at den kan gjennomgås og godkjennes, og på den måte øke troverdigheten og gyldigheten (Tjora, 2012, s. 207).

Det finnes ulike teknikker man kan ta i bruk for å styrke muligheten til å få troverdige resultater i forskningsprosjektet (Johannessen et al, 2020, s. 251). Vi benyttet oss av metodetriangulering, hvor vi valgte å intervjue informanter som kom fra ulike avdelinger og var i ulike stillinger i to forskjellige virksomheter. Dette gjorde at vi ikke så tematikken fra kun en vinkel, men fra flere, noe som styrker troverdigheten. Samtidig hadde vi lest oss opp på feltet, og på den måte var vi mer i stand til å skille relevant og ikke relevant informasjon fra hverandre, enn hvis vi ikke hadde gjort det, såkalt vedvarende observasjon. Hvis vi hadde hatt rikelig med tid ville det vært hensiktsmessig å tilbakeført resultatene til informantene, slik at disse kunne blitt bekreftet, med det lot seg ikke gjøre i dette forskningsprosjektet grunnet tidsrammen.

3.5.3 Generalisering

I kvantitativ forskning snakker man om å gjøre statistiske generaliseringer av funn fra et utvalg til en populasjon, mens i kvalitative studier, hvor man går mer i dybden fremfor bredden og ser på det kontekstuelt unike gjennom datainnsamling fra få individer med visse felles egenskaper, snakker man om overførbarhet (Johannesen et al., 2020, s. 252).

Overførbarheten handler om forskeren klarer å etablere beskrivelser, begreper, fortolkninger og forklaringer som er av relevans for andre områder enn det som studeres, og at det kan overføres til liknende fenomener (Oppen et al., 2020, s.391). Hvis man har gode beskrivelser av detaljer som inngår i et fenomen, vil det være med på å styrke overførbarheten, og det vil gjøre det enklere for lesere å selv vurdere om det som kommer frem er overførbart til andre settinger (Johannessen et al., 2020, s. 252). I tillegg til dette, kan tidligere forskning og teorier støtte opp for å skape en større generalisering (Tjora, 2012, s. 215).

Vi hadde ett utvalg på 5 ledere og 6 fagansatte i to forskjellige virksomheter i kraftbransjen, og med dette kan generaliserbarheten således diskuteres. Samtidig vil vi argumentere for at studien vil kunne være overførbar til andre kraftvirksomheter med bakgrunn i at vi valgte ut to sentrale virksomheter i kraftsektoren og at vi gikk bredt ut i vårt utvalg av informanter som har kjennskap til den digitale sikkerhetskulturen. I tillegg benyttet vi oss av nyere forskning og teorier på området. Vårt håp er at studien vil kunne bidra til økt kunnskap, innsikt og forståelse for problemstillingen for kraftvirksomheter arbeid med digital sikkerhetskultur.

3.5.4 Feilkilder

Det er viktig som forskere å være klar over potensielle feilkilder man kan møte når man bedriver et forskningsprosjekt. Ett sted hvor dette kan bli synlig, er når man driver med datainnhenting gjennom direkte kontakt med informanter, noe vi gjorde som følge av at vi hadde valgt intervju som hovedkilde for datainnsamling. Gjennom erfaringer fra arbeid hvor intervju har vært en sentral del av jobben, var vi klare over fallgruvene vi kunne gå i, og intervjuguiden vi utarbeidet tok høyde for dette. Intervjueffekten handler om at når vi som forskere stiller spørsmål, så må vi forsikre oss om at variasjonen i de svarene vi får ikke skyldes måten vi stiller på spørsmålene på (Oppen et al., 2020, s. 120). Hvis vi som forskere er forutinntatte, kan måten vi påvirker og formulerer spørsmålene på gjøre at informanten i verste fall kan svare det vi ønsker at han skal svare. Vi sørget for å unngå ledende spørsmål i intervjuene, og tilstrebet å stille åpne spørsmål hvor informantene kunne snakke fritt. Samtidig sørget vi for å rydde opp i eventuelle misforståelser, samt fortalte at dersom informanten var usikker eller ikke hadde svar på spørsmålene som ble stilt, skulle han/henne opplyse om dette.

3.6 Kritisk refleksjon over forskningsdesign og metode

Til tross for at vi er fornøyde med de valgene vi har tatt i forskningsprosessen, hva

gjelder metode og fremgangsmåte, vil det alltid være rom for å stille spørsmål til fremgangsmåten vi har valgt, i forhold til potensielle svakheter og andre fremgangsmåter som kunne vært bedre.

Vi kunne ha valgt å inkludere kvantitativ metode som ett tillegg til den kvalitative metoden i studie vårt. Dette kunne gitt oss et mye større datagrunnlag, hvor vi gjennom ett spørreskjema kunne ha nådd ut til flere informanter og kanskje fra flere kraftvirksomheter, slik at vi kunne ha skapt en større overførbarhet eller generalisering av vårt studie. På den andre side, så ville ett spørreskjema ikke ha gitt oss like stor mulighet til å gå i dybden på informantenes opplevelse av fenomenet, noe som vi har gjort med en kvalitativ tilnærming. Det hadde absolutt vært interessant å utforme ett spørreskjema og brukt dette som ett tillegg til dybdeintervjuer, men det hadde vært særs tidskrevende.

Det med begrensninger i tid, gjorde også at vi valgte en tverrsnittsundersøkelse hvor funnene vi gjorde sa noe om fenomenet på det tidspunktet vi innhentet dataen. Vi kunne ha valgt å foretatt en longitudinell undersøkelse som hadde gått over en lengre periode og hvor man kunne se hvordan fenomenet endrer seg over tid (Tjora, 2012, s. 225). Likevel, opplevde vi at informantene fortalte om hvordan reisen hadde vært når det gjelder den digitale sikkerhetskultur i kraftvirksomhetene.

Vi opplevde at vi fikk et godt informantutvalg bestående av ledere og fagansatte som alle hadde god kunnskap og erfaring med digital sikkerhetskultur ved sine respektive virksomheter, og som gjorde at vi ikke opplevde å få mangelfulle svar på spørsmålene våre. Vi hadde ingen tidligere kunnskap eller erfaring med hvordan en informantrekruttering skulle foregå, og derfor gjorde vi en god jobb med kontaktetablering gjennom epost med utfyllende informasjonsskriv, slik at vi økte sannsynligheten for at vi fikk de ønskede informantene. Ettersom vi søkte om informanter som hadde en sentral rolle når det kom til digital sikkerhetsarbeid, enten som fagansatt eller leder, og på den måten ikke etterspurte konkrete stillinger, kjønn, og alder, økte nok dette sjansen for interesserte deltakere, men skapte likevel et slags følelse av manglende kontroll over hvem vi kom til å få som informanter, og til hvilken tid. Noe vi kan spekulere i, er om det fantes andre ansatte i virksomheten vi heller skulle ha pratet med, eller som skulle ha vært en del av vårt informantutvalg. Virksomhetene var forskjellig i størrelse og i antall ansatte, og vi vet ikke om det fantes andre som satt på mer kunnskap enn de som vi fikk som informanter.

I tillegg til intervju, eller som alene, kunne vi ha brukt observasjon som metode for datainnhenting. Da kunne vi ha observert hvordan den digitale sikkerhetskulturen i virksomheten er. Man kunne studert handlinger og relasjoner i sine naturlige omgivelser, og fått en bedre forståelse av forholdet mellom materialitet, teknologi og mennesker (Oppen et al., 2020, s. 357). Dette hadde igjen vært tidkrevende, da vi måtte ha gjort dette over en lengre periode, samt vært til stedet når ulike opplæringer og andre forebyggende tiltak gjøres. Vi anså at intervju var en bedre metode for datainnhenting ved at vi kunne få informantene til å fortelle om deres opplevelse av fenomenet.

I forhold til intervjuguiden vår, så var denne semistrukturert med definerte temaer og spørsmål som var åpne, og etter hvert som vi kom oss lengre ned i temaet, mer spesifikke. Vi ønsket å være fleksible, slik at temaer og spørsmål ble stilt etter hvordan intervjuet med informanten utfoldet seg, men at vi også hadde en struktur å følge. Dersom vi hadde valgt en mer strukturert intervjuguide med definerte spørsmål som stilles i rekkefølge, kunne det kanskje vært mer hensiktsmessig for å sammenligne svarene da alle ville fått samme spørsmål, men vi føler at det ville hatt en innflytelse på intervjuets dynamikk og naturlige gang. Gjennom vår semistrukturerte intervjuguide opplevde vi likevel at vi kunne sammenligne svarene vi fikk av informantene med hverandre.

Vi valgte å benytte oss av analyseverktøyet Nvivo, hvor vi kodet og kategoriserte dataen vi hadde samlet inn. Dette gjorde at vi kunne bruke tekstnære koder, og at vi på samme tekst kunne få flere kategorier og underkategorier. En annen måte å gjøre dette på hadde vært å foretatt en kontinuerlig kategorisk inndeling av dataen vi hadde samlet inn fra intervjuene etter hovedtemaer og spørsmål som kommer frem i intervjuguiden. Dette er en måte som ikke anbefales, da man kan få vide og forhåndsdefinerte kategorier, samt mangel på tekstnære koder (Tjora 2012, s. 179; Johannessen et al., 2020, s. 159).

3.7 Refleksjon over vår rolle som forskere

Som tidligere nevnt har alle forskere med seg en forforståelse inn i forskningsstudiet. Denne forforståelsen er viktig for at vi skal kunne forstå virkeligheten, og gi oss mening på det som skjer rundt oss (Johannessen et al., 2020, s. 26). Vår forforståelse kan prege måten vi gjør forskningsarbeidet på, og det er derfor viktig at vi som forskere redegjør for vårt eget ståsted (Tjora, 2012, s. 203). Dette kan gjøres gjennom at vi forteller om våres erfaringer, fordommer og oppfatninger som kan være en påvirkende faktor for hvordan datamaterialet har blitt tolket og hvordan vi har gått frem i prosjektet (Johannessen et al., 2020, s. 252).

Vi begge hadde ingen erfaring med digital sikkerhetskultur i kraftbransjen fra tidligere, og vi hadde heller ikke særlig stor kunnskap om temaet før vi hadde bestemt oss for å skrive om dette. Det var først etter at vi hadde lest oss opp på offentlige dokumenter, litteratur, tilgjengelige rapporter og artikler at vi forsto at det var et tema som vi hadde lite forkunnskaper om. Basert på det vi leste, gjorde vi oss noen antakelser om hvordan den digitale sikkerhetskulturen kunne være i kraftbransjen og hvilke mulige områder som kunne være av forbedringsmuligheter, herunder blant annet arbeidet med ansattes holdninger og bevissthet. Disse antakelsene pratet vi med hverandre om før vi starter med forskningsprosjektet, slik at vi var bevisst på hva vi som forskere mente og tenkte, før vi startet arbeidet med utarbeidelse av forskningsspørsmål, intervjuguide, datainnhenting og analyse. Dette gjorde vi for å hindre å gi en større verdi til potensielle funn som stemte overens med våre egne antakelser. Det gjorde også at vi forholdt seg nøytral og objektiv i intervjuene med informantene, samt hvordan vi utarbeidet intervjuguiden på med åpne spørsmål og frie forklaringer.

3.8 Etiske betraktninger

Vi har i denne forskningen vært bevisst på de forskningsetiske retningslinjene som er utarbeidet av Den nasjonale forskningsetiske komite for samfunnsvitenskap og humaniora (NESH), og vi har fulgt disse.

Vi har meldt og fått godkjenning av NSD til å drive dette forskningsprosjektet, og kunne behandle personopplysninger i tråd med personvernregelverket.

Gjennom bruk av informasjonsskriv, informert samtykkeskjema og samtale med oss som forskere, har informantene blitt gjort kjent med at deres deltakelse i dette forskningsprosjektet er frivillig, og at de når som helst kunne trekke sin deltakelse uten å måtte begrunne dette nærmere. Informantenes rett til selvbestemmelse og autonomi har derfor blitt ivaretatt.

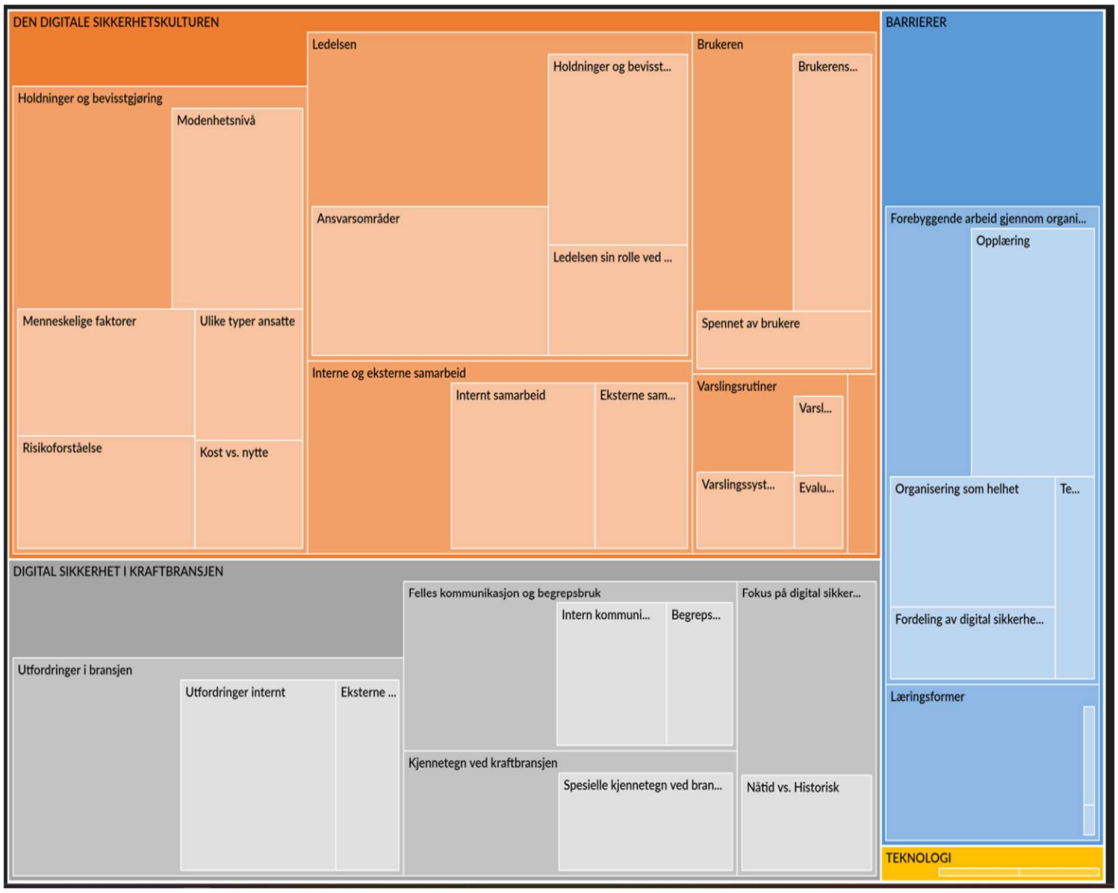
Vi har reflektert over hvorvidt vår forskning kan skade informantene som har deltatt. De spørsmålene og temaene som vi stilte informantene i intervjuet, anså vi som lite belastende å svare på. Vi gjorde oss likevel noen tanker om at informantene, gjennom spørsmålene som ble stilt under intervjuet, kunne ha følt på en slags utilstrekkelighet eller en følelse av manglede kunnskap dersom de ikke kunne svare på noen spørsmål. For å forebygge slike følelser, var vi opptatt av å snakke omkring dette med informantene i forkant av intervjuene.

Som forskere er det også viktig at vi respekterer informantens privatliv. Gjennom anonymisering og bruk av pseudonymer, har vi sørget for at informantene og deres virksomhet ikke skal bli identifisert, noe som er kommunisert ut til de som deltok. De har blitt gjort kjent med at dersom det er informasjon som gjør at man direkte eller indirekte kan identifisere dem eller deres virksomhet, vil dette bli tatt bort fra oppgaven. Vi har også gjort dem kjent med formålet og bruken av forskningsprosjektet, og hvordan deres personopplysninger vil bli behandlet og slettet.

I bunn og grunn handler det om respekt, tillit og konfidensialitet, og vi føler at dette har blitt ivaretatt under vårt forskningsprosjekt.

4 Empiriske funn

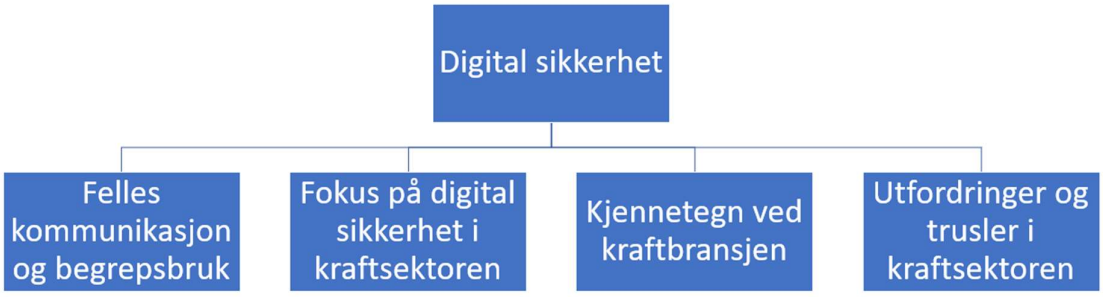
Etter datagenereringen gjennomførte vi en omfattende prosess med koding og kategorisering. Vi endte opp med 4 hovedkategorier og 13 underkategorier i første linje. Flere av underkategoriene hadde igjen egne underkategorier i andre linje. Vi vil i hovedsak presentere funnene i hovedkategoriene og underkategoriene i første linje. Der det er naturlig vil vi også presentere funn fra andre linje. Figur 4.1 viser en oversikt alt det kodede materialet i NVivo.



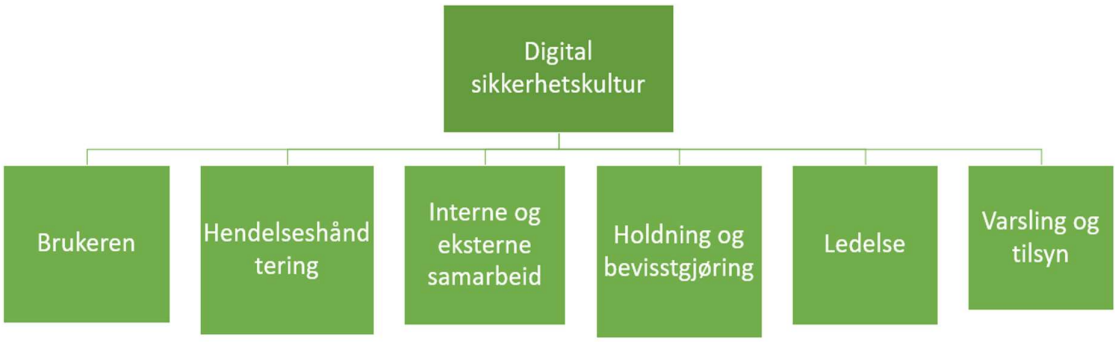
Figur 4.1 Oversikt over hoved og underkategorier, hentet fra NVivo

I arbeidet med kodingen av datamaterialet benyttet vi oss av programmet NVivo. Figuren over viser omfanget av datamaterialet og dybden i analysen gjennom hoved- og under kategorier. Som man ser av oversikten er kategoriene digital sikkerhetskultur og barrierer de to desidert største med tanke på innhold. Vi opprettet også en kategori på digital sikkerhet siden informantene hadde ulike syn på hva dette begrepet innebar. Nederste i høyre hjørne i figuren finner man kategorien teknologi. Denne ble opprettet som en samlepost for alle tekniske og teknologiske systemer som informantene nevnte i intervjuene. Siden vårt fokus

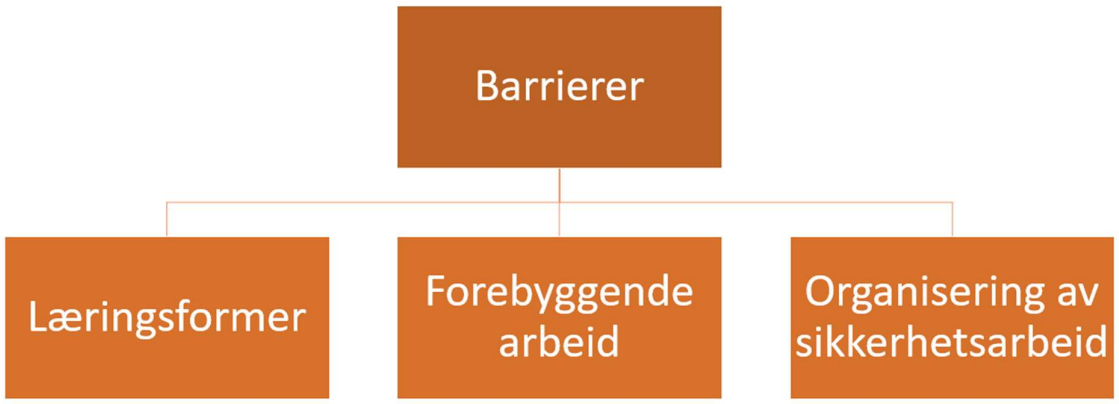
omhandler det organisatoriske og menneskelige faktorer i digital sikkerhetskultur velger vi å se bort ifra denne kategorien og fortsette med digital sikkerhet, digital sikkerhetskultur og barrierer. Figurene under viser hovedkategoriene med underkategorier (første linje). Hensikten med disse figurene er å vise en oversikt over datamaterialet som vil bli presentert i kapittel 4.



Figur 4.2. Viser hovedkategori 1 - Digital sikkerhet - med underkategorier (første linje)



Figur 4.3. Viser hovedkategori 2 - Digital sikkerhetskultur - med underkategorier (første linje)



Figur 4.4. Viser hovedkategori 3 – Barrierer - med underkategorier (første linje)

Videre vil vi presentere de empiriske funnene som tilhører hovedkategoriene. Vi vil slå sammen noen av underkategoriene (første linje) fordi flere av dem er nært knyttet sammen og påvirker hverandre, og bør dermed presenteres i samme avsnitt for å vise helheten i svarene til informantene. Samtidig vil dette bidra til økt leservennlighet. Vi har valgt å fokusere på følgende tre hovedkategorier med tilhørende underkategorier:

4.1 Digital sikkerhet

- Intern kommunikasjon rundt sikkerhets begreper
- Fokus på digitale sikkerhet
- Digitale trusler og uønskede hendelser

4.2 Digital sikkerhetskultur

- Holdninger og bevisstgjøring
- Ledelsen
- Eksterne og interne samarbeid
- Tilsyn i bransjen

4.3 Barrierer

- Forebyggende tiltak
- Spesifikke tiltak for opplæring og bevisstgjøring

Dette kapitelet har som hensikt å fremvise våre funn i intervjuene som er gjennomført og gi et innblikk i hva som er kommet frem fra informantene våre. Empiriske utdrag vil bli benyttet i teksten for å illustrere mangfoldet i funnene våre. Når vi benytter oss av sitater fra

informantene i teksten vil vi merke dem med informantenes pseudonym og om de er fagansatt (F) eller leder (L). I alt gjennomførte vi 11 dybdeintervjuer av ansatte i to forskjellige kraftvirksomheter, herunder 5 informanter med en ledende rolle i virksomheten, og 6 fagansatte på digital sikkerhet. En total oversikt over pseudonymene til informanten finnes i tabell 3.1 i kapittel 3.

4.1 Digital sikkerhet

4.1.1 Intern kommunikasjon rundt sikkerhetsbegreper

Forskjellig begrepsbruk knyttet til digital sikkerhet skaper utfordringer, noe som kom tydelig frem gjennom intervjuene. Flere av informantene forteller at de opplever at forskjellige begrepsbruk kan skape usikkerhet når man snakker om digital sikkerhet, både når det kommer til roller og ansvar, men også når det kommer til forståelsen av hva digital sikkerhet er. Flere av informantene påpeker dette eksplisitt, og andre snakker mer indirekte om det.

> Diskusjonen rundt «safety security» var pågående for 6-7 år siden. Der hadde man to grupperinger med OT-siden på den ene siden og IT-siden på den andre. Begge sidene skrek om sikkerhet. Det viste seg at begge sidene egentlig mente det samme. En IT-person snakker om IT-sikkerhet og cybersikkerhet. En person som jobber med OT snakker om personsikkerhet, driftssikkerhet og miljøsikkerhet. Det som på engelsk heter «safety», altså trygghet. Det å få adressert dette på en tydelig måte mellom miljøene i selskapet er viktig. Da gikk det fra å skrike på hverandre til at man startet å samarbeide om å løse problemstillinger. Man så hverandres behov og hvor skillene gikk mellom hvem som kunne gjøre hva, og hvilke ansvarsområder den enkelte avdeling hadde (Espen, leder).

Gjennom intervjuene ble det tydelig at ulikhet i fagmiljøer internt i virksomhetene spiller en stor rolle når det kommer til kommunikasjon. Det å ha et felles begrepsapparat er viktig for en effektiv og berikende kommunikasjon. Espen (L) forklarer hvordan han som leder har påvirket denne kommunikasjonsutfordringen internt mellom fagmiljøene.

> Siden jeg har en tverrfaglig bakgrunn skjønte jeg begge språk. Med den forståelsen innabords skjønte jeg at vi ikke snakket om det samme selv om man trodde det internt. Da jeg forklarte hva vi måtte legge i de ulike begrepene ble det en aha-

> opplevelse for de ansatte. Det gikk fra en ukonstruktiv tilværelse, til etter min subjektive oppfattelse, en konstruktiv tilværelse (Espen, leder).

Flere andre informanter peker på at begrepsbruken kun kan bli bedre hvis søkelyset og kunnskapen om hvor man vil med digital sikkerhet økes. Nils (F) forklarer det på denne måten.

> Nå ser man alt under ett, der man har det IT-tekniske, informasjonssikkerhet og cyberdomenet samlet under en paraply. Her har de nasjonale myndighetene økt bevisstheten. Vi må skape en kultur rundt det digitale rom. Vi må løfte de ansatte ved å gi de en forståelse av hva digital sikkerhet innebærer, og oppklare hva de ulike begrepene innebærer. Vi må tilpasse budskapet til alle de ulike ansatte (Nils, fagansatt)

De begrepene som er gjennomgående i intervjuene er informasjonssikkerhet, IT-sikkerhet og cybersikkerhet. Samtlige informanter beskriver en stor positiv utvikling i forståelse og kunnskaper knyttet til digitale begreper de siste fem til syv årene.

> Vi er veldig opptatt av at verken IT eller IT-sikkerhet kun skal ha et teknisk fokus. Bare IT som begrep er veldig bredt. Det er så mange ulike stillinger innenfor IT. IT i seg selv er et ord som rommer veldig mye. IT-sikkerhet kan bety alt og ingenting. Det vi jobber mye med i selskapet er at IT ikke skal ha et mål for seg selv. Det er selskapet som skal ha et mål. Alt som har med IT å gjøre må inn i virksomhetsstrategien i selskapet. Men vi har en visjon som beskrives gjennom en firkantetmodell. Den består av menneske, prosess, data og teknologi. Hele poenget med den modellen er å vise at alle disse punktene må ses på i sammenheng (Josefine, leder).

Informantene som er knyttet til fagmiljøet på digital sikkerhet forteller også om store ulikheter i kunnskap og forståelse rundt begrepsbruk hos de ansatte. I den forbindelse trekker Petter (F) frem at mange ord blir oppfattet likt av dem som ikke har digitalt arbeid som sin primæroppgave i virksomheten. Denne usikkerheten fører til misforståelser og kan oppleves som hemmende for arbeidet med digital sikkerhet.

Oppsummering av intern kommunikasjon rundt digitale begreper

Informasjonen som kommer frem under intervjuene, peker på ulike utfordringer og løsninger rundt intern kommunikasjon om digitale sikkerhetsbegreper. Flertallet av informantene trekker frem et manglende felles begrepsapparat som en kommunikasjonsutfordring. Virksomhetene i kraftbransjen er preget av mange ulike

fagmiljøer som igjen har egne termer på faguttrykk. Når ulike fagmiljøer skal samarbeide om å løse samme problem, er det et behov for et felles begrepsapparat. Har man ikke da landet noen klare prinsipper om hvordan man skal snakke sammen, kan mye av effektiviteten i arbeidet stoppe opp.

4.1.2 Fokus på digital sikkerhet

Informantene forteller om et endret fokus i bransjen. Der man før hadde fysisk sikkerhet som førsteprioritet har man nå, gjennom føringer fra NVE, satt en prioritering på digital sikkerhet. Et stort flertall av informantene sier at søkelyset på digital sikkerhet har kommet langt på vei på kort tid. Gjennom hendelser som har skjedd i bransjen og økt fokus fra media opplever informantene et mye sterkere fokus på digital sikkerhet nå enn tidligere.

> Den digitale sikkerheten er absolutt en del av den totale beredskapen vi som selskap har. NVE har flere ganger kommunisert at hvis det kommer et angrep mot kraftbransjen vil det være et hybridangrep. At flere ting skjer samtidig. Vi hadde tre hendelser i høst der drone ble brukt over våre anlegg. Vi opplever dette som en klar testing av oss og fremvisning av ressurser. Den digitale trusselen er i fred med å sette den fysiske i skyggen (Amanda, fagansatt).

Flere av de fagansatte informanter peker på at bransjen som helhet stadig blir mer og mer avhengig av digitale løsninger og sikkerheten tilknyttet de nye løsningene. Videre peker de på at samspillet mellom markedsavdelingene og OT-avdelingene utfordrer bruken av digitale løsninger, men også at denne friksjonen driver arbeidet med digital sikkerhet fremover.

> Vi blir mer og mer eksponert for trusler fra den digitale verden. Samtidig blir vi mer og mer avhengig av digitale løsninger. Det å rulle tilbake og klare seg uten de digitale systemene blir bare vanskeligere og vanskeligere. De løsningene man hadde før, forsvinner samtidig som man digitaliserer seg videre fremover (Torgeir, fagansatt)

Blant informantene er det stor variasjon når det kommer til fokus på digital sikkerhet internt i virksomhetene. Noen trekker frem ulikheter mellom fokuset til de IT-ansatte og fokuset til andre avdelinger som marked og OT-miljøene.

> Jeg opplever at folk i organisasjonen forstår hvor viktig det den digitale sikkerheten er på driftsanleggene. Holdningene knyttet til egen atferd har nok et lavere fokus. Hva skjer hvis jeg trykker på denne lenken? Hvilken informasjon sitter jeg på

> personlig? Her har vi lagt inn en kjempeinnsats for å løfte de ansatte. Det å få de ansatte til å forstå at OT henger sammen med IT er helt avgjørende for å opprettholde god sikkerhet generelt. Få de ansatte til å få et overordnet søkelys på sikkerhet (Josefine, leder)

Spesielt trekker de fagansatte informanter frem dette med forskjellen på bevissthet og kunnskap. Bevisstheten til de ansatte ble oppfattet som bra og at de ansatte ønsker å levere på dette området. Mangelen på kunnskap om hvordan man i praksis skal oppføre seg i det digitale rom eller hvilke faresignaler man skal se etter er dårligere.

Videre ble bruken av konsulenter trukket frem som en digital sikkerhetsutfordring. Siden en konsulent ofte er inne i et prosjekt i kort tid, kan dette senke fokuset de har på digital sikkerhet. De som ikke har kjennskap til bransjen, kan ha vanskeligheter med å forstå alvoret og viktigheten av digital sikkerhet i arbeidet de utfører for virksomheten.

En positiv faktor som ble trukket frem er den etablerte beredskapskulturen som ligger i kraftbransjen. Gjennom at kraftsektoren er en samfunnskritisk funksjon, er de ansatte vant med et stort fokus på sikkerhet. Denne sikkerheten har tidligere dreid seg om fysisk sikkerhet, men i de siste årene har det blitt tydelig hvilke negative følger ett digital angrep ville fått, og dermed har fokuset på digital sikkerhet økt.

> I kraftbransjen ligger det allerede en etablert beredskapskultur. Den er med på å gi en stor hjelp i sikkerhetsarbeidet. Det innebærer at mange vet hva det å sette beredskap betyr og hva som ligger i begrepet beredskap. Beredskapsarbeidet var veldig basert på flom tidligere. Gjennom Covid-19 og krigen i Ukraina har fokuset på kritisk infrastruktur økt. Fokuset på cyberhendelser har også bidratt til et økt fokus på digitalt beredskapsarbeid. Vi som selskapet har fått en oppvåkning. (Josefine, leder)

Oppsummering av fokuset på digital sikkerhet

Når det kommer til fokuset på digital sikkerhet i kraftbransjen trekker flere informanter frem den allerede etablerte beredskapskulturen som en viktig positiv faktor. Siden bransjen alltid har hatt et fokus på sikkerhet ligger dette godt implementert i de ansattes tankegang. En klar utfordring som flere nevner er den lave kunnskapen de ansatte innehar om digital sikkerhet, fordi spennet i de ansatte er stort, og erfaring rundt digitale plattformer er ulik. Noen informanter trekker frem bruken av konsulenter som utfordrende. Dette fordi de ofte er inne i virksomheten i en kort tidsperiode og ikke på samme måte blir en del av sikkerhetskulturen. Samlet sett forteller informantene om at fokuset på digital sikkerhet har

gått opp. NVE og media blir trukket frem som to viktige faktorer som har økt fokuset til de ansatte og ledelsen.

4.1.3 Digitale trusler og uønskede hendelser

Det er tydelig at de fleste informantene har et forhold til digitale trusler og uønskede hendelser. Det fortelles om både direkte rettede angrep mot virksomhetene og angrep som er ment å treffe en bred målgruppe, og flere forsøk blir stoppet av systemer som overvåker trafikken døgnkontinuerlig. Ingen av informantene opplyser om digitale angrep som har ført til alvorlig skade, for eksempel med tap av sensitiv informasjon eller nedetid på systemene i virksomhetene.

> På loggen til IKT ser man en stadig strøm av angrep som kommer mot virksomheten. Det kan være masseskadevare og direkte angrep. Brannmurene holder den beredskapen oppe hele tiden og dette er tjenester som vi betaler for at folk overvåker. Her blir vi oppdatert med informasjon om ulike type faktorer vi må se etter på epost eller andre områder (Amanda, fagansatt).

Flere at de fagansatte informantene forteller om mer utspekulerte trusselutøvere nå enn før. Angrepene er mer skreddersydd og målrettede mot spesifikke ansatte. Det innebærer at det kan være innhold som et tilpasset årstiden vi befinner oss i, som for eksempel at ved juletider kommer det hentemeldinger fra posten, og mot sommeren kommer det innhold som ligner en digital skattemelding. Phising-angrep og ransomware (løspengevirus) blir nevnt av de fleste informantene som de mest vanligste digitale angrepene virksomhetene opplever, og epost blir beskrevet som den største angrepsvektoren.

> Skreddersydde og målrettede angrep mot ansatte er veldig vanskelig å forebygge. Angrepet vil være så innarbeidet at de har sett på dialoger som personen har hatt i det daglige med andre. De ser på hvordan denne personen har kommunisert med den ansatte på mail. Da kan man bruke dette mot andre personer i bedriften. Stopp og tenk mentaliteten må være på plass (Petter, fagansatt).

Når det gjelder digitale angrep fra statlige aktører, forteller flere informanter om at man må ha som utgangspunkt at statlige aktører har både evne og vilje til å bryte seg inn i systemene.

> Vi vet lite om evne og vilje til statlige aktører. Vi vet at disse har kapasitet til å ta seg inn hvis de ønsker det. Vi må ta utgangspunkt i at de aktørene har både vilje og evne til å bryte seg inn i systemene våre (Amanda, fagansatt).

Informantene forteller at krigen mellom Russland og Ukraina har gjort at de som samfunnskritisk funksjon følger nøye med på situasjonen.

> Når det kommer til trusler, så er vi veldig klare over det som skjer i Ukraina, og er veldig klar over vår posisjon. Vi er jo en samfunnskritisk infrastruktur. Det betyr at hvis vi går over i en situasjon i krise/krig-skalaen, så er vi veldig utsatt. Så vi følger situasjonen nøye. Nå har den pågått i snart ett år, og vi innser at det er den nye normalen at vi alltid må være beredt (Ivar, fagansatt).

Oppsummering digitale trusler

Kraftbransjen opplever og mottar digitale trusler, men ingen av informantene har opplevd vellykkede angrep. De fleste digitale angrep blir stoppet av overvåkningssystemer. Phising-angrep og løsepengevirus blir trukket frem som de mest aktuelle digitale truslene. Disse truslene blir beskrevet som mer utspekulerte, troverdige og vanskeligere å detektere. Skreddersydde og målrettede angrep mot ansatte oppleves som vanskelig å forebygge, og epost blir beskrevet som den største angrepsvektoren. Som en samfunnskritisk infrastruktur er informantene klare på at de er ett potensielt mål for statlige aktører, og det tas utgangspunkt i at statlige aktører har både vilje og evne til å bryte seg inn i systemene.

4.2 Den digitale sikkerhetskulturen

4.2.1. Holdninger og bevisstgjøring

4.2.1.1 Menneskelige faktorer

Samtlige informanter trekker frem betydningen av den menneskelige faktoren i det digitale sikkerhetsarbeidet som viktig. Flere forteller at de tekniske systemene fungerer godt, men at de tekniske systemene i seg selv ikke er nok til å ha et tilstrekkelig godt forsvar mot digitale trusler. Nesten alle informantene legger stor vekt på at et vellykket angrep mot virksomheten mest sannsynlig innebærer en menneskelig svikt.

> Teknologien vil bestandig kunne brukes som man vil, men det er kulturen som skaper det samholdet som gjør at de ansatte tar gode og selvstendige beslutninger. Det at hver enkelt avdekker faremomenter selv er viktig. At de ansatte selv tør å

> spørre om å få se adgangskort på personer de er usikre på, er der vi ønsker å ende opp. Å ha en kultur som gjør at folk sammen avdekker disse sikkerhetshullene er viktig, og dette skjer gjennom å ha kunnskap og interesse. Vi har tatt store steg på dette området gjennom å ta dette inn i alle prosesser i virksomheten (Nils, fagansatt).

Bjørn (F) beskrev hva ha han legger i menneskelige faktorer ved å bruke et eksempel der et menneske bor i en landsby med butikker og hus. Det hele starter med at menneske blir redd for tingene sine inne i huset, og dermed setter opp et gjerdet rundt huset. Huset blir veldig sikkert, og ingen kommer seg inn i huset til personen. På et tidspunkt må personen på butikken fordi personen blir sulten. Han lager en port i gjerdet, og dermed opprettholdes ikke integriteten til gjerdet, fordi det kan åpnes med en dør. Poenget med denne beskrivelsen er at menneske alltid vil være påvirkelig til å gjøre handlinger som ikke er helt sikre og hvis tiltakene oppleves som svært inngripende vil menneske mest sannsynlig finne en annen metode for å komme rundt sikkerhettiltaket. Simen (F) påpeker at det alltid vil være mennesker som opererer de tekniske barrierene til selskapet. Derfor vil den menneskelige faktoren alltid være avgjørende for å forhindre et angrep.

Nils (F) forteller at det er viktig å sette inn tiltak for å styrke det holdningsskapende arbeidet. Den tekniske infrastrukturen vil svært sjeldent føre til uønskede hendelser, så han mener at det å fokusere på holdninger hos de ansatte i virksomheten tilknyttet det digitale er viktig. Videre trekkes det frem av flere informanter at det digitale sikkerhetsarbeidet bør likestilles med HMS-arbeidet (helse, miljø og sikkerhet), og om den menneskelige faktoren skal tas på alvor og underbygge det statistikken sier om hvem som er mest utsatt, må man prioritere mer penger og ressurser på området.

> IT-sikkerhet er litt som HMS. Du kan ikke kjøpe løsninger som fikser HMS problemet helt og fullt. I bunn og grunn så er det folks holdninger som utgjør om HMS-arbeidet er godt eller ikke. Fokuset på folks holdninger er viktig her. Man må lære folk opp i hva risiko er, og når og hvordan man skal ta kontakt hvis man er usikker. Først da vil man skape gode holdninger rundt digital sikkerhet. Det er ikke nok med tekniske løsninger (Petter, fagansatt).

Noen informanter sier at den enkelte ansattes fokus på digital sikkerhet har økt, men at holdningene til de ansatte er noe som tar tid å få på plass.

> Det er en endring i folks syn på verden, ikke nødvendigvis holdningene. Hvis vi tar et eksempel: du kjører bil, og ser at det har kommet opp ett skilt med gul bakgrunn

> og en fartsgrense som er lavere enn det du bruker å kjøre der til vanlig. Du ser ingen som jobber i området, og spørsmålet blir da hvor lenge du gidder å kjøre i 50 km/t, da det i tilfellet skulle være noen som jobbet der en eller annen dag. Du vet at du skal følge reglene eller at du burde ha gjort det, men du gjør det ikke (Bjørn, fagansatt)

Josefine (L) beskriver rollen menneske har i hennes tilnærming til arbeidet med digital sikkerhetskultur. Hun legger vekt på at teknologi og menneske må ses på som en helhet og dermed ikke kan utelukkes fra hverandre.

Oppsummering av menneskelige faktorer

Informantene trekker frem ulike punkter når de omtaler menneskelige faktorer. Det som er tydelig gjennom intervjuene er at alle omtaler menneske som helt avgjørende for å lykkes med god digital sikkerhet, da tekniske systemer ikke kan sørge for den digitale sikkerheten alene. Informantene er usikre på om de ansatte har forståelse for eller kunnskap om hva en enkel feil hos dem kan utgjøre. Det brukes mye tid og ressurser på å treffe riktige tiltak for å bedre det holdningsskapende arbeidet og gjennom dette forbedre menneskets holdninger, bevissthet og kunnskap om digital sikkerhet.

4.2.1.2 De ansattes bevissthet og kunnskap om digital sikkerhet

De fleste informantene beskriver at det virker som om de ansatte har gode holdninger og bevissthet til digital sikkerhet, men at kunnskapen i mange tilfeller er mangelfull. Informantene trekker frem ulike metoder for å øke bevisstheten gjennom kunnskap om digital sikkerhet, med for eksempel ulike phising-tester, e-læring, samt informasjon om teamet digital sikkerhet. IT-ansatte har en god bevissthet og kunnskap på digital sikkerhet, mens de som ikke jobber direkte med IT har en vei å gå. De fleste er enige om at arbeidet har kommet godt på vei.

> Bevissthet rundt cyberdomenet har økt. Man har kommet lengre enn at man bare tenker IT tekniske løsninger. Når ser man alt under ett der man har IT tekniske, informasjonssikkerhet og cyberdomenet. Her har de nasjonale myndighetene økt bevisstheten. Vi må skape en kultur rundt det digitale rom. Vi må løfte folk ved å gi de en forståelse av hva det innebærer. Oppklare hva de ulike begrepene innebærer. Tilpasse budskapet til alle de ulike ansatte. (Nils, fagansatt)

Kunnskaper er viktig for å øke bevisstheten. Espen (L) forteller om en bransje som har brukt utallige millioner på å unngå fysiske skader. Han mener at testene og informasjonen som omhandler digital sikkerhet blir for sporadisk, og at det vil kreves en helt annen satsning

for å komme til det modenhetsnivået man bør inneha på digital sikkerhet. Fokuset som enda ligger på holdningsskapende arbeid rundt HMS må i større grad dreies over på det digitale. Det handler om å ha en strategi som påfører de ansatte nok opplæring og kunnskap til å skape gode motstandsdyktige ansatte på digital sikkerhet.

Ivar (F) opplever at holdningene til de ansatte er gode, og at det er gjennom opplæring fra de fagansatte og tydelige prioriteringer fra ledelsen, at bevisstheten og kunnskapen vil øke til et tilfredsstillende nivå.

> Utfordringen går ikke på holdninger, men det går på kunnskap og erfaring. Sånn at jeg opplever ikke at noen stiller seg på bakbeina og sier dette bare er tull. Det handler mer om at de ikke har visst hvordan de skal forholde seg til det, eller ikke er i stand til å definere trusler eller anonymiteter eller rare e-poster, fordi de vet ikke hva de skal se etter. De har ikke gjort det før, og har heller ikke mye erfaring med bruk av pc. Jeg opplever ikke motstand til det vi gjør. Det er åpenhet og interesse for å lære om teamet (Ivar, fagansatt).

Espen (L) trekker frem de ansattes bevissthet rundt bruken av sosiale medier. Det at mange gir fra seg store mengder personlig informasjon på ulike apper er utfordrende, og kan bidra til at trusselutøverene lykkes i sitt digitale angrep mot virksomheten. Bevisstheten den enkelte ansatte har rundt egen adferd på nett er lav mener informanten, og dermed kan dette gi negative konsekvenser for virksomheten sin digitale sikkerhet. Det at ansatte ikke klarer dette skille mellom jobb og privat er et problem sikkerhetsmessig. Videre ble ulikheten mellom de unge og de eldre ansatte trekket frem, og han er mer bekymret for de unge ansattes ukritiske opptreden på internett enn de eldre ansatte som i liten grad benytter seg av sosiale medier.

Oppsummering holdninger og bevisstgjøring

Informantene har pekt på mange ulike måter å jobbe med bevisstgjøringen rundt digital sikkerhet. Kunnskap er nøkkelen mener flere av informantene. Skal man klare å påvirke de nok og riktig, må enkeltindividene forstå hvilken rolle de har i dette arbeidet. Ulikheten som finnes hos de yngre og eldre ansatte i virksomheten når det gjelder bruk av sosiale medier, trekkes frem som en utfordring. Videre sier informantene at de jobber mye med å treffe riktige tiltak i opplæring og kunnskapsoverføring av de ansattes bevissthet og holdninger til digital sikkerhet.

4.2.1.3 Marked versus digital sikkerhet

Alle virksomheter vil måtte gjøre prioriteringer med de midlene man har til rådighet

ifølge flere informanter. Informantene setter søkelyset på skjæringspunktet mellom markedssiden og OT-miljøet på den andre siden. Kjernen i dette temaet er tilgangen på data som igjen danner grunnlaget for markedssituasjonen i virksomhetene. Flere peker på at å selge inne ekstra sikkerhet er vanskelig og krevende. Noen informanter trekker også frem at kraftbransjen er i en særskilt stilling siden de produserer strøm som alle må ha, og har dermed en god flyt av penger. Dette skaper et godt utgangspunkt for å drive digitalt sikkerhetsarbeid.

> Nå vil man innhente data fra anlegget som sier noe om statusen til komponentene. Dette vil være ekstremt kostnadsbesparende, og gjøre at man i stor grad kan gå bort fra vedlikeholdsarbeid som har vært styrt av tidsintervaller. Får å få til dette må du ha ut data som tradisjonelt kun har ligget i beskyttede soner. Her vil et samarbeid for å lage et rammeverk som sier hvordan denne dataen sikkert kan hentes ut være viktig (Petter, fagansatt).

Flere av informantene mener at dette er kjernen av kost/nytte utfordringene i virksomhetene. Hvor mye data skal bli tilgjengeliggjort og hvor sikkert skal denne tilgjengeliggjøringen være for at det ikke skal gå ut over den digitale sikkerheten til selskapet.

> En annen utfordring er at noen sier at alt kan løses ved nok tilgang på data. Dette er en sannhet med modifikasjoner. Vår hovedoppgave er å produsere strøm. Denne produseres ved vann og lite data. Derimot går vi nå ut og sier at vi skal bli ledende innen prediktivt vedlikehold. Da har vi staket ut en kurs som krever enorme mengder data. Men da er det er målrettet og gjenkjennbart fokus som de fleste kan kjenne seg igjen i og forstår. Det er en stor forskjell fra det utsagnet til at vi bare skal finne noe fantastisk bare vi får tilgang på data. Gjennom å ha dette fokuset på hva som er målet, skapes en god kultur rundt digital sikkerhet (Espen, leder).

En fagansatt informant underbygger dette synet og sier at dette arbeidet aldri vil være godt nok, men at man sammen må ha et sterkt fokus på å løse de sikkerhetsutforinger som dukker opp. Gir man OT-miljøet rett vil virksomheten tape penger, mens hvis markedsmiljøet vinner denne striden vil risikoen være større og beredskapen vil trolig svekkes ved anleggene.

> Du kan ikke i den digitale verden si at nå har vi løst sikkerhetsutfordringen, det er et kontinuerlig arbeid. Det er hele tiden nye sårbarheter og utfordringer som må løses for å opprettholde produksjon av strøm som er vår viktigste oppgave. Vi må på en måte ta hull i veggen som skulle være tett. Dette må vi gjøre på en sikker måte (Ivar, fagansatt)

Et annet synspunkt som kom frem fra enkelte informanter er satsningen til ledelsen på digital sikkerhet. Her opplevde noen av informantene et større fokus på utvikling og innovasjon enn digital sikkerhet. Kraftsektoren lever av å selge strøm, så det vil ofte oppstå en kamp mellom hvem som skal få hvilke ressurser. Stian (L) forteller om et stort fokus på utvikling i virksomheten. Ledelsen har ansatt masse ansettelser av utviklere, men har ikke klart å utligne dette som han mener er det mest elementære, altså sikkerhetsfolk. Han tror det skyldes at det oppleves som kjedelig å bruke penger på, og at det er vanskelig å måle effekten av forebyggende arbeid på digital sikkerhet. Han sier videre at denne sikkerhetskapasiteten slår negativt ut på den digitale sikkerheten i prosjekter. Han sier tilslutt at det at IT-folkene er overarbeidet er en sikkerhetsrisiko i seg selv.

> Jeg var redd for at det bare skulle bli ansatt utviklere, og folk som drev med innovasjon. Og at vi som drev med forvaltningen av de mest kritiske tingene var litt underbemannet, det var ubehagelig en periode (Stian, leder)

Oppsummering av sikkerhet versus marked

Det fremstår på flere informanter at markedskreftene kan styre mye av ressursene og at sikkerheten kan komme litt i andre rekke. Dette kan tyde på en kamp mellom det å tjene penger på nye produkter versus det å lage sikre produkter. Flere peker på at ledelsen har et spesielt ansvar her for å kunne opprettholde en balanse mellom innovasjon og sikkerhet.

4.2.2 Ledelsen

4.2.2.1 Ansvarsfordeling

De fleste informantene opplever ansvarsfordelingen til ledelsen som god. Det mange derimot peker på er at beslutningene omkring digital sikkerhet må tas på riktig nivå og med personer med tilstrekkelig digital kompetanse. Flere informanter forteller om en god utvikling i arbeidet med å fordele ansvar på riktig nivå og at det oppleves som at tilliten til de fagansatte er god. Det resulterer i at flere avgjørelser kan tas fortløpende og i mindre grad bremser arbeidet i selskapene.

> Ledernivå 1 i selskapet ville ikke forholde seg til slike diskusjoner. Det for mange forkortelser og for teknisk. Derfor ble det lagt til nivå 2 i selskapet. Her hadde krigen stått før. Det å enes om ansvarsområder og finne prinsipper å jobbe etter ble nøkkelen. Du må ha nok fagkunnskap for å skjønne betydningen av det du snakker om, samtidig som du må se en større helhet (Espen, leder).

Josefine (L) snakker også om det samme. Hun peker på at når man skal utfordre etablerte prosesser kreves det at riktige folk snakker sammen og finner gode digitale sikkerhetsløsninger.

> En diskusjon man ofte havner i er hvem som skal eie risikoen for prosjektet. Jeg ser at det å tydeliggjøre ansvar og eierskap er helt avgjørende i prosessene. Når du utfordrer de etablerte prosessene, er det viktig å ta de riktige diskusjonene. Når en krise inntreffer ser man gjerne hvem som burde hatt hvilke ansvar. Hvordan fungerer prosessene og hvem hadde eierskap. Dette er viktige diskusjoner å ta tidlig for å unngå ansvarsfraskrivelse (Josefine, leder)

Amanda (F) forteller om en ledelse som har positive holdninger til digital sikkerhet, men mangel på motivasjon til å sette seg inn i avansert IKT-materie. Hun sier de har en grei forståelse av at hvis selskapet blir utsatt for et angrep vil det få store konsekvenser for selskapet. Men siden materien ofte er teknisk eller komplisert faller mange ledere av på det øverste nivået. Dette har resultert i at beslutningsmyndigheten har blitt flyttet ned til de fagansatte på digital sikkerhet. Hun tror at det digitale sikkerhetsarbeidet oppleves som en brems og litt tungvint hos enkelte i ledelsen.

En annen leder informant tar også opp denne problemstillingen som nevnt over. Han kaller det for modenhet. Han ser at det digitale sikkerhetsarbeidet er forankret hos ledelsen, men at det er veldig opp til den enkelte fagansatte å selge dette inne på en slik måte at sikkerhetsarbeidet kommer inn på riktig nivå og tidspunkt. Han mener at ledelsen i veldig stor grad legger dette ansvaret over på de fagansatte og at de må være veldig på for å lykkes. Han ser på de fagansatte på sikkerhet som selgere. Lykkes de med å være med fra start, blir de oppfattet som en katalysator, mer enn en bremsekloss.

Petter (F) på sin side påpeker at ledelsen med hell kan komme med enda klarere føringer for hvem som skal drive det digitale sikkerhetsarbeidet. Han peker på at tradisjonelt sikkerhetsarbeid som HR (Human Resources) kunne spilt en større rolle på informasjonssikkerhetsarbeidet.

> Informasjonssikkerhet er noe IT jobber med og vi har ansvar for gjerne de digitale løsningene. Like viktig er arbeidet til HR her. HR skal sørge for at kompetansenivå til de ansatte er riktig i forhold til den stillingen og arbeidsoppgaver de utfører. I mange land spiller HR en større rolle i informasjonssikkerhetsarbeidet enn det de kanskje gjør

> i Norge. Jeg tror man kunne høstet mer nytte av HR i digitalt sikkerhetsarbeid (Petter, fagansatt).

Tre av informantene forteller om hvordan ledelsen i selskapet hadde innført noe som het tjenesteorganisasjon. Dette innebærer at alt som innføres av tjenester eller produkter skal ha en tjeneste-eier som skal stå ansvarlig for risikoen og kostnader ved prosjektet. På den måten har man flyttet mye av ansvaret bort fra IT-avdelingen og over på de ulike avdelingene som faktisk utvikler tjenesten. Dette mente flere av informantene har økt modenhetsnivået og at den totale digitale sikkerhetskulturen har løftet seg. Ved denne organiseringen kan man ikke lenger bare peke på IT hvis noe blir fort dyrt eller ikke funker.

> For tanken med domenearkitektur er at vi går fra kommunisme til demokrati. Tidligere var alt styrt med jernhånd i fra IT, men nå er det det frie valg. Nå er det sånn at domenene kan velge å kjøpe tjenesten fra noen andre. Det er bare et men. Det får noen konsekvenser. Og når vi ramser opp de konsekvensene, ender det med at de kjøper det fra oss allikevel. For single-sign on, monitorering, back up, alt som vi har bygget inn i tjenestene våre. De må ordne dette selv, og det skjønner de at de ikke er i stand til (Stian, leder)

Espen (L) forklarer at det koker ned til å kommunisere og bygge organisasjoner som utvikler gjensidig tillit mellom de ulike avdelingene. For å løse problemstillinger må det gis nødvendige rammer som inneholder tilstrekkelig tid og kompetanse. Dette er så enkelt og så vanskelig på samme tid. Siden bransjen inneholder så mange ulike interessenter, må alle bli hørt og sett. Hvis dette ikke skjer med gode nok rammer, vil ikke de gode løsningene finne hverandre og dermed vil arbeidet stoppe opp.

Oppsummering ansvarsområder

Flere informanter sier at ansvaret for digital sikkerhet har tradisjonelt sett ligget hos IT-avdelingene i selskapene. At ansvaret nå i større grad forankret hos ledelsen i selskapene fører til at andre avdelinger føler et større eierskap til digital sikkerhet. Flertallet av informantene setter søkelyset på at diskusjonene om hvilke ressurser og kompetanse bør finne sted på riktig nivå i virksomhetene. Det vises også til at en forankring hos ledelsen ikke nødvendigvis er tilstrekkelig, men at man også har behov for klare retningslinjer og instrukser for å vite hvem som har ansvaret.

4.2.2.2 Ledelsens holdninger og bevissthet knyttet til digitalt sikkerhetsarbeid

Flere informanter forteller at holdningene og bevisstheten til ledelsen i selskapene har

hatt en stor utvikling de fem siste årene. Gjennom konferanser og trusselbildet i Europa har fokuset til ledelsen dreid seg fra mer tradisjonell sikkerhet til digital sikkerhet. Både nasjonale og internasjonale uønskede hendelser og kriser at løftet holdningene og bevisstheten til ledelsen.

> Ledelsen har også fått et økt fokus på digital sikkerhet. Det tas opp mye hyppigere på konferanser enn tidligere. Det har vært flere hendelser som har kostet aktører mye penger. Hydro eksempelet blir brukt mye i vår bransje. Nortura blir også trukket frem som et skrekkeksempel. Der stoppet prosessen opp på bakgrunn av et digitalt cyberangrep. Der kostet det flere hundre millioner å gjenopprette produksjon. Disse hendelsene øker interessen hos ledelsen, og jeg ser tydelig et skifte i økt fokus for ca. 3-4 år tilbake siden. Før tenkte ledelsen at dette er noe IT har kontroll på, mens nå følger ledelsen i større grad med på det digitale sikkhetsarbeidet (Petter, fagansatt).

Petter (F) trekker frem at siden kraftbransjen er regnet som en samfunnskritisk funksjon må ledelsen ta innover seg selskapenes betydning i samfunnet og sårbarhet for digitale trusler. Han peker videre på at etterretningsarbeid i fredstid er noe man vet flere aktører driver med, og at informasjon som innhentes i fredstid vil bli brukt ved en fremtidig konflikt. Han mener ledelsen har en bedre risikoforståelsen i dag enn tidligere, og derfor får forebyggende digitalt sikkerhetsarbeid mer fokus og ressurser.

> Før jeg startet var det ikke noen særlige digitale prosesser på gang og heller ikke noen organisasjon som støtte opp under dette. Når har man bygget opp dette på en helt annen måte. Det å få tak i dyktige folk er vanskelig så man må bygge opp mye selv i virksomheten. Man har iverksatt dette strategisk i virksomheten, i det operative leddet og i en kombinasjon med beredskapsleddet. Dette skal det skape de egenskapene man trenger til å håndtere oppdukkende hendelser. Dette er proaktive, reaktive og detekterende tiltak (Nils, fagansatt)

Mange informantene bruker mye tid på å påvirke ledelsen gjennom informasjon om digital sikkerhet. Flertallet opplever dette informasjonsarbeidet som krevende, men helt avgjørende for å vise viktigheten av jobben deres på gulvet. Holdningen og bevisstheten til ledelsen er det som til syvende og sist avgjør hvilke rammebetingelser som skal besluttes i de ulike avdelingene.

> Ledelsen er de som godkjenner hvor mye ressurser som skal brukes og de som sitter ved ansvaret. De må vurdere risikoen. Jeg merker et økt fokus på digital sikkerhet.

> Gjennom de foraene ledelsen får informasjon fra ser man et økt fokus på digital sikkerhet. Jeg initierer ofte selv kontakt med ledelsen hvis jeg ser informasjon på området som jeg selv mener er relevant for ledelsen. Det går som regel fra meg og opp i systemet. Ofte er fokuset styrt av oss på IKT. Jeg opplever gehør i ledelsen på de tingene jeg tar opp. Hvis vi dokumenterer en problemstilling godt med kost/nytte vurderinger har ledelsen så høy tillit til oss at de godkjenner våre anbefalinger (Petter, fagansatt)

Espen (L) forteller at holdningene til digital sikkerhet er god blant ledelsen, men han trekker frem viktigheten av kunnskap om digital sikkerhet. Han har et inntrykk av at noen ledere bare sier ja uten å kjenne til konsekvensene av avgjørelsen som blir tatt. Derfor legger han stor vekt på sammensettingen av mennesker som sitter i ledergruppen. Det å ha et ledelsesmiljø som lytter og ikke opptrer overkjørende er viktig. Han trekker frem at det er i detaljene at utfordringene i problemløsningene sitter. Det å ha ledere med inngående kjennskap til digital sikkerhet er til stor hjelp. Josefine (L) underbygger dette poenget med at ledelsen sin rolle er å gi støtte til de ansatte og vise gjennom prioriteringer at digital sikkerhet blir tatt på alvor. Det holder ikke bare å snakke i store ord uten å vise handlekraft og faktisk betale den prisen det koster. Hun forteller at digital sikkerhet har blitt løftet til topp 3 risikofaktorer i virksomheten. Ved å plassere dette så høyt på prioriteringslisten, må ledelsen forholde seg til det.

Magne (L) forteller at stillingen CISO (Chief Information Security Officer) har vært avgjørende for å forbedre holdningene og bevisstheten til lederne i virksomheten. Samspillet som stillingen CISO fører til, gir store positive effekter. Han ser at denne rollen påvirker ledelsen til å opprettholde et godt bevissthetsnivå som bidrar til bedre risikoforståelse i ledelsen.

> Nå har vi gjort noe smart, som CISO skal ha æren for. Ved en gjennomgang av trusselbildet og mer, skapte CISO et slags beslutningsunderlag, hvor han ønsket at konsernledelsen forpliktet seg til at vi skulle opp på et modenhetsnivå på fire av fem på IT-sikkerhet. Og jeg føler at det er ganske viktig og avgjørende, fordi du ønsker jo backing i fra øverste hold når du skal investere i ressurser og teknologi for å sikre seg mot trussel og aktører. Det har gjort arbeidet vårt mye enklere når vi innfører ny arkitektur som er kostbar. Sikkerhet er kostbart. Det er sånn berømt trekant, som heter kostnad, tilgjengelighet og sikkerhet. Også skal du balansere mellom der (Magne, leder)

Oppsummering ledelsens holdninger og bevissthet knyttet til digitalt sikkerhetsarbeid

Informantene forteller at ledelsens holdninger og bevissthet har en stor påvirkning på det digitale sikkerhetsarbeidet. Informantene er tydelige på hvilken rolle ledelsen spiller ved å gi riktige ressurser og sette gode rammer for dette arbeidet. Det at konkrete stillinger som CISO jobber med samhandling peker flere av informanter på som et stort utbytte for ledelsen og de fagansatte i virksomheten når det kommer til risikoforståelse og digital sikkerhet. Holdningene og bevisstheten til ledelsen har også fått drahjelp fra sikkerhetshendelser som har skjedd.

4.2.2.3 Ledelsens rolle ved utvikling og bevisstgjøring av digitalt sikkerhetsarbeid

Flere informanter er klare på at ledelsen spiller en stor rolle knyttet til å utvikle og bevisstgjøre de ansatte i arbeidet med digital sikkerhetskultur. Det ble sagt at samspillet mellom lederne og de ansatte er avgjørende for å bedre den digitale sikkerhetskulturen.

> Som leder er mitt ansvar å sette IT sikkerhet på agendaen, heie og få inn riktige folk med riktig kompetanse. Dette er ett området som er i konstant utvikling. Det handler i stor grad om læring og feiling. Gjennom dette å bli bedre og bedre. Når du skal drive dette arbeidet som leder kan du ikke bruke pisken og være for rigid. Du kan ikke kjefte på folk. Det handler om å skape trygghet og glede hos de ansatte når de jobber med IT sikkerhet. På den måten vil de oppleve mestring på dette området (Josefine, leder).

Noen av de fagansatte beskrev dette arbeidet som langsomt og vektla samspillet mellom de ansatte og ledelsen. Det å endre er organisasjon er noe som tar tid. Her ble det tatt opp at den nye digitale sikkerhetskulturen må tilpasses den gamle og gradvis bygges opp over tid. En av informantene beskrev det han kalte for «security champions». Dette innebærer at nye ansatte ser opp til personer som leder vei og gir opplæring på en trygg og god måte om digital sikkerhet. Dette vil resultere i at de ansatte blir vare på sine omgivelser og melder ifra hvis noe er unormalt eller ikke passer inne i hverdagen.

Flere informanter trekker frem at ledelsen har sett betydningen av en CISO og på den måten løftet det digitale sikkerhetsarbeidet flere hakk. Det at ledelsen har innsett hvor viktig denne stillingen er har gjort at slike stillinger har blitt opprettet i flere virksomheter, og på den måten har ledelsen tilrettelagt for et godt miljø rundt digital sikkerhet.

> Jeg opplever at ledelsen ønsker å satse på sikkerhet og holdningsskapende arbeid. De ønsker at vi skal satse på sikkerhet, fordi de ser gevinsten, men også fordi CISO er

> veldig flink til å informere om trusselbilde og argumentere for å gjøre det vi gjør. Så han spiller oss veldig god, så vi får drive med det vi tror er viktig (Ivar, fagansatt).

Enkelte informanter har uttrykt at forventingene til ledelsen i større grad enn tidligere henger sammen med gjennomføringene av tiltakene til ledelsen. Espen (L) sier det har vært uønskede hendelser der inntrykket av ledelsen har vært at de ikke bryr seg eller henger med på hva denne hendelsen innebar eller kunne ført til av skade på virksomheten. Nå ser han en tydelig endring der ledelsen har rigget virksomheten på en helt annen måte. Det har blitt ansatt flere spesialister, og kunnskapen internt har økt på det digitale sikkerhetsområdet. Dette samspillet skaper en god friksjon som igjen finner de beste løsningene. Her har ledelsen inntatt en betryggende rolle ovenfor de ansatte og innehar nå en god forståelse hva det innebærer å finne sikre nye løsninger for virksomheten. Derfor mener informanten at forventingene i mye større grad henger sammen med gjennomføringene som ledelsen iverksetter.

Oppsummering ledelsen sin rolle ved utvikling og bevisstgjøring av digital sikkerhet

Flere informanter er bevisste på hvilken rolle ledelsen spiller i det digitale sikkerhetsarbeidet. Informantene ser at sammenhengen mellom forventingene fra de ansatte til ledelsen og hva ledelsen faktisk gjør på dette området, har styrket seg. Mange peker på stillingen som CISO som mye av nøkkelen til at ledelsen har løftet dette arbeidet. Det har ført til jevnlig påfyll til ledelsen om hvordan situasjonen er i virksomheten, noe som igjen fører til en økning i fokuset ledelsen har når det gjøres prioriteringer rundt digital sikkerhet. Noen trekker frem hvordan ledelsen kan trygge og ta ansvar for å skape gode tverrfaglige team som finner løsninger sammen og med riktige rammebetingelser.

4.2.3 Eksterne og interne samarbeid om digital sikkerhet

4.2.3.1 Eksterne samarbeid

Flere informanter forteller om hvor sentralt det eksterne samarbeidet er med andre aktører. Det mest sentrale som blir trukket frem er rollen som Kraftcert spiller for å opplyse og gi nødvendig kunnskap for å bekjempe digitale trusler.

> Kraftcert har vokst og er et forum der du kan dele erfaringer og løsninger som vi burde jobbe i fellesskap med. Vi har også mindre forum som FSK [Forum for sikkerhet i kraftforsyningen]. Dette er et eldre samarbeid enn Kraftcert. Her jobbes

> det mye med felles maler på hvilke krav man skal stille til leverandørene. Får man til dette vil det bli lettere å kjøpe tjenester, samt sette et kvalitetskrav (Petter, fagansatt).

Nils (F) forteller om et samspill som består av flere aktører. Kraftcert og NVE utfyller hverandre med å ha ulike ansvarsområder. Han trekker også frem FSK som er viktig forum for å utvikle samarbeidet mellom selskapene og sammen lage veiledere som øker den totale digitale sikkerheten. Siden bransjen hele tiden ønsker å digitalisere løsninger fra fysisk til digitalt, er behovet for eksternt samarbeid stort.

Espen (L) delte det eksterne samarbeidet opp i fysiske og digital samarbeidet. Han så tydelig en ulikhet i hvordan informasjonen fra hendelser ble delt til bransjen. Ved fysiske hendelser kommer informasjonen veldig raskt, mens ved digitale hendelser kan det ta lengre tid.

Andre informanter forteller om personavhengig samarbeid, og at det finnes en redsel for å dele for mye informasjon med andre virksomheter i kraftsektoren.

> Vi er ikke konkurrerende på sikkerhet. Det er ikke der vi skal hente pengene. Vi er alle interessert i at forsyningssikkerheten er god i Norge (Ivar, fagansatt).

Noen av informantene forklarer at det er en tendens i bransjen at alle sitter på hver sin tue og utvikler de samme løsningene for å kunne tjene penger på det de lager. Kraftselskapene lager noe, bransjen utvikler ting selv og underleverandørene utvikler ting. Dette kan være med å bremse utviklingen, fordi de optimale løsningene finnes når disse aktørene går sammen om å løse problemer og utfordringer.

Oppsummering av eksterne samarbeid

Det finnes etablerte samarbeidskanaler i bransjen og det finnes noen uformelle kanaler som baserer seg på et personavhengig samarbeid. En utfordring fremstår på enkelte informanter å ligge i den konkurransen som er mellom virksomhetene. Det fører til at virksomhetene selv utvikler løsninger uten å samarbeide seg frem til den beste løsningen som øker den totale digitale sikkerheten i kraftsektoren. Kraftcert trekkes frem som et eksempel på et positivt eksternt samarbeid alle i bransjen deler. Dette virker å gi trygghet på deling og opplæring rundt digital sikkerhet.

4.2.3.2 Interne samarbeid

Flere av informantene forteller at virksomheten har ulike fagmiljøer internt. På den ene siden har man markedsavdelingen som selger strøm, og på den andre siden har man driften og

produksjonen av selve strømmen som er en kritisk infrastruktur med høy grad av sikkerhet. Informantene belyser dette med å beskrive friksjonen som ligger i det interne samarbeidet.

> Jeg er veldig opptatt av friksjon. Det er friksjon mellom avdelinger hos oss. Mellom de som driver med sikkerhetsarbeid og de som driver med marked. Det er friksjonen som driver oss fremover. Jeg tenker det egentlig ikke handler om sikkerhetskultur. Det handler like mye om arbeidsprosesser. Du har en veldig rask prosess og en veldig sakte prosess. Her ligger det mye friksjon. Her er det viktig å anerkjenne egenskapene og kompetansen i begge miljøer, og etablere gode prosesser for samhandling og involvering (Josefine, leder).

Stian (L) forteller om et mindre bra samarbeid, der IT i hovedsak kommer inn for sent i prosjektene til markedsavdelingene og dermed ender opp med å måtte rydde opp etter dem. Han ser en utvikling i fokuset marked har på hvilken rolle IT spiller i dette arbeidet. Han mener det er de fagansatte på digital sikkerhet som løfter markedssiden og ikke omvendt. Hastigheten i arbeidet til marked blir for høy, noe som igjen gjør at IT-folkene føler seg som bremseklosser i selskapene. Det beskrives en god utvikling på dette området av flere informanter. Nå tar marked i større grad kontakt med IT før de iverksetter nye prosjekter.

Noen informanter peker på samarbeidsutfordringer som dårlig kommunikasjon og stammespråk. For å løse dette kreves det grupper med riktig kompetanse. Bruken av forkortelser fra IT-verden var noe flere trakk frem som negativt for det interne samarbeidet. Brukes det mange forkortelser faller de ansatte fort av. Det igjen utviklet holdninger som gjorde at ansatte ikke stolte på hverandre og problemløsningen stoppet helt opp i flere tilfeller. Tillit til hverandre gjennom godt samarbeid er nøkkelen. Videre ble opprettelsen av en egne samarbeidsgrupper i virksomhetene trukket frem som gode forum for problemløsning. Der flere eksperter på ulike fagområder sitter sammen med en leder som har en bred forståelse og kan sette gode rammer for videre samarbeid.

Ivar (F) setter søkelyset på at den fysiske sikkerheten representert ved beredskapskoordinatorer snakker godt sammen med den digitale sikkerheten, representert ved CISO-rollen. I dette samspillet blir det tydelig hvordan den digitale verden virker på den fysiske verden. Beredskapskoordinatoren kan si hvor det er viktig med sikring, mens CISO kan si hvordan dette best mulig kan sikres digitalt. På denne måten kan man få sikre og brukervennlige løsninger som gir mening for de ansatte ved virksomheten.

Oppsummering interne samarbeid

Flere informanter er enige om at samarbeidet internt må bedres for å øke den total digitale sikkerheten i selskapet. Det er flere av informantene som mener IT-siden ofte kommer sent inn i prosjektene til markedssiden, mens andre mener samarbeidet preges av IT-stammespråk og dermed hemmer samarbeidet. Totalt sett er mange enige om at samarbeidet er greit, men at flere tiltak kan bidra til bedre effektivitet og økt sikkerhet.

4.2.4 Tilsyn i bransjen

Flere informanter tok opp tilsynet som NVE utfører mot virksomhetene, og noen fortalte at forholdet mellom forventingene NVE setter til innføringer av nye retningslinjer og krav ofte ikke står i stil med deres egen kompetanse på området. Noen pekte på manglende ressurser hos NVE og presiseringer om hva de nye tiltakene innebærer og hvordan de bør utføres.

> Jeg hadde ønsket meg flere stedlige tilsyn. At de faktisk kommer ut og kan borre litt mer i dybden. Det hadde også vært bedre hvis de selv kunne svare ut problemstillinger som vi sitter å tolker selv (Torgeir, fagansatt).

Espen (L) omtalte NVE som dårlig rigget på digital sikkerhet. Han forteller at det har blitt innført et eget avsnitt i kraftberedskapsforskriften om digital sikkerhet, men at det preges av å være skrevet fra et kontor. Enkelte informanter sier NVE ikke vil svare på spørsmål for å ikke sitte på ansvaret selv hvis ting ikke går etter planen. Kraftcert og NSM trekkes frem av noen som avgjørende for at selskapene skal kunne tolke føringene fra NVE. Gjennom å bruke grunnprinsippene for IKT-sikkerhet gitt av NSM, samt rådføring med Kraftcert, føler flere av informantene at de klarer i stor grad å tolke riktig de føringene som blir innført i bransjen.

Amanda (F) kom med synspunkter på hva føringene fra NVE gjør med de mindre kraftvirksomhetene. Det var gjennomgående fra informantene at NVE stiller de samme kravene uavhengig hvilken størrelse virksomhetene har. Dette medfører et stort behov for riktig kompetanse og prioriteringer rundt hva som er viktigste å gjøre først. Hun opplever at siden sikkerhetsmiljøet i selskapet er sterkt så klarer man ofte å forutse hvilke føringer som kommer, men det fører til at andre områder på digital sikkerhets må settes på vent. Dette kan for eksempel være øvelser og trening for de ansatte.

> Når vi får mange føringer fra NVE angående digitale forbedringer må vi prioritere dette og flytte mannskap over for å løse de mest prekære oppgavene. Dette resulterer

> i at det er andre områder som må vente på IKT siden. Dette er uheldig. (Amanda, fagansatt).

Tilbakemeldingene var derimot ikke utelukkende negative, og noen trakk frem positive sider med tilsynet som NVE utfører. En informant forteller at etter at NVE fikk kritikk av Riksrevisjonen for ett par år siden, har NVE satset mer på digital sikkerhet. Flere informanter opplever hyppigere tilsyn og revisjoner, noe som fører til økt bevissthet hos ledelsen og mer ressurser til arbeidet. Videre har NVE blitt flinkere til å gjennomføre høringer der de mottar innspill fra bransjen før de fatter endelige vedtak som må innføres hos selskapene.

> Revisjon kan enten gjennomføres som spørreundersøkelser eller fysiske besøk. Da varsles det på forhånd hvilke temaer som vil bli tatt opp. Dette er det nærmeste man kommer et direkte kontrollorgan i bransjen. Bransjen er ikke underlagt sikkerhetsloven. Jeg tror det vil bli tatt en ny vurdering av hvilken lov vi skal ligge under. Uten strøm vil andre grunnleggende tjenester falle bort i samfunnet (Petter, fagansatt)

Oppsummering av tilsyn i bransjen

Flere trekker frem tolkning av vedtak fra NVE som et stort arbeid som løses internt og i samarbeid med samarbeidspartnere. De opplever at NVE i liten grad kan svare ut de vedtakene som innføres i kraftsektoren. Kravene som settes er like for alle selskapene, noe som føre til tøffe prioritering i de mindre selskapene. Dette kan igjen føre til at det totale arbeidet med digital sikkerhet blir ulikt etter hvilke vedtak som fattes av tilsynsorganene.

4.3 Barrierer

4.3.1 Forebyggende arbeid av uønskede digitale hendelser

Flere informanter forteller at det å være godt rustet til å håndtere uønskede hendelser som oppstår i virksomheten er viktig for den digitale sikkerheten. Nils (F) forklarer viktigheten av å ha det organisatoriske på plass og gjøre nivåsetting når de forholder seg til uønskede digitale hendelser ved sin virksomhet.

> Ved en digital hendelse håndterer IT denne hendelsen først lokalt, og nivåsetter denne i forhold til hva som kreves av kompetanse og ressurser for å håndtere hendelsen. Hvis omfanget er av en viss størrelse og kritikalitet vil det bli satt beredskap. Da setter man en strategisk organisasjon som allokerer inn personell som kan bidra til å løse hendelsen. Det kan også settes med en operativ leder som

> håndterer hendelsen. Jeg får også varsler fra IT der de rådfører seg med meg og beredskapsorganisator for å finne riktig nivåsetting, om det holder med vanlig linjeaktivitet eller om man må sette noen form for ekstra beredskap (Nils, fagansatt).

Josefine (L) forteller at måten de håndterer uønskede hendelser er avgjørende for den digitale sikkerheten, og sier følgende om sin rolle som leder oppi dette.

> Hvordan vi håndterer uønskede hendelser er helt avgjørende for å ha en god digital sikkerhet. Som leder er jeg da helt bakerst i rekken. Når det kommer til stridsledelse er jeg som leder ikke verdt noe som helst. Det jeg som leder må gjøre er å sørge for at teamet som skal håndtere dette er trent og har de rammevilkårene som trengs for å løse utfordringene når det inntreffer. Det handler om teknisk kompetanse, men det handler veldig mye om tillit og trygghet til hverandre. Det er viktig at folk kjenner sine ansvarsområder og beslutningsmyndighet. På den måten kan de operere fritt og ta viktige selvstendige avgjørelser. Jeg som leder er klar på at jeg står bak dem (Josefine, leder)

Forebyggende tiltak som bevisstgjøring og opplæring av ansatte i virksomheten er noe som flere informanter trekker frem som viktig for å forebygge at uønskede hendelser inntreffer. For Ivar (F) er arbeidet med den menneskelige faktoren viktig i det forebyggende arbeidet, for å gjøre de ansatte i stand til å ta egne sikre digitale valg og inneha en god risikoforståelse. Skapes det ansatte som er kritiske til digital opptreden og informasjonssikkerhet settes virksomhetene i stand til å oppdage uønskede hendelser før de inntreffer.

Espen (L) viser til en konkret utfordring når det gjelder opplæring og bevissthet rundt digital sikkerhet, nemlig det med hvordan man kommuniserer risiko.

> Historien som blir fortalt til de ansatte og lederne viktig. Det å fortelle en historie for å øke bevisstheten må være gjennomtenkt. Hvis historien som fortelles er at vi hele tiden er under digitale angrep, må det vises til konkrete eksempler. Det er farlig å stå å si noe som ingen ser eller føler på. Skal de ansatte ha troverdighet og tillit til denne historien burde det vises ofte til konkrete hendelser, gjerne fra egen virksomhet (Espen, leder).

Petter (F) presiserer at tekniske sikkerhetsløsninger alene ikke er nok til å si hvor god digital sikkerhet du har, og at man må ha med seg flere andre faktorer. Han mener digital

sikkerhet og forsikring kan sammenlignes. Uansett hvor mye penger man bruker på ulike sikkerhetsløsninger, vil man aldri med total sikkerhet sikre seg mot angrep eller uønskede hendelser. Man er avhengig av å se de forebyggende tiltakene i sammenheng. Her trekker han frem organisering, varslingssystemer og rutiner for håndtering av hendelser. Som en del av de tre burde man ha fokus på opplæring for å opprettholde løsninger man har implementert. Som Nils (F) sier, så hjelper det lite med gode brannmurer hvis brukeren av de tekniske systemene gir fra seg brukernavn og passord. Det å ha en god balanse mellom den tekniske sikkerheten og den organisatoriske med de ansatte er avgjørende for å forhindre hendelser, sier Nils (F).

Når det kommer til hvor mye fokus det å drive med forebygging av uønskede hendelser får i virksomheten, var det noe delte svar fra informantene. To av de fagansatte informantene etterlyser flere ressurser og mer tid til dette. Det oppleves som at det forbyggende arbeidet kommer i andre rekke og at man i det store bildet ender opp med brannslukking av hendelser som oppstår, sier Amanda (F). Hun ser viktigheten av trening og opplæring, og ønsker mer ressurser og tid satt av til dette. Hvis virksomheten ikke har opplæring satt i system, sier flere av informantene at det ofte koker litt bort og man ender opp med å bruke ressurser på ting andre ting.

Det å ha en dårlig bevissthet rundt digital sikkerhet kan ha noe med at opplæringen ikke er presis nok, og Petter (F) mener at det burde vært mer skreddersydde opplæringsløsninger:

> De løsningene som brukes i opplæring er nok litt for lavterskel. Jeg kunne ønsket meg mer skreddersydde løsninger, der de som deltar blir ratet etter hva de svarer. På den måten for man et innhold som treffer den enkelte bedre. De flinke får bedre tilpasset innhold, mens de svake ville fått et enklere opplegg (Petter, fagansatt).

Nils (F) forteller at det handler om å skape en god sikkerhetskultur i virksomheten, hvor alle ansatte er opptatt av digital sikkerhet. Han snakker om det å skape «security champions», hvor det handler om å skape en interesse hos de ansatte, og få dem til å ville lære selv.

> Vi må sikte oss inn på å skaffe personell som kan gjennomføre opplæring i virksomheten. Det å komme med pekefingeren er ikke løsningen. Man må skape en interesse hos de ansatte. De må ville lære det selv. Får man folk til å hjelpe hverandre har man kommet langt. Vi ønsker å selge sikkerhet med et smil. Jeg tror nok finanssektoren har kommet langt her og vi har mye å lære av dem. Vi har også samme ambisjoner, men da må vi starte arbeidet med å sette ting i system og få det inn i alle prosesser vi gjør. Man må skape det man kaller security champions. Når

> nye kommer inn skal de føle en kultur som er stolt av det digitale arbeidet de gjør (Nils, fagansatt).

Petter (F) ønsker seg et mer formelt løp innenfor digital sikkerhet, og sammenligner det med de formaliserte kravene som er i virksomheten rundt arbeid med høyspent. Stian (L) ser også på de formaliserte kravene som finnes i kraftbransjen i dag, og ønsker seg et pålagt sikkerhetskurs årlig for ansatte. Han har ett ønske om at ledelsen tar ansvar og beslutter at slike kurs er implementert i virksomheten.

> Akkurat som at du ikke får gå inn i en kraftstasjon, hvis du ikke har bestått det pålagte kurset. På samme måte burde digitale kurs være basert på å få en godkjent poengsum som kvalifiserer den ansatte til bruk av systemene. Det trenger ikke å være spesielt innviklet, men at det kommer årlig er viktig, og at man faktisk må levere et resultat (Stian, leder).

Oppsummering av forebyggende arbeid

Det å være godt rustet til å håndtere uønskede hendelser fremstår som viktig for den digitale sikkerheten i virksomhetene. Her viser flere informanter til at det er viktig å ha det organisatoriske på plass, og gjøre riktig nivåsetting av hendelser. Tekniske løsninger er en viktig barriere for å forhindre digitale angrep, men flere informanter forteller at dette er ikke avgjørende. Man må inkludere det organisatoriske og menneskene. Her kommer forebyggende tiltak som opplæring og bevisstgjøring inn, noe som de fleste informantene trekker frem som viktig arbeid for å øke kunnskapen og holdningene til digital sikkerhet. Det er delte meninger om hvor stort fokus dette får i virksomheten. Noen informanter ønsker mer ressurser og tid på dette, mens andre fremhever viktigheten av at opplæring er satt i system. Noen ønsket seg skreddersydde opplæringsløsninger som treffer den enkelte bedre, mens andre ønsket seg et mer formelt opplæringsløp innenfor digital sikkerhet.

4.3.2 Spesifikke tiltak for forebygging

Flere informanter forteller om spesifikke opplæringstiltak de gjør i virksomhetene for å drive øke bevisstheten og kunnskapen til de ansatte på digital sikkerhet. I det følgende vil presentere det som informantene pratet mest om, herunder phising-tester, workspace, e-læring og øvelser.

4.3.2.1 Phising-tester

Det å gjennomføre phising-tester på de ansatte er noe de fleste informantene sier blir

gjort regelmessig i virksomheten, og det fortelles om en positiv effekt når det gjelder å øke bevisstheten hos de ansatte.

> Vi har hatt en rekke phising-tester i virksomheten som har gått på dette med epost. De fleste sjekker ikke hvem adressanten er. Mange i selskapet hadde stort utbytte av de phising-testene som ble kjørt på de ansatte. Det var en vesentlig forbedring etter testene var gjennomført. Det som blir et resultat av disse testene er at den totale bevisstheten øker, også ute i kraftverkene. Det er ikke artig å få en lang nesemail fra IT om at du har bommet. Dette treffer etter min mening fagarbeidernivået og er et effektivt tiltak for å løfte bevisstheten til de ansatte. Dette trenger vi alle mer av for å være på tå og hev (Espen, leder).

Nils (F) snakker om «learning by burning, og forteller at phising tester på de ansatte, har ført til økt årvåkenhet og rapportering av hendelser ti IT.

> Jeg tror de eldre er mer umodne på digitale løsninger. Det er vanskelig å få dem til å forstå hva de skal trykke på eller ikke. Da vi gjennomførte den første phising-testen ble det en snakkis under lunsjen. Det gjorde utslag ved at vi så antall henvendelser til IT økte betraktelig ved test 2 og 3. Det er learning by burning. Du kan løfte det opp til et minimum nivå (Nils, fagansatt)

Ivar (F) forteller om viktigheten av å være bevist hvordan man svarer de ansatte som blir lurt i en phising-test. Han vil ikke at det skal bli opplevd som et mas fra IT, og mener også at man må ha noe mer i tillegg til disse testene.

> Etter at vi har hatt phising tester, så sier de ansatte at dette var flaut at man ble lurt. Det er viktig å være bevist på hvordan du svarer de som henvender seg til deg. Man kommer ikke bort fra at man blir flau, men vi må gjøre det vi kan og si at det er menneskelig, du er ikke eneste, da kan du bli bedre neste gang. Phising-tester har kommet for å bli. Det kommer vi til å gjøre regelmessig i uoverskuelig framtid, men det må komme noe i tillegg. Ellers vil gevinsten av dette falle bort etter hvert. Da vil det bli det maset fra IT igjen. Du må forstå hvorfor vi gjør det, og det er vi må jobbe med (Ivar, fagansatt)

I Torgeir (F) virksomhet følger de opp phising-testene ved å overføre de ansatte som lar seg lure til ett påfølgende e-læringsprogram.

4.3.2.2 Workspace

Det var flere informanter som fortalte at informasjon omkring digital sikkerhet blir lagt ut på selskapets eget intranett, såkalt workspace. Her legges det ut aktuelle artikler, hva man skal være ekstra varsom på, og ulike digitale hendelser og scenarioer som har skjedd.

> Nå skal det sies at det er kjørt en del kampanjer, noe vi kaller for workplace, som er arbeidsplassen sin Facebook. Der har man lagt ut en del artikler om IT-sikkerhet og om ulike scenarioer som eposter med ondsinnede koder, og prøvd å informere dem om at hvis de oppdager noe muffins, så skal de kontakte oss på IT-sikkerhet. Jeg opplever at folk har tatt innover seg dette, og vi har fått en del meldinger fra sluttbrukere som da identifiserer noe som de mener er verdt å melde fra om, også har vi tatt tak i det umiddelbart. Der er vi flinke, når vi får saker, så reagerer vi så raskt som mulig (Stian, leder).

Flere informanter forteller utfordringen med bruk av workplace er at man ikke vet om alle ansatte ved virksomheten får det med seg. Man er avhengig av at den ansatte går inn selv og leser det som står der

> «Du kan si at det å legge ut på workplace er veldig bra og veldig mange følger med der, men jeg er ikke så sikker på om alle får det med seg. Mekanikeren langt vekke, jeg vet ikke om sitter å følger med i workspace så ofte. Så mitt innspill til ciso er, slik som man har førstehjelpskurs en gang i året, burde man hatt en slags portal hvor man måtte gå gjennom et par spørsmål eller et digitalt kurs. Kanskje det burde vært et krav. I Forsvaret har man det, der må man minimum en gang i året gå gjennom ulike spørsmål. Det ville virkelig øke bevisstgjøringen vår» (Stian)

4.3.2.3 E-læring:

De fleste informantene forteller at e-læring er noe som blir gjennomført i virksomheten. Det beskrives som enkelt å forholde seg til og at man får kjøpt ferdiglagde pakker med opplæringsinnhold. Petter (F) forteller at de i sin virksomhet ukentlig sender ut små informasjonskampanjer med ulike temaer innenfor digital sikkerhet per epost til ansatte. Dette er tjenester de kjøper fra et norsk selskap som driver med akkurat slike tilpassende digitale opplæringsopplegg.

E-læring er også noe Bjørn (F) kjøper inn og sender ut til ansatte i virksomheten. Han forteller at det er bedre at de ansatte får smådrypp hele tiden, enn at man sender en uinteressert ansatt på kurs.

> Jeg vet hva som skal til. Det er kompetanse og endringer av holdninger, og en dypere forståelse av det du driver med. Vi prøver å kjøre nano-learnings program der hvor vi kjøper inn fra noen som kan pedagogikk, som har satt opp noen sett med slides som du kan gå igjennom i løpet av 2-5 minutter. Sånn nano-learning eller mikro-learning hvor man får smådrypp hele tiden, tror jeg har mer for seg, enn å sende en person som er totalt uinteressert på et to ukers kurs. Det er repetisjon. Hvis du repeterer en ting en gang i året, så har du åtte ganger større retensjon på kompetansen enn om du bare hører det en gang. (Bjørn, fagansatt)

Nils (F) forteller at de i sin virksomhet lager nanolæringer med ulike temaer selv, og etterlyser gode evalueringer og en felles e-læringsplattform. Han ønsker mer egne forum som driver med utvikling av slike e-læringsopplegg og en diskusjon rundt hva som gir best effekt på de ulike typer ansatte som finnes. Han påpeker også at det å lage egne opplæringer er en fordel fordi man kjenner sin egne ansatte godt og dermed lettere kan treffe dem som har størst behov for påfyll av digital kompetanse.

4.3.2.4 Øvelser

Når det kommer til øvelser i virksomheten forteller flere informanter at det gjennomføres øvelser i virksomheten med digital sikkerhet som fokus. Stian (L) forteller om interne øvelser på sin IT-avdeling, samt at de gjennomfører øvelser ut til forretningen, noe han ser stort læringsutbytte av.

> I forhold til øvelser, gjennomfører vi en kombinasjon av kryptoskadevare og disaster-recovery øvelser. Vi har noen interne øvelser, der vi simulerer at alt er nede, også handler det om å bygge det opp igjen. Vi har også øvelser med forretningen, og de er kanskje de morsomste, fordi da får vi som lager øvelsene sette dem litt på plass. For forretningsområdene er dette veldig god læring, fordi da skjønner de for eksempel at de burde ha hatt noen pcer i reserve som hadde 4G-kort (Stian, leder).

Ivar (F) forteller at det gjennomføres større øvelser noen ganger i løpet av året, men at han ser mer effekt av mindre øvelser med færre involverte.

> Vi hadde en stor øvelse i 2021, også har vi 2022 hatt et par øvelser på de som sitter på driftssentralen, altså de som styrer kraftverkene. Det jeg ønsker er at vi skal ha mindre øvelser. Hvis du skal øve hele IT-avdelingen, så krever det enormt mye. Men med mindre øvelser kan vi for eksempel trene de tre som jobber med nettverk. Da kan jeg gå å nappe kabelen. Det vil kreve mindre. Så det jeg ønsker å få til er å holde

øvelsene enklere, mindre, kortere og mer kompakte, i stedet for en svær, tung øvelse en gang i året. Vi må trene hele organisasjonen, men du kan få veldig god effekt av å gjøre det litt mindre, litt kortere, og ikke involvere så mange (Ivar, fagansatt).

5 Analyse

Problemstillingen for denne studien er: *Hva kjennetegner norske kraftvirksomheter sitt arbeid med digital sikkerhetskultur, sett fra fagansatte og ledelsen sitt perspektiv?*

Gjennom problemstillingen og de tilknyttede forskningsspørsmålene, har vi fått et omfattende empirisk grunnlag om risikoforståelse, holdninger, ledelse, læring og forebyggende tiltak. Vi vil nå gjennomføre en grundig drøfting av funnene gjort i empiridelen, opp mot relevant teori innenfor begrepet digital sikkerhetskultur og besvare forskningsspørsmålene våre mer direkte. Gjennom kapittel 4 har vi oppsummert de empiriske funnene knyttet til de tre hovedkategoriene «digital sikkerhet», «digital sikkerhetskultur» og «barrierer». I all hovedsak har empiridelen belyst menneskelige og organisatoriske faktorer som påvirker arbeidet med digital sikkerhetskultur i kraftsektoren. Tabellen under viser koblingene mellom forskningsspørsmålene og våre empiriske funn.

Forskningsspørsmål	**Empiriske hovedfunn**
Hvilken digital risiko opplever kraftselskapene at de står overfor?	• Forskjellig begrepsbruk skaper utfordringer mellom avdelinger i selskapene. • Mangel på kunnskaper om digital sikkerhet hos de ansatte. Ulike miljøer internt i selskapene har ulike risikooppfattelse. Flere ansatte har et naivt syn på engen rolle i det digitale sikkerhetsarbeidet. • Stort antall spam-mail blir stoppet hver dag. Flere tilfeller av tilpassede profesjonelle angrep på enkeltindivider i selskapene.
Hvordan påvirker de ansattes holdninger til digital sikkerhet arbeidet med digital sikkerhetskultur?	• Ulike miljøer innad i selskapene har ulikt fokus. Stort spenn hos de ansatte i erfaring og kunnskaper rundt digitaliseringen som foregår i selskapene. • Stort fokus på at den menneskelige faktoren spiller en avgjørende rolle i arbeidet med sikkerhetskultur. • Holdningene er generelt gode, men store ulikheter rundt digital kompetanse.
Hvilken rolle spiller ledelsen i arbeidet med digital sikkerhetskultur?	• Ledelsen har fått et større fokus på digital sikkerhet og risikoforståelsen til ledelsen er bedret gjennom økt fokus. • Ulikheter i fokuset ledelsen har i de ulike selskapene. Større fokus på innovasjon enn sikkerhet. • Lederne spiller en avgjørende rolle ved å forankre det digitale arbeidet og setter i større grad tydelig mål for alle ansatte i selskapet.

Hvilke faktorer spiller inn ved ivaretakelse av varsling og læring?	• Usikkerhet rundt hva som kan deles av informasjon, hindrer samarbeid og utvikling i bransjen. • Ledelsen har stort fokus på å gi riktige rammebetingelser for varsling. • Mange ulike opplæringsprogram i bransjen. Flere jobber med egne ting og dermed lite samarbeid.
Hvilke utfordringer opplever selskapene i møte med brukeren?	• Stort fokus på fysisk sikkerhet i kraftbransjen. • Store geografiske avstander og mange ulike kulturer. • Høyt tempo i innovasjonsarbeidet bidrar til svekkes fokus på digital sikkerhet.
Hvilke forebyggende tiltak benyttes for å styrke den digitale sikkerhetskulturen?	• Oppleves som vanskelig å nå frem til alle brukerne på riktig nivå pga ulike kulturer innad i selskapene. • Selskapene utvikler mye opplæring selv og kjøper inn enkelte tester. Stor bruk av phising-tester i samtlige selskap. • Myke tiltak som organisering av det digitale arbeidet er løftet gjennom CISO rollen.

Tabell 5.1 Viser kobling mellom forskningsspørsmålene og empiriske funn gjort i intervjuene.

I kapittel 2 presenterte vi teorigrunnlaget i oppgaven, noe som danner grunnlaget for videre drøftingen i analysen. Vi vil også trekke inn nyere nasjonal og internasjonal forskning for å øke forståelsen av de tema vi drøfter. Problemstilling omhandler kjennetegn ved digital sikkerhetskultur og derfor velger vi å innlemme «digital sikkerhet» i hovedkategoriene «digital sikkerhetskultur» og «barrierer». Dette gir en hensiktsmessig og helhetlig fremstilling i vår analyse, da mange faktorer omhandler det samme temaet og påvirker hverandre.

De viktigste funnene i studien dreier seg om bevissthet, holdninger og risikoforståelse rundt digital sikkerhet, ledelsens påvirkningskraft på det digitale sikkerhetskulturarbeidet, varsling og læring, samt hvilke forebyggende tiltak selskapene har for å påvirke de ansattes bevissthet og risikoforståelse tilknyttet digital sikkerhet. Vi vil deretter ta for oss de to hovedområdene «digital sikkerhetskultur» og «barrierer», og drøfte og analysere disse inngående opp mot det teoretiske rammeverket presentert i kapittel 2.

Vi vil starte med hovedkategori «digital sikkerhetskultur». Her vil vi i all hovedsak drøfte og analysere hvordan kraftsektoren kjennetegnes opp mot vårt teoretiske rammeverk på området. Vi har valgt å presentere analysen i tre underkategorier. Disse er «bevissthet», «ledelsens rolle i arbeid med sikkerhetskulturarbeidet» og «varsling og læring». Under «bevissthet» drøfter vi empiriske funn rundt risikoforståelse og holdninger. Under den andre underkategorien ønsker vi å vise hvordan ledelsen påvirker arbeidet med sikkerhetskultur og

hva som her kjennetegner kraftsektoren. Den tredje kategorien tar for seg varslingsmetoder og læring, med et særlig fokus på Reason (1997) sin teori om informerende kultur. Etter dette vil vi ta for oss hovedkategori to som er «barrierer». Her ønsker vi å analysere hvilke organisatoriske og menneskelige forhold som finnes, samt forebyggende tiltak som virksomhetene benytter seg av i påvirkning av de ansattes bevissthet rundt digital sikkerhet.

5.1 Digital sikkerhetskultur

Etter en gjennomgang av empiriske funn i kategorien digital sikkerhet satt vi igjen med to hovedkategorier som utmerket seg i dybde og omfang. Inne i hovedkategori «bevissthet» har vi tatt for oss sikker adferd med kunnskap og kompetanse, risikoforståelse og holdninger som viktige faktorer i sikkerhetskulturarbeidet. Under hovedkategori «ledelsens påvirkning» har vi drøftet varsling og læring, rollemodeller og forpliktelser opp mot digitalt sikkerhetsarbeid.

Figur 5.2 En overordnet modell for digital sikkerhetskultur basert på våre empiriske hovedfunn og kjent teori om digital sikkerhetskultur.

I analysen og drøftingen under vil vi presentere ulike kategorier som inneholder punkter fra modellen over. Noen av kategoriene er delt opp for å gjøre det mer oversiktlig og leservennlig. Noe av innholdet drøftes mer inngående enn andre fordi informantene nevnte visse kategorier oftere enn andre. Etter hver kategori vil vi oppsummere hva som kjennetegner funnene opp mot teorien på området. Overskriftene under blir som følger:

- **Bevissthet** - Risikoforståelse, Kompetanse og holdninger
- **Ledelse** – Forankring av digital sikkerhetsarbeid i ledelsen- ledelsen som rollemodeller – Organisering og målsetninger fra ledelsen
- **Varsling og læring** – Rapporterende kultur og fleksibel kultur

5.1.1 Bevissthet

Gjennom intervjuene ble det tydelig at informantene nevnte bevissthet rundt digital sikkerhet og sårbarheter i mange ulike sammenhenger. I empiridelen av oppgaven knyttes bevissthet til kompetanse, forståelse av digital sikkerhet og kunnskap. I denne delen av oppgaven vil vi knytte bevissthet til risiko. Vi vil drøfte empiriske funn opp mot kjente beredskapsteoriers fokus på bevissthet. På bakgrunn av informasjon fra informantene og påfølgende analyser vurderes det at bevisstheten til enkeltindivider (ansatte) og virksomhetene som et kollektiv er avgjørende for en god håndtering av trusler og sårbarheter.

5.1.1.1 Risikoforståelse- Et samspill av flere faktorer

Virksomhetens risikoforståelse baseres på hvordan enkeltindividene oppfatter risikoen sammen med kollektivet i virksomheten. Risikoforståelsen påvirkes av mange ulike forhold, eksempelvis verdier, holdninger, erfaringer, tilgang på informasjon og sårbarheter. Mennesker opplever risiko ulikt, og dermed blir risikoforståelsen farget av øynene som ser og enkeltindividets oppfattelse av risikoen. Dette gjør risikoforståelse til noe subjektivt og dermed kan ikke risikoforståelse bare ses på med et realistisk kunnskapssyn (Engen et al., 2021, s. 92-95; Aven et al., 2019, s. 37-39). En god risikoforståelse er en avgjørende faktor i sikkerhetsarbeidet. Som nevnt over er ikke risikoforståelse bare kalkulasjon av fakta - det har også mange svært subjektive faktorer. Et eksempel på slike subjektive faktorer er omhandlet i en studie av Parson med flere (2010) der man så at risikoforståelse hos enkeltindivider har stor betydning for adferdsmønstre. Studien pekte på at enkelte har en urealistisk optimisme i møte med risiko. Mange mente at det de gjør på egen datamaskin er under deres kontroll og at digitale trusler derfor fremstår som mindre alvorlige (Parson, McCormac, Butavicius & Ferguson, 2010, sitert i Bergsjø et al., 2020, s. 39-40).

Informantene beskriver at man har et vidt spenn av ulike typer mennesker i virksomhetene. For mange er det digital rom litt nytt og ukjent. Dette påvirker hvordan de ansatte oppfatter risikoen ute på anleggende versus hvordan de som jobber administrativt opplever digital risiko. De ansattes risikoforståelse er ulik fordi de har ulike arbeidsoppgaver, erfaring og kunnskap om digital sikkerhet. De fagansatte på digital sikkerhet jobber aktivt med å spre denne kunnskapen om digital risiko for å bedre risikoforståelsen til de ansatte ute i virksomhetene. Det beskrives også en dreining i kraftsektorens sikkerhetsfokus de siste årene, fra et sterkt fokus på fysisk sikkerhet til mer mot digital sikkerhet. Informantene forteller om en god fysisk beredskapskultur som er vant til å forholde seg til sikkerhetsrisiko og ikke den digitale risikoen. Dette er noe som ligger i ryggraden til de fagansatte og ansatte som har jobbet lenge i bransjen. Denne historikken med fysisk sikkerhet kan føre til en urealistisk optimisme rundt den digitale risikoen som virksomhetene utsettes for. Hvilken betydning den enkelte har for selskapets digitale sikkerhet trekkes også frem av flertallet av informantene som en utfordring. Det å få de ansatte til å forstå at OT henger sammen med IT er helt avgjørende for å opprettholde god sikkerhet forklarer flere av informantene. I en studie om cyberrisiko av Larsen og Soldal (2021) kommer det frem at risiko oppleves veldig subjektivt (Larsen & Soldal, 2021). Vi velger å benytte oss av to funn i studie til Larsen og Soldal (2021) for å beskrive digital risikoforståelse, herunder «umiddelbarhet av risikokonsekvenser» og «kunnskap om risiko». Det første funnet i studien viser at jo større umiddelbarhet en person har til en cybertrussel, jo større er den opplevde risikoen. Dette underbygges av tidligere arbeid på feltet som indikerer at opplevd risiko reduseres når negative konsekvenser sannsynligvis vil være forsinket. Den andre funnet omhandler kunnskapen den enkelte ansatte har om cybertrusler. Den forteller oss at mennesker opplever risikoen som større ved begrenset kunnskap, for eksempel om digitale trusler, og mindre når de innehar mer kompetanse om teamet. (Larsen & Soldal, 2021). En av informantene forteller at de ansatte kan få en feiloppfatning av digital risiko når historien som blir fortalt på dette området ikke treffer de ansatte gjennom å bruke lokale forhold. Flertallet av informantene forteller om at de ansatte ikke innser den reelle risikoen når de ikke er kjent med hvilke digitale trusler de står ovenfor.

Risikoforståelsen har blitt løftet gjennom at NVE har satt et større fokus på digital sikkerhet, og fortalt bransjen at et angrep mest sannsynlig vil forekomme i form av et hybrid angrep. Hybride angrep vil kunne ramme fysiske installasjoner og teknologiske løsninger hos virksomhetene. Turner (1978) hevdet at risikovurderinger kan være problematiske fordi risiko

blir tolket og oppfattet ulikt av ulike interessenter. Turner sin teori vektlegger at synet organisasjonene har på hvordan ulykker inntreffer, spiller en stor rolle for om man tolker risikoen man står ovenfor på en hensiktsmessig måte (Turner, 1978). Gjennom informantene fremstår det som virksomhetene baserer sine risikovurderinger på reelle trusler og sårbarheter, gjennom å bruke PSTs, NSMs og egne risikovurderinger i virksomheten. Utfordringen som mange informanter påpeker, er å bedre risikoforståelsen til de ulike ansatte og vise med konkrete eksempler hvilken risiko de faktisk står ovenfor, og hvordan den enkelte er med å påvirke det digitale sikkerhetsarbeidet.

Informantene i denne oppgaven jobber i all hovedsak med digital sikkerhet og er dermed farget av at de innehar mer kompetanse og interesse for tematikken sammenliknet med andre ansatte i virksomheten. Det er samsvar mellom hva informantene vektlegger rundt bevissthet og risikoforståelse, og hva teorien sier på området. En utfordring er knyttet til stor variasjon i fagmiljøer. Dette kan medføre at risikoforståelsen hos den enkelte blir ulik og at den ikke står i forhold til de faktiske truslene som virksomhetene står ovenfor. Siden risikoforståelsen er subjektiv, kreves det at alle treffes av den «riktige kunnskapen» i de samme kanalene. Dette vil kunne løfte enkeltindividenes risikoforståelse og dermed virksomhetenes kollektive risikoforståelse.

5.1.1.2 Bevissthet – Digital sikkerhetskompetanse

Kompetanse, læring og risikoforståelse er tett knyttet sammen. For å kunne mene noe om digital risiko kreves det at de ansatte har noen kunnskaper om teamet digital sikkerhet. Dette kan være ondsinnede vedlegg eller e-poster som samtlige av informantene trekke frem som hyppige digitale angrep mot virksomheten. Det at de ansatte har kunnskaper om at de selv er mulige innganger til virksomhetenes datasystemer er viktig for å forstå risikoen de står ovenfor. De bør også inneha kunnskaper om hvor ofte det skjer og hva som kjennetegner en utrygg e-post for å kunne gjøre riktige vurderinger (Bergsjø et al., 2020, s. 39).

Informantenes oppfattelse av hvilke digitale trusler og sårbarheter kraftvirksomhetene står ovenfor, er i all hovedsak ganske lik. Alle var innforstått med at de har en samfunnskritisk rolle ved at de produserer strøm som samfunnet er avhengig av for å fungere. De anerkjente også at store statlige aktører har kapasitet til å ramme virksomhetene digitalt og at virksomhetene da er et yndet mål. På den andre siden vurderte de angrep på e-post, som rammer enkeltindivider, som den største angrepsvektoren. Derfor ble fokuset på menneskelige faktorer vektlagt høyt av samtlige informanter.

Forståelse og kunnskap om de truslene vi er utsatt for er sentralt når vi skal bedre risikoforståelsen vår (Renn, 2008, s. 99). Det er uheldig at flere blir databrukere ute i virksomhetene, uten å nødvendigvis inneha den nødvendige kompetansen (Daler et al., 2019, s. 172-173). Gjennom økt bruk av teknologi og digitalisering har trusselbildet og den digitale risikoen økt. Teknologien og det menneskene som bruker kan ikke vurderes isolert, da disse komponentene påvirker og former hverandre. For å kunne håndtere digitale risiko må vi forstå hvordan digitale risikoer oppstår og hvordan de kan identifiseres (Jasanoff (2014) sitert i Engen et al., 2021, s. 247-249). Det betyr at kompetansen de ansatte har om digital risiko er viktig, og også en del av NorSIS sine åtte kjernepunkter for god sikkerhetskultur (2016). Hvordan og av hvem man lærer, kan få stor innvirkning på hva man lærer, og dermed hvor godt rustet man er til å motvirke digitale trusler. Hva som regnes som «riktig kunnskap» endres over tid og derfor er det viktig å inneha personer eller helst miljøer i virksomhetene som fremmer «riktig kunnskap» til de ansatte (Bergsjø et al., 2020, s. 41). Nesten alle informantene trekker frem stillingen CISO som avgjørende for å samle denne kunnskapen og presentere den på en helhetlig måte for alle ansatte i virksomhetene. Det fremkom også informasjon om at slike stillinger er noe alle virksomheter ønsker seg, men at ikke alle tar seg råd til å opprette slike stillinger. CISO-rollen har som formål å samle den digitale sikkerhetskompetansen, utvikle produkter som bidrar til læring og som et resultat av dette skape bedre risikoforståelse for alle ansatte i virksomheten.

I teorien om høypålitelige organisasjoner er et av prinsippene for å oppnå høy pålitelighet anerkjennelse av kompetanse (Weick & Sutcliffe, 2015, s. 7-14). Dette prinsippet tar for seg evnen virksomheten har til å utnytte egen intern kompetanse. Like viktig er anerkjennelse av hvilken kompetanse man mangler i selskapet og dermed trenger for å dekke hele spekteret av digital sikkerhet (Weick & Sutcliffe, 2015). Kraftcert blir omtalt av et stort flertall av informantene som en viktig sparringspartner når det kommer til formidling av digital sikkerhets kompetanse. De er også flinke på å tilby rådgivning og bistand ved større uønskede hendelser.

Både det informantene nevner om kompetansearbeid og det som kommer frem i teorien viser at kraftsektoren kjennetegnes av å ha stort fokus på å bygge digital sikkerhetskompetanse. Opprettelsen av CISO-stillinger i kraftsektoren har en åpenbar positiv effekt for å samle dette arbeidet og presentere «riktig kunnskap» til alle i selskapene. Samspillet mellom virksomhetene og sikkerhetsmiljøene i sektoren fremstår positiv rundt at den er med å påvirke risikoforståelsen til de ansatte ved rådgivning og direkte bistand.

5.1.1.3 Bevissthet – Holdninger til de ansatte

God risikoforståelse er en sentral bidragsfaktor i de ansattes holdninger til digital sikkerhet. Mange informanter sier dette arbeidet tar lang tid og noe som må modnes hos de ansatte. Da de i mange år har levd et liv med fysisk sikkerhet som prioritet, vil det nødvendigvis ta tid å oppnå samme digitale kompetansenivå. En av informantene sammenlignet holdninger med bilkjøring. Hvis det mangler opplæring og jevnlig påfyll av kompetanse vil de fleste velge å kjøre fortere enn anbefalt. De vil finne veier rundt etablerte regler og til slutt ende opp med å droppe de sikkerhetstiltak som er helt nødvendig for virksomhetens totale digitale forsvar. For å lukke disse sikkerhetshullene som ligger hos de ulike ansatte i virksomheten, trenger de jevnlig påfyll av riktig kompetanse og ulike opplæringsvarianter som er spesialtilpasset målgruppen. Her kan det igjen virke som at rollen CISO er avgjørende. Men det å bare basere seg på enkeltpersoner i organisasjonen kan være farlig. Bergsjø (2020) mener dette kompetansearbeidet burde settes i system, slik at holdningene til de ansatte jevnlig blir påvirket i riktig retning (Bergsjø et al., 2020, s. 41).

Alle informantene forteller om at virksomheten legger mye ressurser i å øke den digitale bevisstheten til de ansatte. Mange ansatte har opplevd det som vanskelig å henge med på begrepsbruken til IT- folkene i virksomheten. Dette har skapt en del misforståelser og bidratt til at tilliten mellom avdelingene har fått seg en knekk. Informantene opplever at markedssiden i virksomhetene ofte beveger seg for fort fremover i prosjekter. Det er ofte stort fokus på å vinne konkurransen om å utvikle nye effektiviseringsprogrammer og spare inn penger på sikkerhetstiltak. Dette medfører ekstraarbeid for IT-fagfolkene som føler de må rydde opp i sikkerhetsarbeid som burde vært håndtert på en bedre måte, tidligere i prosessen.

Flere av informantene med lederansvar nevnte at friksjonen mellom CISO, fysisk beredskapskoordinator og markedsavdelingen er avgjørende for et godt samspill. Flertallet av disse informantene mener at positive samarbeid skapes gjennom gode rammevilkår og at personer med riktige kompetanse snakker sammen før prosjekter rulles i gang. Andre informanter trekker frem at fokuset på HMS fortsatt tar for mye plass og at dette må likestilles med digitalt sikkerhetsarbeid. En leder-informant sier at det i stor grad handler om å lage et system som gir nok sikkerhetsopplæring og kunnskap til å skape digitalt motstandsdyktige ansatte. Alle informantene opplever en åpenhet og interesse fra de ansatte om å lære mer om teamet.

Et annet interessant funn som ble gjort var de ansattes bruk av sosiale medier. Spesielt de unge ansatte ble trukket frem som risikobrukere fordi de legger igjen store spor av personlig

informasjon om seg selv på nettet. Dette kan bli plukket opp av trusselutøvere og bli en del av et vellykkede angrep mot virksomhetene. En informant forklarte at eldre ansatte som jobber med fysisk produksjon vil kanskje ikke gi fra seg informasjon på samme måte og dermed kanskje være mer skjermet for digital risiko gjennom mindre bruk av sosiale medier.

Informantene beskriver holdningene om digital sikkerhet i kraftsektoren som generelt gode og at læringsvilligheten fremstår høy. Skal de gode holdningene opprettholdes må det påføres nok strukturert opplæring og kunnskap over tid, som teorien sier. Her viser informantene til at ulike avdelinger har ulike holdninger. Noen vil kjøre over fartsgrensen, mens andre vil ligge litt under for å være på den sikre siden innenfor digital sikkerhet. Funnene viser også det fysiske HMS-arbeidet tar for mye plass i en hektisk hverdag og at dette påvirker de digitale- holdningene til de ansatte på en negativ måte. Digital sikkerhet og HMS arbeid kan med fordel likestilles. Dette vil med stor sannsynlighet øke bevisstheten rundt digital sikkerhet og bedre den digitale risikoforståelsen. Teorien viser at holdninger tar tid å påvirke og derfor burde det ikke være for store ulikheter mellom det holdningsskapende arbeidet med HMS-arbeid og digital sikkerhet.

5.1.2 Ledelsens rolle ved arbeid med digital sikkerhetskultur

5.1.2.1 Forankring og organisering av arbeid med digital sikkerhetskultur hos ledelsen

Flere ganger har mangelfull planlegging, styring og gjennomføring av det digitale sikkerhetsarbeidet i norske virksomheter vært et tema i NSMs årlige risikovurderinger. Dette kan tyde på at ledelsen i virksomhetene ikke innehar den handlekraften som er nødvending og risikoforståelse av hvilke trusler og sårbarheter de står ovenfor. For å kunne drive et godt styrings- og gjennomføringsarbeid i virksomheten trengs det en tydelig forankring i ledelsen og styret (NSM, 2017 sitert i Bergsjø & Windvik, 2018, s 27).

Reasons (1997) teori om organisatoriske ulykker setter søkelys på latente forhold som årsak til at ulykker inntreffer. Her vektlegges de organisatoriske forholdene med ledelsen i spissen, heller enn menneskelige feil. Disse organisatoriske forholdene baserer seg ofte på beslutninger fattet av ledelsen i organisasjonen. På bakgrunn av denne teorien viser Reason (1997) til viktigheten av en god oppdatert risikoforståelse og at det fattes kunnskapsbaserte beslutninger fra ledelsen om ressurser og penger til arbeidet med digital sikkerhet. Informantene mener at ledelsens risikoforståelse de siste fem årene har tatt store steg i riktig retning. Der dette arbeidet tidligere ble tillagt fagansatte på digital sikkerhet, har det nå blitt løftet inn i virksomhetene sine styrer. Flere forteller om egne personer med ansvar for digital

sikkerhet som sitter i styrene. Dette har ført til mer ressurser på feltet og en større aksept for å bruke mer penger på forebyggende digitale tiltak. Noen informanter sier at arbeidet har blitt løftet, men at man i stor grad ennå ønsker å bruke mer penger på innovasjon, enn forebyggende digitale tiltak. Disse områdene står ikke i stil til hverandre og medfører en friksjon som stanser/hemmer virksomhetenes utvikling.

Flere teorier om sikkerhetskultur viser til at ledelsens forpliktelser til sikkerhetsarbeid er avgjørende. Velger ledelsen å ikke ta sine forpliktelser på alvor og delegere ansvaret til for eksempel IT- avdelingen, vil det med stor sannsynlighet bli nedprioritert til fordel for andre områder (Reason, 1997; Turner, 1978; Weick & Sutcliffe, 2015). Noen få informanter forteller om at digital sikkerhet ofte blir flyttet bort fra toppledelsen i virksomheten. Dette fordi IKT-materien er vanskelig og kompleks å forholde seg til for ledere uten særlig digital sikkerhetskompetanse. Dette kan være med på å gjøre at det digitale sikkerhetsarbeidet ikke får den plassen det fortjener og burde ha. Flere av leder-informantene deler dette synet, men mener det er helt avgjørende å flytte dette arbeidet nedover i organisasjonen, slik at de rette beslutningene kan treffes av personer med riktig kompetanse. Det ble også nevnt at «domenearkitektur» hadde blitt innført i en av virksomhetene. Dette innebær at de som leder ulike prosjekter i virksomheten har ansvaret for den totale sikkerheten i det aktuelle prosjektet de har ansvaret for. Mange informanter trekker frem dette eksemplet som noe positivt. Det gjør at alle i virksomheten må forholde seg til sikkerhetsaspektet når de utvikler nye produkter eller jobber med samarbeidsprosjekter. Dette har bidratt til å frigjøre noe ansvar fra IT-avdelingene og anerkjenne arbeidet med digital sikkerhet. De fagansatte informantene er enig i at dette er bra. De ansatte på digital sikkerhet får tydelig fremhevet hvor viktig deres arbeid er, og andre avdelinger ser verdien at de er med fra start, slik at sikkerhetsperspektivet i prosjektet blir ivaretatt.

Informantene er enige i at styringen av det digitale arbeidet har bedret seg. Teorien viser også tydelig at ledelsen spiller en avgjørende rolle her. Noen funn peker mot at store ulike krefter, spesielt på markedssiden i selskapene, enda får større oppmerksomhet og mer ressurser enn det digitale sikkerhetsarbeidet. Dette må ledelsen ta på alvor og forankre det digitale sikkerhetsarbeidet tydeligere slik at de fagansatte føler seg sett og tatt på alvor. Det er også viktig for ledelsen å inneha nok kompetanse til å forstå de digitale problemstillingene de har foran seg. Dette mener leder-informantene må løses ved å sette tydelige rammer fra ledelsen og skape diskusjonsrom med riktig kompetanse. De fagansatte er langt på vei enig i dette, men savner mer digital kompetanse hos ledelsen. De opplever enda at de selv må selge

inn et budskap for å få innvilget ressurser eller godkjent innkjøp. En sterkere forankring inne i toppledelsen hadde tatt bort mye av denne følelsen mener de fagansatte informantene.

5.1.2.2 Ledelsen som rollemodeller for digital sikkerhet

Flere informanter sier at klare mål som er uttalt fra ledelsen er viktig for å skape god kultur rundt digital sikkerhet. Et eksempel som blir trukket frem her er arbeidet med prediktivt vedlikehold (databasert vedlikehold) ute på kraftanleggene. En informant sier det er stor forskjell på å si «alt kan løses ved nok tilgang på data» enn å si «vi har som mål å bli ledende på prediktivt vedlikehold». Det at ledelsen går frem med klare mål for det digitale arbeidet er avgjørende for at kollektivet av ansatte skal se veien frem til målet og det legger til rette for et sunt samarbeidsklima mellom de ulike fagavdelingene. Betydningen av forståelige mål fra ledere trekkes frem av Bergsjø & Windvik (2018) som en viktig faktor når virksomhetene skal etablere styringssystemer for sitt digitale sikkerhetsarbeid (Bergsjø & Windvik, 2018, s.27).

Alle informantene beskriver en kamp om ressursene og at den fysiske sikkerhetskulturen står sterkt i bransjen. Informasjon knyttet til trusselen/risikoen for fysiske sikkerhetshendelser og produksjon er lettere for ledelsen å forstå enn digitale hendelser. Reasons (1997) sin teori nevner også at digital sikkerhet ofte knyttes til fravær av negative hendelser og det må større uønskede hendelser til for at ledelsen skal sette det øverst på sin agenda. Rolige perioder uten at virksomhetene blir utsatt for uønskede hendelser kan lede til mindre fokus på digital sikkerhet. Det kan igjen føre til at man glemmer hvilke trusler man står ovenfor og etablerer et sikkerhetsnivå som ikke står i stil til truslene som selskapene utsettes for (Reason, 1997, s. 4).

Arbeid med digital sikkerhetskultur er et ledelsesansvar, men for å lykkes må alle i virksomheten bidra. Ledelsen må sette klare mål for hva bedriften ønsker å oppnå, og jobbe målrettet over tid med digital sikkerhetskultur gjennom ulike tiltak. Bergsjø (2020) viser til at endringer i kulturen både kan skje top-down og buttom-up (Bergsjø, 2020, s. 44) Informantene mener fokuset har beveget seg fra en buttom-up-tankegang til en mer top-down-tankegang i virksomhetene. Før ble det digitale sikkerhetsarbeidet i større utstrekning drevet av de digitale fagansatte. Fagansatte har hatt høy tillit hos ledelsen, noe som har muliggjort innføring av endringer de mener er nødvendige for å forebygge uønskede digitale hendelser. Nå ser informantene oftere at ledelsen selv driver frem satsningen på digital sikkerhet. NSMs grunnprinsipper skal bidra til bedret informasjonsflyt om sikkerhetstilstanden i virksomhetene. For at dette arbeidet skal lykkes har NSM (2020) laget en figur som viser samspillet mellom toppledelsen, forretnings- og IT- ledelsen og til implementasjon- og

driftsnivå. NSM (2020) beskriver i denne modellen at toppledelsen har ansvaret for organisatorisk risiko (NSM, 2020, s. 4). Fokuset på denne typen risiko gjør at toppledelsen kan fastsette forretningsprioritet, kommunisere risikotoleransen til virksomheten og tildele budsjettmidler. Det står presisert at eierskapet og ledelsens involvering i sikkerhetsarbeidet er avgjørende. Videre sier modellen at forretnings- og IT-ledelsen har ansvaret for oppdaterte risikooppdatering for virksomhetene og anbefalinger til hvilke tiltak som skal iverksettes. Dette samspillet viser at ledelsen sin risikoforståelse er helt avgjørende for å fatte hensiktsmessige tiltak på digital sikkerhet (NSM, 2020, s. 5).

Et flertall av informantene sier også at ledelsen med fordel i større grad kan fordele ansvaret for digitalt sikkerhetsarbeid bredere i organisasjonen. Eksempelvis mener informantene at informasjonssikkerhet som er en del av digitalt sikkerhetsarbeid kan fordeles ut til HR-avdelingene i virksomhetene. Dette vil bidra til bedre risikoforståelse hos HR og øke bevisstheten i deres arbeid ved for eksempel rekruttering av nye medarbeidere. At HR gjør gode digitale sikkerhetsvurderinger på hvilke tilganger som er nødvendige og hvilken opplæring den enkelte burde ha for å utføre sine arbeidsoppgaver på en sikker måte. En informant sier at ledelsen har satt dette i system på en helt annen måte enn før. Arbeidet med å inneha tilstrekkelig kompetanse for å håndtere uønskede digitale hendelser er i full gang. Dette er tiltak som er proaktive, reaktive og detekterende digitale sikkerhetstiltak. Flere informanter sier at den digitale sikkerhetskulturen må tilpasse seg den gamle og gradvis bygges opp.

Det at oppdaterte digitale risikooppdateringer blir fremlagt ukentlig er like viktig som at beredskapskoordinatoren legger frem de fysiske sikkerhetshendelsene og sårbarhetene sier flere av informantene. Bildet informantene maler av ledelsens rolle i sikkerhetskulturen er positiv, men at det varierer i hvilken grad det tas på alvor og er satt i system. Informantene peker på en tendens til at IT- avdelingen selv må jobbe for å få gjennomslag, fremfor at ledelsen setter klare mål og viser gjennom handling hva som tas på alvor. Informantene trekker spesielt frem at det fysiske HMS- arbeidet enda tar for mye plass i virksomheten. Skal kraftsektoren lykkes med å inneha samme modenhetsnivå på digitalt sikkerhetsarbeid, må ledelsen i større grad vise dette gjennom å være gode rollemodeller og tilføre nok ressurser for å drive dette arbeidet. Målene som settes i selskapene må komme frem på en tydelig og helhetlig måte fra ledelsen. Hvis ikke tyder funnene i studien på et mindre helhetlig arbeid med digital sikkerhet og at de ulike fagmiljøene i større grad vil jobbe hver for seg i prosjekter.

5.1.3 Varsling og læring

Bergsjø (2020) vektlegger ledelsens kommunikasjon om digital sikkerhet. De ansatte skal ikke være i tvil om hvorfor de digitale sikkerhetstiltakene er iverksatt i selskapet og tiltakene skal ha en klar og tydelig forankring i ledelsen (Bergsjø et al., 2020, s. 28). Denne kommunikasjonen vil være med å danne grunnlaget for det Reason (1997) kaller en informerende kultur. Reason (1997) trekker frem fire elementer som underbygger en informerende kultur; rapportering, rettferdighet, fleksibilitet og læring (Reason, 1997, s.195). Vi velger i denne oppgaven å se nærmere på fleksibel kultur og rapporterende kultur da våre funn i størst grad belyser disse to elementene.

Fleksibel kultur

Dette innebærer at virksomheter med hierarkiske system, endrer fra sentralisert til desentralisert beslutningstaking. Denne endringen er ment å være dynamisk slik at den kan endres tilbake når behovet for denne organiseringen ikke lenger er gjeldende (Reason, 1997, s. 213-218). Alle informantene trekker frem bruken av beredskap ved uønskede hendelser. Det at de har beredskapsplaner for digitale hendelser gjør virksomhetene i stand til å forebygge og drive skadebegrensning tidlig i en uønsket hendelse. Flertallet av informantene sier at ledelsen har stor tillit til at de rette fagfolkene finner sammen og fatter riktige beslutninger, og at beslutningsmyndigheten ved digitale hendelser er flyttet til ansatte med riktig kompetanse. Bruk av beredskap i normalsituasjon bidrar til god læring og øving forteller informantene. En informant mener at bruken av å sette beredskap er litt for utbredt og at dette kan skape en avstand til truslene hos de ansatte. Flertallet viser også til at føringer som kommer fra NVE raskt og effektivt blir tatt tak i og utbedret på en god måte. Virksomhetenes evner å utbedre pålagte tiltak samtidig som de opprettholder god produksjon er viktig. Hvis de ansatte ikke opplever å være berørt av at beredskapsledelsen setter beredskap, kan bevisstheten til de ansatte falle og de kan oppleve at hendelsene som blir håndtert ikke er så alvorlige.

Rapporterende kultur

Det kan være flere grunner til at de ansatte unnlater å rapportere, deriblant at de ansatte føler at rapportering medfører merarbeid, det er mangel på tillit eller at de ansatte har et ønske om å glemme feilen sin (Reason, 1997, s. 198-199). Samtlige leder-informanter forteller om viktigheten av å skape tillit til de ansatte slik at de tørr å varsle og rapportere avvik. Flertallet av informantene sier at arbeidet med rapportering og bevissthet må kjennetegnes ved trygghet og ikke ved krasse og harde tilbakemeldinger uten en begrunnelse. Tilbakemeldinger er en

viktig del av en slik informerende kultur og innebærer at ledelsen og fagpersoner gir gode tilbakemeldinger til de ansatte og ikke fordeler skylden etter en. Dette vil være positivt for de ansatte da de ser hvordan avvik blir håndtert og dermed ser verdien av å rapportere avvik. Tilbakemeldinger kan også brukes til å gratulere arbeidstakerne i sitt kollektive bidrag til å forbedre sikkerhetskulturen (Reason, 1997, s. 200). Her forteller informantene om et godt samarbeid med ledelsen i virksomhetene. De fagansatte er opptatt av at ledelsen må tørre å stå frem selv for at de ansatte skal følge etter. En av informantene trekker frem det han kaller «security champions» i virksomheten. Dette er personer som innehar god kompetanse om digital sikkerhet og evner å dele denne kunnskapen med andre. Dette fører til at de ansatte blir opptatt av å levere på digital sikkerhet og at terskelen for å innrømme feil blir senket, ifølge et flertall av informantene.

Informantene forteller om fleksibel kultur stemmer godt med teorien på området. At virksomhetene er godt drillet ved bruk av beredskap ved mindre hendelser tyder på en fleksibel og lærende kultur i kraftsektoren. Gode tilbakemeldinger fra ledelsen og fra de fagsansatte rundt opplæring og avvik fremstår på et godt nivå og bevisstheten rundt hvilke konsekvenser denne jobben har virker å ligge langt fremme hos virksomhetene.

5.2 Forebyggende arbeid og myke barrierer

I det følgende vil vi se på måten virksomhetene driver forebyggende arbeid i virksomheten på. Beredskap og forebygging er sentralt når det kommer til den digitale sikkerhetskulturen i kraftsektoren, og flere informanter påpeker viktigheten av at man driver forebygging gjennom konkrete tiltak, opplæring og kompetanse for å hindre at uønskede hendelser i det hele tatt inntreffer.

5.2.1 Forebygging av uønskede hendelser – den menneskelige faktor

Reason (1997) er opptatt av at sikkerhetsstyring skal være noe som er kontinuerlig og som er en del av virksomhetens kjerneområde, og ikke oppfattes som et tillegg (Reason, 1997, s 114). Digitale trusler er i en voldsom utvikling, noe som gjør at det å unngå uønskede digitale hendelser, er nesten unngåelig. Reason sier at man i stedet for å fokusere på å ha direkte kontroll over uønskede hendelser, bør man heller fokusere på å drive med jevnlig utbedring og måling av sikkerhetstiltak i virksomheten (Reason, 1997). Dette kan for eksempel være arbeid med myke barrierer som bevisstgjøring, kunnskap og kompetanse hos de ansatte. Dette er noe informantene legger stor vekt på, og vi vil her redegjøre for barrierer og sikringstiltak som skal redusere risikoen for digitale angrep. Disse kan deles inn i kategoriene menneskelige, organisatoriske og teknologiske (NSM, referert i Bergsjø et al,

2020, s. 20). Vi vil ikke se på tekniske sikkerhetstiltak, men vi fokuserer på myke barrierer, nemlig de menneskelige og organisatoriske.

Det er forskjellige meninger hos informantene om hvor mye forebyggende sikkerhetsarbeid som utføres for å forhindre at uønskede hendelser oppstår i virksomheten. Enkelte mener at de får god tid til dette, og fremhever CISO-rollen som avgjørende for å sette forebyggende arbeid i praksis gjennom blant annet opplæring. En informant opplever at det forebyggende arbeidet kommer i andre rekke i sin virksomhet, og at man ender opp med brannslukking av hendelser som oppstår. Flere informanter forteller at forebyggende tiltak er vanskeligere å måle og se effekt av, noe som kan være en faktor som gjør at dette ikke prioriteres.

Til tross for gode tekniske sikkerhetsløsninger i virksomheten, er det flere av informantene som hevder at teknologi ikke er nok for å forsvare seg fullt ut mot digitale trusler. I de aller fleste situasjoner er det den menneskelige faktoren som er avgjørende for å hindre at uønskede hendelser inntreffer og ofte kan manglende kunnskap, kompetanse, forståelse og bevissthet rundt digital sikkerhet føre til at man enklere lar seg lure, og at man blir et offer for blant annet et phising-angrep (Bergsjø, et al., 2020, s. 135). Man hører ofte at den menneskelige faktoren er årsak til at ting har gått galt. (Norsis, 2020, s. 62).

I sin teori om organisatoriske ulykker snakker Reason (1997) om menneskelige feil. Han forteller at ulykker kan unngås ved at man har et såkalt «defences in depth». (Reason, 1997, s. 54-56). Dette er et forsvarsverk, som innebærer at det etableres flere barrierer mot en uønsket hendelse, slik at det er god nok beskyttelse for at en ulykke ikke skal inntreffe. Han forteller at myke barrierer handler om en menneskelig handling, som for eksempel kunnskap, kompetanse og trening, men også regler, prosedyrer og sertifiseringer, mens harde barrierer er det som går for eksempel på teknologiske sikkerhetsløsninger. (Reason, 1997, s. 8). For at en uønsket hendelse ikke skal inntreffe, bør alle sikkerhetslag være tette, men som oftest oppstår det hull, og dette skyldes aktive feil eller latente forhold (Reason, 1997, s. 7). Menneskelige feilhandlinger mener Reason skyldes latente forhold, som blant annet manglende opplæring og trening, og at dette ofte baserer seg på beslutninger fra ledelsen. Et tenkt tilfellet kan være at dersom ledelsen ikke prioriterer kompetanseheving hos de ansatte, så kan dette føre til en feil, som skaper et hull i forsvarsverket. Informanten som forteller at forebyggende arbeid kommer i andre rekke i deres virksomhet, kan vise til ett latent forhold i virksomheten som resulterer i en feil.

HRO-teorien snakker om opptatthet om feil, og setter fokus på at den minste feil kan bli en større feil og gi virksomheten store konsekvenser (Weick & Sutcliffe, 2015, s. 46-48). Ved å tidlig ta hånd om feil, kan man forebygge at den utvikler seg til noe større. For at man skal kunne håndtere feilen, må man identifisere den, og dette fordrer kunnskap og kompetanse om digital sikkerhet. Skal en ansatt unngå å trykke på en ondsinnet link i en epost, må han kunne være i stand til å oppdage den, noe som krever kunnskap og kompetanse. En informant forteller at de bevisst jobber forebyggende i sin virksomhet med den menneskelige faktoren for å skape ansatte som har sikker digital opptreden og god risikoforståelse, og jobber med å gi de ansatte kunnskaper og erfaringer. Flere andre informanter forteller at forebyggende tiltak som opplæring og bevisstgjøring er med på å øke kompetansen hos de ansatte, og at dette er noe de gjennomfører i virksomheten sin. For en informant handler det om å få en varsellampe til å lyse hos de ansatte hvis de ser noe unormalt, og at de er i stand til å flagge en hendelse videre til riktige fagpersoner.

Det at menneskelig feil alltid vil oppstå i virksomheter, gjør mennesker til en viktig faktor i sikkerhetsarbeidet, og de fleste informantene enes om at målet må være å skape en digital sikkerhetskultur med ansatte som er bevisst sin digitale atferd og hvilken rolle de har for å forebygge at digitale uønskede hendelser inntreffer.

5.2.2 Digital opplæring og bevisstgjøringsprogrammer – et verktøy for atferdsendring?

Flere informanter forteller at de driver forebyggende arbeid gjennom opplæring og bevisstgjøring av de ansatte ved virksomheten. Forebyggende tiltak som phising-tester, e-læring og informasjonsdeling i workspace blir nevnt, og mange mener at de ser en effekt av dette ved at blant annet IT-avdelingen mottar flere rapporteringer og det blir en «snakkis rundt bordet». Andre informanter etterlyser ett bedre opplæringstilbud som er mer formelt og/elle mer skreddersydde opplæringsløsninger som tilpasser seg den enkelte ansatte.

NorSIS (2020) slår fast i sin rapport om digital sikkerhetskultur at til tross for masse opplæringstilbud innen digital sikkerhet, og at de fleste blir opplært i digital sikkerhet gjennom arbeidsgiver, så uteblir den ønskede atferdsendringen.. De spekulerer i om den digitale kunnskapsoverføringen som gjøres i dag ikke er nok for å få til en atferdsendring. De mener at dagens digitale opplæringsprogrammer må evalueres, og at man må se mer mot motivasjonspsykologi og mestringsforventning, og på den måten mer effektivt påvirke den menneskelige faktoren, og dermed atferd (Norsis, 2020, s 61-63).

I ett studie gjort av Bada, Sassa og Nurse (2019) som omhandler opplæring og

bevisstgjøringskampanjer innen digital sikkerhet blir det sagt at endring av atferd krever mer enn at de ansatte bare mottar informasjon om risiko og informasjon om sikker digital adferd. De ansatte må for det første anerkjenne at informasjonen er relevant for dem, for det andre forstå hvordan de bør reagere, og for det tredje være villig til å reagere på denne måten i møte med andre krav de er satt til å gjøre. Kunnskap og bevissthet er ikke alltid alene tilstrekkelig for å endre atferd, men fordrer ofte også en bredere forståelse av hvorfor mennesker handler som de gjør, herunder personlige og kulturelle faktorer. (Bada & Sassa & Nurse, 2019, s 2 og 3). Dette viser at opplæringsprogrammer krever mer enn det man tror for å påvirke atferd, og er kanskje en grunn til hvorfor enkelte informanter ønsker et bedre og mer skreddersydd opplæringsprogram innen digital sikkerhet.

Det som påvirker menneskets digitale atferd er personlige faktorer som kunnskaper, evne og forståelse av digital sikkerhet, samt erfaringer, holdninger og tro (Bada & Sassa & Nurse, 2019, s. 3). Noen informanter forteller at de ansattes holdninger til digital sikkerhet er relatert til hvilken rolle dette har for dem i deres virke. Et eksempel som trekkes frem av en av informantene er at de eldre ansatte oppleves som mer umodne på digitale løsninger, og som for eksempel bruker datamaskinen kun for å føre timer og svare epost. Han mener at deres forståelse og evne til digital sikkerhet er lav. Digitale farer ofres ikke en tanke, og man er fornøyd dersom ting fungerer som det skal (Nätt et al, 2019, s. 25). Viktigheten av at opplæringen er enkel å følge, og oppleves som personlig og aktuell for denne gruppen, blir nøkkelfaktorer for et effektivt opplæringsprogram, og at det ikke oppleves som enda en obligatorisk økt som den ansatte må gjennom (Bada & Sassa & Nurse, 2019, s. 2). Når det gjelder personlig opplæring, forteller en av informantene at det er viktig å være bevisst på hvilken historie som fortelles til de ansatte. Dersom historien oppleves som konkret og nærliggende, for eksempel om en digital hendelse i virksomheten, så skapes det troverdighet til historien. På den andre side kan det oppstå følelser av frykt og fortvilelse, dersom opplæringen inneholder overkomplisert informasjon og skremselshistorier (Bada et al, 2019, s 5-6). Som læringsteorien viser, er følelser av frykt en barriere for god læring (Sommer et al, 2020, s 100). Målet bør være at de ansatte får en opplevelse av at de behersker det som blir forespeilet, noe som kan gjøres ved at de får enkle, konsekvente atferdsregler som de faktisk klarer å følge og forstå. Dette er det som omtales som opplevd kontroll, og som anses som en avgjørende faktor for en større aksept av den ønskede digitale atferden som forsøkes opplært (Bada & Sassa & Nurse, 2019, s. 4).

Flere informanter forteller at repetisjon er nøkkelen for å bedre den digitale forståelsen hos de

ansatte, da hyppige påminnelser ville bidra til økt bevissthet om digital sikkerhet hos den ansatte. NorSIS (2020) har utfordret denne tankegangen, og mener at det er en overforenkling at den ansatte skal ta til fornuft bare den får repetert et budskap mange nok ganger (Norsis, 2020, s 62) Weick & Sutcliffe nevner også dette, og sier at dersom man forenkler ting kan det gjøre det vanskelig å forestille seg uønskede konsekvenser (Weick & Sutcliffe, 2015, s. 63). De ansatte må forstå tydelig forstå hva opplæringsprogrammet prøver å lære dem og hvorfor det er relevant for dem i deres hverdag.

5.2.3 Phishing-tester – hvor effektivt er det?

Det å øke bevisstheten til de ansatte gjennom phishing-tester, er noe flere av informantene sier at gjøres regelmessig i virksomheten. Virksomhetene erfarer gode resultater med bruk av dette ved at de observerer færre ansatte som lures, og flere rapporterer mistenkelige e-poster. To av informantene forteller også at dette anses som en enkel måte å måle sårbarheten til virksomheten på når det gjelder de ansattes digitale atferd.

Det har vært en del forskning på hvor effektiv anti-phishing tester er for å forebygge at ansatte lar seg lure lure. Ett stort studie ble gjort i 2021 hvor man studerte en stor organisasjon i femten måneder med over 14.000 deltakende ansatte, og hvor de ansatte ble tilsendt phishing-tester jevnlig gjennom studieperioden (Lain, Kostiainen, Capkun, 2021). Funnene som ble gjort var blant annet at de som hadde blitt sendt til en opplæringsside etter at de hadde latt seg lure av en phishing test, klikket oftere på linker/vedlegg i fremtidige phishing-tester, enn de som ikke hadde mottatt trening. En mulig årsak til dette var at opplæringen ga en falsk trygghet, eller at man følte mindre ansvar for å stoppe slike angrep (Lain, Kostiainen, Capkun, 2021).

Flere av informantene forteller om at dersom man lar seg lure av en phishing-test hender det at man blir sendt til en opplæringsside. Selv om funnene i studien nevnt over viser at dette potensielt kan ha en negativ effekt, opplever flesteparten av informantene økt bevissthet og risikoforståelse hos ansatte i virksomheten ved bruk av phishing-tester. Informantene opplever phising-tester som et effektivt verktøy for å kartlegge hvilke fagmiljøer som har størst behov for digital bevissthet.

Et annet interessant funn i deres studie var at crowdsourcing, noe man på norsk kan omtale som nettdugnad, var en effektiv måte for deteksjon av phishing-eposter. Dette funnet ble underbygget med at de ansatte hadde en korrekt varsling av 68% av phishing-eposter som ble sendt ut, og som hjalp sikkerhetsavdelingen med å forebygge phishing-angrep.

Crowdsourcing i dette tilfellet går på at de ansatte hadde en varslingsknapp til sikkerhetsavdelingen lett tilgjengelig, og at de hadde muligheten til å trykke på denne for å varsle til sikkerhetsavdeling ved mistenksomme e-poster (Lain, Kostiainen, Capkun, 2021).

Ingen av informantene forteller spesifikt om crowdsourcing som verktøy, men flere forteller at de har varslingssystemer for de ansatte. En av informantene forteller at de har en rapporteringsknapp i Outlook, men at den ikke har fungert så bra hos dem, og at de heller har fokusert på å lære de ansatte til å sende mistenksomme eposter til en postkasse som går til IT-avdelingen. Det som i midlertidig blir påpekt av flere er at det må oppleves som enkelt å varsle, samt at den ansatte ikke må føle ubehag i form av flauhet og frykt for å varsle. Vi har tidligere nevnt at frykt er en barriere for læring, og det er nærliggende å tenke at flauhet også er en barriere, hvor ansatte som har gjort en feil, ikke tør å varsle om det som har blitt gjort. Flere av informantene forteller at de er bevisst på dette, og prøver å få bukt med disse følelsene ved å fortelle de ansatte at det er menneskelig å gjøre feil.

Det nevnes en rekke spesifikke tiltak fra informantene som brukes til å øke kunnskap og bevissthet rundt digital risiko i selskapene. Vi har valgt å trekke frem phishing- testing fordi samtlige informanter forteller at dette blir brukt i studien. Det er tydelig at mange fagfolk innen digitalt sikkerhetsarbeid legger mye arbeid i å lage slik tester og at sektoren selv opplever testene som verdifulle.

5.2.4 Ulike opplæringsverktøy evne til å øke bevisstheten

Khan, Alghathbar, Nabi og Khan (2011) har forsket på opplæringsverktøyenes effekt på bevissthet rundt informasjonssikkerhet, og har målt de ulike verktøyene ut fra en femstegs-modell som omfatter kunnskap, holdning, subjektive normer, intensjon og atferd. Jo høyere opp på tabellen, jo mer er verktøyet egnet til å øke bevisstheten. Utgangspunktet for modellen ligger i teorien om planlagt atferd, hvor intensjonen til et menneske er utslagsgivende for endring i atferd. Holdninger og subjektive normer er det som påvirker en persons intensjon. (Khan, Alghathbar, Nabi og Khan, 2011, s. 2 og 3). For å eksemplifisere, kan man si at for å endre en ansatts digital sikkerhetsatferd, vil hans atferd (intensjon) være avhengig av om han liker eller misliker digital sikkerhet (holdning), samt hvordan han tror andre ansatte mener han må gjøre (subjektiv norm).

Gruppediskusjon blir satt på øverste trinn i modellen. Her vektlegges interaksjon, hvor deltakere kan diskutere ulike sikkerhetsutfordringer. Dette gir økt motivasjon, og man bruker sosial interaksjon for å påvirke menneskets forståelse av digital sikkerhet. Gjennom

forandring i holdninger og subjektive normer kan intensjonen endres (Khan, Alghathbar, Nabi og Khan, 2011, s. 4). For å konkretisere, så kan en ansatt gjennom en gruppedialog, endre sin digitale atferd gjennom å få nye holdninger og høre hvordan andre snakker om dette. Som et forebyggende tiltak ønsket enkelte av informantene å reise mer ut i virksomheten og nettopp samle ansatte for å snakke om digital sikkerhet.

På nest laveste trinn i modellen, kommer blant annet nyhetsbrev. Flere av informantene forteller om bruken av virksomhetens Workspace, hvor det legges ut informasjon og artikler om temaer innen digital sikkerhet. Dette er en enkel måte å dele og gi ut informasjon i virksomheten på, og dersom informasjonen er god og relevant, kan dette være en god form for opplæring når det kommer til kunnskapsoverføring og holdningsarbeid. Dog er det vanskelig å forsikre seg om at ansatte faktisk leser innholdet (Khan, Alghathbar, Nabi og Khan, 2011, s. 4), noe informantene som snakker om Workspace er enige i. Selv om de ansatte har lest informasjonen, er det også vanskelig å vite om den ansatte har forstått det som står skrevet. Da utsendelse av nyhetsbrev, til forskjell fra gruppediskusjon, mangler subjektive normer, er det mer utfordrende å endre leserens intensjon, og dermed også i forlengelse av dette, vedkommendes atferd.

Databasert trening (CBT), som innbefatter E-læring, er et digitalt opplæringsverktøy som flere informanter forteller at virksomheten bruker. Fordelene med en slik læring, er at det krever lite ressurser, er enkelt å forholde seg til, kostnadseffektivt og at den ansatte kan gjennomføre opplæringen i eget tempo og foretrukne omgivelser (Khan, Alghathbar, Nabi og Khan, 2011, s.4 og 5). En informant forteller at de kjøper inn ferdig e-læring med ulikt innhold regelmessig sendes ut til de ansatte. Bakdelen med e-læring er at man er avhengig av at den ansatte faktisk gjennomfører e-læringen, og man har heller ingen garanti for den ansatte bare klikker seg igjennom. I tillegg, så mangler den på lik linje som nyhetsbrev subjektive normer, da det ikke legger opp til noe dialog. Bruk av ferdiglagde pakker, medfører at innholdet heller ikke er tilpasset og spisset det virksomheten ønsker å treffe. Det kan føre til en opplevelse av at innholdet ikke er relevant, noe som Bada & Sassa & Nurse (2019) mener er at krav for at atferdsendring kan skje.

6 Konklusjon

Høy grad av digitalisering i kraftsektoren fordrer et fokus på digital sikkerhet. For at denne utviklingen ikke skal få store negative konsekvenser for kraftsektoren må den digitale sikkerheten ivaretas fortløpende både av nasjonale myndigheter og selskapene selv. For å lykkes med dette arbeidet er vi som samfunn avhengige av at virksomheter jobber effektivt og riktig med sikkerhetskulturen sin. Kraftsektoren som helhet må jobbe sammen for å skape en god digital sikkerhetskultur. For å finne ut om hvordan statusen er på dette har vi stilt problemstillingen: *Hva kjennetegner norske kraftselskaper sitt arbeid med digital sikkerhetskultur, sett fra fagansattes og ledelsen sitt perspektiv?*

For å besvare problemstillingen har vi undersøkt hvordan kraftselskaper i Norge opplever \ arbeidet med digital sikkerhetskultur. Vi har spurt både store og mindre virksomheter og hatt fokus på perspektiver fra både ledelsesnivå og fra de fagansatte for å gi en bredere forståelse av hvordan dette oppleves i kraftsektoren. Studien gir et innblikk i utfordringer knyttet til å drive digitalt sikkerhetsarbeid i kraftsektoren og hvilke faktorer som påvirker arbeidet positivt og negativt. Informantene har alle bidratt med relevante erfaringer, opplevelser og informasjon om arbeidet med digital sikkerhetskultur, noe som har muliggjort en inngående og dypere forståelse av tematikken. Faktorene trukket frem i dette forskningsprosjektet har gitt en stor innsikt i temaet, men det påpekes at dette er spesielt for kraftsektoren og det kan være andre faktorer påvirket arbeidet med digital sikkerhetskultur generelt/i andre samfunnskritiske funksjoner.

Gjennom empiriske funn og utvalgt teoretiske rammeverk kom vi frem til at to hovedkategorier vurderes å kunne ha stor betydning for å forstå den digitale sikkerhetskulturen i kraftsektoren. Under disse hovedkategoriene er det igjen trukket frem underpunkter for å vise bredden i arbeidet og på en hensiktsmessig måte besvare våre forskningsspørsmål.

- **Digital sikkerhetskultur**
  - Bevissthet - Risikoforståelse, Kompetanse og holdninger
  - Ledelse – Forankring av digital sikkerhetsarbeid i ledelsen- ledelsen som rollemodeller – Organisering og målsetninger fra ledelsen
  - Varsling og læring – Rapporterende kultur og fleksibel kultur
- **Barrierer**
  - Forebyggende arbeid og myke barrierer

- Arbeid med spesifikke opplæringsmetoder

Forskningsprosjektet vårt om digital sikkerhetskulturarbeidet i kraftbransjen har i all hovedsak tatt for seg menneskelige og organisatoriske forhold. Resultatene fra studier viser at kraftbransjens digitale sikkerhetskulturarbeid er på rett vei, men at fremgangsmåte, metode og tilnærming varierer fra i de ulike virksomhetene og at de ulikt oppfatter hvilke faktorer som er mest avgjørende. Ledelse-informantene er i stor grad samstemte med de fagansatte informantene. De vektlegger noen områder ulikt, men resultatene viser er godt samspill i arbeidet med digital sikkerhetskultur. Risikoforståelsen i kraftsektoren fremstår noe splittet med de fagansatte som jobber med digital sikkerhet på den ene siden og et større OT - miljø ute på anleggene som jobber med andre digitale utfordringer. Denne avstanden, i hvordan man forholder seg til digital sikkerhet, er viktig å være bevisst slik at det ikke oppstår ulike oppfatninger av den faktiske risikoen virksomhetene står ovenfor, og betydningen den enkelte ansatte har for å utbedre digitale sårbarheter. Friksjonen mellom markedsavdelingene og sikkerhetsfolkene i selskapene problematiseres av informantene, men begge påpeker at en tydelig ledelse er viktig for å skape gode rammer for samarbeid om digital sikkerhet. Ledelsen virker å ha kommet langt ved å ha innført en mer effektivt organisering av dette arbeidet, basert på mer kunnskap om digital sikkerhet hos ledelsen og en bedre risikoforståelse. Betydningen av at ledelsen jevnlig mottar oppdatert tidsriktig kunnskap om trusler og sårbarheter gjennom presentasjon fra de fagansatte på digital sikkerhet i virksomheten er viktig. Ledelsen må også gå foran som gode rollemodeller og tørre å innrømme egne feil slik at de ansatte opplever et trygt varslings- og rapporteringsmiljø.

Den menneskelige faktoren blir nevnt i nasjonale risikovurderinger og i spesiell grad av de fagansatte informantene. Det å ha et tydelig opplærings- og bevisstgjøringsprogram er avgjørende for å endre de ansattes bevissthet- og øke kunnskapen til de ansatte om digital sikkerhet. Kraftsektoren med sitt store spenn i ansatte setter spesielle krav til opplæringen og øvingen av de ansatte. En kombinasjon av ulike og tilpassede læringsopplegg trekkes frem som mest effektivt, og at man har en tydelig oppfatning av hvilke ansatte som trenger hvilket opplæringsløp. Informantene sier de gjerne skulle hatt mer tid til dette arbeidet. Alle informantene sier de jobber med egne opplæringsopplegg og at dette krever mye av de digitalt fagansatte. En styrking av samarbeidet mellom virksomhetene i kraftsektoren på dette området vil kunne gi en mer effektivt og hensiktsmessig utvikling av opplæringsprogram. Her nevnes det noen samarbeidskanaler, men mye av denne kontakten kan fremstå som noe uformell og lite strukturert. Tabell 6.1 viser en kobling mellom funn, teori, og implikasjoner.

Hovedfunn	Kjerneområder fra teorien	Detaljer fra kraftsektoren	Praktiske implikasjoner
Bevissthet - Risikoforståelse	• Risikoforståelse- noe subjektivt. • Enkelte har en urealistisk optimisme i møte med risiko. • Opplevd digital risiko er større ved begrenset kunnskap.	• Digital sikkerhet oppfattes for noen nytt og fremmed. • Stor ulikhet internt hos de ansatte om betydning de selv har for digital sikkerhet.	• Synet selskapet har på hvordan ulykker inntreffer vil påvirke de ansattes risikooppfattelse • Tydelig «riktig kunnskap» fra CISO rollen bidrar til økt bevissthet og hensiktsmessig risikoforståelse hos de ansatte.
Ledelsen	• Ledelsen har ansvaret for det digital sikkerhetsarbeidet. • Ledelsen spiller en betydelig rolle i opplæring og bevisstgjøring gjennom klare mål og tydelig kommunikasjon	• Varierende kunnskaper hos ledelsen påvirker fokus og strategi. • Holdningene til ledelsen er gode og digital sikkerhet tas i større grad inn i styrearbeidet og i toppledelsen.	• NSM sine retningslinjer viser hvordan ledelsen kan påvirkes positivt. Vitkig med jevnlig risikopresentasjoner om nå- situasjonen. • Ledere er avgjørende for å samle alle ansatte rundt et felles mål.
Varsling og læring	• Sikkerhetskultur bygges på varige, suksessfulle tiltak og felles læringsprosess. • Fleksibilitet rundt beslutningstaking er en fordel • Gode positive og negative tilbakemeldinger er viktig for å skape tillit til rapportering av avvik.	• God innarbeidet beredskapskultur som kan brukes i fred og krig. Dynamiske selskaper. • Opptatt av å skape tillit og at ledelsen går frem som rollemodeller.	• Ledelsen må spille er tydelig og ydmyk rolle ved etablering av rapporterings og varlsingskultur • Bevisstheten rundt gode tilbakemeldinger øker tilliten til de ansatte og de vil mest sannsynlig rapportere flere avvik og på den måten tette sikkerhetshull.
Forebyggende arbeid og spesifikke tiltak for opplæring og bevisstgjøring	• Menneskelige faktor må vektlegges i stor grad ved opplæring. • Sammensatte opplæringssystemer er viktig for god læring. • Tiltakene har som hensikt å øke bevisstheten rundt truslene selskapene står ovenfor. • Opplæringer må være satt i system og komme jevnlig.	• Forebyggende arbeid prioriteres i større grad enn før, men fortsatt en del brannslukking. • Stort spenn i typen ansatte setter store krav til indivudualiserte opplæringsprogram. • Påvirkning av bevisstheten gjennom opplæring og kunnskap står sterkt i kraftsektoren. Friksjonen mellom marked og sikkerhet hemmer utviklingen.	• Kulturelle ulikheter må hensyntas ved utarbeidelse av opplæringsprogrammer. • Ulike opplæringsmetoder i et samspill gjør at bevisstheten øker hos de ansatte. • Kartlegging av hvilke ansatte man har i organisasjonen er avgjørende for å påvirke dem i positiv retning rundt digital sikkerhet.

6.1 Videre forskning

Vi har i denne studien intervjuet fagansatte på digital sikkerhet og ledere i virksomhetene som i stor eller mindre grad jobber med digital sikkerhetsarbeid. Det betyr at informasjonene som informantene har kommet med har vært preget av gode kunnskaper rundt teamet digital sikkerhetskultur. En naturlig videreføring av studien hadde vært å intervjue ansatte og ledere som ikke har digital sikkerhetsarbeid som sin stillingsbeskrivelse og da videre undersøkt om de funnene som kommer frem i denne studien samsvarer med hva de andre ansatte og lederne oppfatter rundt digital sikkerhetskultur og hvordan de opplever opplærings og bevissthetsarbeidet. Sikkerhetskultur inneholder mange ulike faktorer og kan dermed være vanskelig å måle på en korrekt måte. Dermed har hensikten i denne oppgaven være å finne ut hva som kjennetegner den digitale sikkerhetskulturen i kraftsektoren. En slik videreføring som nevnt over ville gitt et enda bredere kunnskapsgrunnlag og hadde med stor sannsynlighet gitt verdifulle svar til dem som jobber med dette i det daglige arbeidet sitt.

Referanser

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K. (2019). *Samfunnssikkerhet*. (9. utg.). Oslo: Universitetsforlaget.

Aven, T. & Renn, O. (2010). *Risk Management and Governance*. (1. utg.). Berlin: SpringerVerlag.

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. Hentet fra: https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf

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

Bergsjø, H. & Windvik, R. (2018). Datasikkerhet for ledere – *hvordan beskytte din virksomhet*. (1. utg.). Oslo: Universitetsforlaget

Bergsjø, H., Windvik, R. & Øverlier, Ø. (2020). *Digital sikkerhet – en innføring*. Oslo: Universitetsforlaget

Blaikie, N. (2010). *Designing Social Research*. (2. utg.). Cambridge: Polity

Bryman, A. (2016). *Social Research Methods*, 5.utg. Oxford: Oxford University Press.

Daler, T., Gulbrandsen, R., Høie, T., Sjølstad, T. (2019). (4. utg.) Bergen: Fagbokforlaget

Departementene. (2019). *Nasjonal strategi for digital sikkerhet.* Hentet fra: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf

Departementene. (2019). *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*. Hentet fra: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf

Direktoratet for samfunnssikkerhet og beredskap (DSB) (2016). *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Versjon 1.0. Hentet fra: https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Engen, O. A. H., Pettersen Gould, K. A., Kruke, B. I., Hempel Lindøe, P., Olsen, K. H. & Olsen, O. E. (2021). *Perspektiver på samfunnssikkerhet*. (2. utg.). Oslo: Cappelen Damm Akademisk

Johannessen, A., Christoffersen, L. & Tufte, P. A. (2020). *Forskningsmetode for økonomisk administrative fag*. (4. utg.). Oslo: Abstrakt forlag

Justis- og beredskapsdepartementet. (2017). *Risiko i et trygt samfunn – Samfunnssikkerhet*. (Meld. St. 10 (2016-2017). Hentet fra: https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/?ch=1

Jøsang, A. (2021). Informasjonssikkerhet – *Teori og praksis*. (1. utg.). Oslo: Universitetsforlaget

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. Hentet fra: https://academicjournals.org/article/article1380536009_Khan%20et%20al.pdf

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

Lain, D., Kostiainen, K., Capkun, Srdjan. (2021). *Phising in Organizations: Findings from a Large-Scale and Long-Term Study*. Switzerland: Department of Computer Science. Hentet fra: https://arxiv.org/pdf/2112.07498.pdf

Larsen, M., Lund, M. (2021). *Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review.* Hentet fra: Cyber_Risk_Perception_in_the_Maritime_Domain_A_Systematic_Literature_Review[23058430092155733 22].pdf

Meld. St. 9 (2022-2023). *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet – så åpent som mulig, så sikkert som nødvendig*. Justis og beredskapsdepartementet. Hentet fra: https://www.regjeringen.no/no/dokumenter/meld.-st.-9-20222023/id2950130/

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

Nasjonal sikkerhetsmyndighet (NSM) (2019). *Helhetlig digitalt risikobilde 2019*. Hentet fra: https://nsm.no/getfile.php/133669-1592830841/NSM/Filer/Dokumenter/Rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf

Nasjonal sikkerhetsmyndighet (NSM) (2020). *Helhetlig digitalt risikobilde 2020*. Hentet fra: https://nsm.no/getfile.php/131421-1587034764/NSM/Hermans%20undermappe%20med%20bilder/NSM_Risiko_2020_web_0104.pdf

Nasjonal sikkerhetsmyndighet (NSM) (2021). *Nasjonalt digitalt risikobilde 2021*. Hentet fra: https://nsm.no/getfile.php/137495-1635323653/NSM/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf

Nasjonal sikkerhetsmyndighet (NSM) (2023). *Risiko 2023 – Økt forutsigbarhet* krever høyere beredskap. Hentet fra: https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

Nilssen, V. (2012). *Analyse i kvalitative studier – Den skrivende forskeren*. (1. utg.). Oslo: Universitetsforlaget

Norges vassdrag- og energidirektorat (NVE). 2021. *Ekstern rapport*. https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_19.pdf

Norsk senter for informasjonssikring (NorSIS) (2016). *The Norwegian Cyber Security Culture*. Hentet fra: https://norsis.no/content/uploads/2022/05/trusler-og-trender-2016_final-c.pdf

Norsk senter for informasjonssikring (NorSIS). (2020). *Nordmenn og digital sikkerhetskultur 2020. Kommentar til årets befolkningsundersøkelse av Bjarte Malmendal*. Hentet fra: https://norsis.no/content/uploads/2022/05/Nordmenn-og-digital-sikkerhetskultur-2020-web-1.pdf

Næringslivets sikkerhetsråd (NSR) (2022). *Mørketallsundersøkelsen 2022*. Hentet fra: https://www.nsr-org.no/aktuelt/morketallsundersokelsen-2022-er-na-tilgjengelig

Nätt, T. H. & Heide, C. F. (2019). *Datasikkerhet – ikke bli svindlerens neste offer*. (2. utg.). Oslo: Gyldendal

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

Riksrevisjonen (2021) *Undersøkelse av NVEs arbeid med ikt sikkerhet i kraftforsyningen*. https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen/

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

Turner, B. A. (1978). *Man-Made disasters*. (1. utg.). London: Wykeham Science Press.

Weick, K. E. & Sutcliffe, K. M. (2015). *Managing the unexpected – Sustained Performance in a Complex World.* (3. Utg.). Hoboken, New Jersey: Wiley

Vedlegg

Vedlegg 1-Informasjonsskriv og samtykkeerklæring

Vil du delta i intervju i ett forskningsprosjektet

Cybersikkerhet i kraftbransjen

Vi tar kontakt deg for å høre om du har lyst til å delta i et forskningsprosjekt i forbindelse med ett masterstudie ved Høgskolen i Innlandet, erfaringsbasert master i offentlig ledelse og styring. I dette informasjonsskrivet, vil du få informasjon om prosjektets formål, og hva en deltakelse for deg innebærer.

Formål:
Masteroppgaven skal forsøke å belyse hva som kjennetegner den digitale sikkerhetskulturen i kraftsektoren, i møtet med de utfordringene cybertrusselen i dagens samfunn utgjør. Hensikten er å få en bredere forståelse omkring de utfordringene som kraftsektoren møter på veien i arbeidet mot en digital sikkerhetskultur. En bedre forståelse og informasjon om dette, kan være med på å bidra til bedre kunnskap, kompetanse og forbedre det digitale arbeidet i kraftsektoren.

Dette er en samfunnsvitenskapelig masteroppgave, og vi vil derfor ikke gå inn på hvilke teknologiske løsninger kraftseksjonen bruker i kampen mot cybertrusler. Med andre ord vil vi ikke gå inn på sensitive opplysninger som er taushetsbelagt med tanke på sikkerhetsteknologiske løsninger.

Vi vil se på menneskelige og organisatoriske forhold, og forsøke å kartlegge samarbeid, holdninger og bevissthet rundt digitalt sikkerhetsarbeid i kraftsektoren.

Hvem er ansvarlig for forskningsprosjektet?
Ansvarlig for prosjektet: Høgskolen i Innlandet.
Veileder: Mass Soldal Lund
Studenter: Leiv Andreas Krohn og Stian Singsaas

Hvorfor får du spørsmål om å delta?
For å innhente informasjon som er relevant i forhold til masteroppgavens problemstilling og mål, er det viktig for oss å få intervjuet fagansatte som jobber med digital sikkerhet, samt ledere som jobber eller har en sentral rolle, når det kommer til digital sikkerhet i virksomheten.

Vi har henvendt oss med samme informasjonsskriv til flere ulike kraftselskaper i Norge. Det å kunne intervjue sentrale personer fra forskjellige kraftselskaper, vil gi oss et bredt datamateriale som danner et bedre grunnlag for å kartlegge utfordringer når det kommer til cybersikkerhet i kraftbransjen.

Hva innebærer det for deg å delta?
Vi vil foreta personlig intervjuer av personer fra hvert kraftselskap som ønsker å delta.

Dersom du velger å delta, vil det innebære at du møter opp til et intervju. Intervjuet vil helst foregå personlig, men det kan også gjøres over telefon/annen digital løsning.

Intervjulengden vil være på ca. 1 time, avhengig av informasjonen som framkommer. Det vil bli tatt lydopptak av intervjuet, og det vil bli transkribert i etterkant.

Det er ønskelig å få gjennomført intervjuene i løpet raskest mulig, helst i desember/januar 2022.

Det er frivillig å delta
Det å delta i intervju, er frivillig. Du kan når som helst trekke tilbake samtykket ditt om å delta, uten å begrunne dette nærmere. Det vil ikke ha noen konsekvenser for deg, og alle dine personopplysninger vil bli slettet.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Personopplysninger og informasjon som kommer frem under intervjuene, vil bli behandlet konfidensielt og etter personvernregelverket, og kun brukes til det formålet beskrevet i dette skrivet.

Intervjuobjekt og arbeidsplass vil anonymiseres. Det eneste formålet med disse er å bruke det for oss til å skille mellom de forskjellige intervjuobjektene. Det vil ikke være mulig å spores tilbake til en person eller arbeidsgiver i selve masteroppgaven. Det vil kun være oss og veileder som vil ha tilgang til opplysningene.

Dine personopplysninger vil ikke framkomme i masteroppgaven, men de vil lagres i den hensikt å skille intervjuene fra hverandre.

Tiltak som iverksettes for å sikre at ingen uvedkommende får tilgang til personopplysningene
Personopplysninger vil bli skrevet inn i et dokument som blir lagret på en passord-beskyttet ekstern lagringsenhet.

Det vil bli gitt en unik identitet til hvert intervjuobjekt som blir lagret på eget dokument atskilt fra resten av dataene. Under skriving av masteroppgaven, vil denne identiteten bli brukt fremfor navn. Dette gjelder også arbeidsplass. Når oppgaven er ferdig skrevet, vil denne identiteten tas bort fra oppgaven. Der hvor vi eventuelt vil referere til et intervjuobjekt, vil vi benytte et pseudonym i stedet for ekte navn.

Hvert intervjuobjekt vil få sitt pseudonym, og vi vil omtale arbeidsplassen under bransjenavn, f. eks «kraftprodusent».

Lydfilene fra intervjuet vil bli lagret på en ekstern lagringsenhet som er passord-beskyttet, og som det ikke er mulig å kople til internett.

I masteroppgaven er det resultatet fra dataanalysen som blir publisert, altså de funn som er gjort. Hvilke virksomheter som har deltatt vil ikke komme frem i publikasjonen.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Når masteroppgaven avsluttes og er blitt godkjent, henholdsvis sommeren 2022, vil alt av personopplysninger og lydopptak slettes.

Dine rettigheter:
Når de deltar i forskningsprosjektet, og du kan identifiseres i datamaterialet, har du følgende rettigheter:
- rett til innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene
- rett til å få rettet personopplysninger om deg
- rett til å få slettet personopplysninger om deg
- rett til å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hva gir oss rett til å behandle personopplysninger om deg?
Vår behandling av dine personopplysninger, er basert på ditt samtykke. Gjennom Høgskolen i Innlandet har NSD (Norsk senter for forskningsdata AS), vurdert at behandlingen av personopplysningene i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Ved spørsmål om denne masteroppgaven, eller du ønsker å benytte deg av dine rettigheter, kan du ta kontakt med:
• Høgskolen i Innlandet ved veileder Mass Soldal Lund, E-post: mass.lund@inn.no
• Studenter Leiv Andre Krohn, E-post: leiv_andreas@hotmail.com og Stian Singsaas, E-post stian.singsaas@gmail.com

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

Stian Singsaas og Leiv Andreas Krohn

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Cybersikkerhet i kraftbransjen*, og jeg har fått anledning til å stille spørsmål.

Jeg samtykker til:

☐ å delta i intervju

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

- ----------
-

(Signert av prosjektdeltaker, dato)

Vedlegg 2 – Godkjenning fra NSD

Vurdering av behandling av personopplysninger

Referansenummer	Vurderingstype	Dato
611595	Standard	03.01.2023

Prosjekttittel
Masteroppgave i offentlig ledelse og styring ved HINN 2020-2023

Behandlingsansvarlig institusjon
Høgskolen i Innlandet / Handelshøgskolen Innlandet - Fakultet for økonomi og samfunnsvitenskap / Institutt for økonomifag

Prosjektansvarlig
Mass Soldal Lund

Student
Leiv Andreas Krohn

Prosjektperiode
03.08.2022 - 26.05.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 16.06.2023.

Kommentar

OM VURDERINGEN
Sikt har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

TYPE OPPLYSNINGER
Prosjektet vil behandle alminnelige kategorier av personopplysninger.

KOMMENTARER TIL INFORMASJONSSKRIVET
Informasjonsskrivet ditt mangler noen punkter loven krever er med. Du må derfor legge til disse punktene i informasjonsskrivet før du gir dette til forskningsdeltakerne dine. Du trenger ikke å laste opp den oppdaterte versjonen i meldeskjemaet:
• At du behandler opplysningene om dine forskningsdeltagere basert på deres samtykke
• Kontaktopplysninger til din institusjon sitt personvernombud
• Endre dato for prosjektslutt til sommeren 2023

FØLG DIN INSTITUSJONS RETNINGSLINJER
Vi har vurdert at du har lovlig grunnlag til å behandle personopplysningene, men husk at det er institusjonen du er ansatt/student ved som avgjør hvilke databehandlere du kan bruke og hvordan du må lagre og sikre data i ditt prosjekt. Husk å bruke leverandører som din institusjon har avtale med (f.eks. ved skylagring, nettspørreskjema, videosamtale el.)

Personverntjenester 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).

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Se våre nettsider om hvilke endringer du må melde: https://sikt.no/melde-endringar-i-meldeskjema

Intervjuguide

Innledning

Informasjon om prosjektet vårt og hvorfor vi har valgt informanten

Informasjon om innhenting av personopplysninger
- sjekke at informanten har lest og forstått informasjonen i informasjonsskrivet
- at vi tar lydopptak

Informasjon om intervjuets oppbygning
- ønske at informanten forteller så mye som mulig og at han snakker fritt

Om informanten
Kan du fortelle oss litt om din bakgrunn, hvor du er ansatt og hvilken rolle du har i virksomheten?

Hovedspørsmål

Informer om at det mest sentrale spørsmålet i intervjuet kommer tidlig fordi vi ønsker at intervjuobjektet snakker fritt om det før vi har snakket om det, og intervjuobjektet blir påvirket av spørsmål og av mine tanker og oppfatninger om temaet.

Hva mener du kjennetegner norske kraftvirksomheter arbeid når det kommer til digitalt sikkerhetsarbeid?

Digital sikkerhet i virksomheten

Begrepsavklaring
Hva legger du i begrepet digital sikkerhet?
Brukes det ett annet begrep?
Hva mener du er målet med digital sikkerhet?

Betydning av digital sikkerhet:
- Hvilken betydning har digital sikkerhet på din arbeidsplass?
- er det viktig for virksomheten drift og oppgaver å ha en god digital sikkerhet?
- hvorfor mener du det er viktig i din virksomhet?
- er man opptatt av å ha en god digital sikkerhet i virksomheten?

Uønskede hendelser og utfordringer
- Kan du fortelle oss om hvilke digitale utfordringer/trusler virksomheten deres ovenfor? Fortell gjerne om erfaringer.
- Hvilke er de mest vanligste digitale utfordringene/truslene i deres virksomhet?
- Hvilke digitale utfordringer/trusler er dere mest redd for? Hva er ytterste konsekvens?

Digital sikkerhetskultur

Organisering og ansvar:
Kan du fortelle meg hvordan dere er organisert med tanke på digital sikkerhet i virksomhetens deres?

- Hvordan er dere organisert i forhold til tradisjonell sikkerhet?

- Hvem har ansvaret for den digitale sikkerheten i deres virksomhet? Er det definerte ansvarsområder?
- Hvem har beslutningsmyndighet ved digitale sikkerhetshendelser?

Håndtering:

- Kan du fortelle oss hvordan din virksomhet jobber med digitalt sikkerhetsarbeid?
- Hva mener du er viktig for din virksomhet når det kommer til en god håndtering av digitalt sikkerhetsarbeid? Hva mener du er det viktigste forsvaret mot cybertrusler?
- Hva fungerer spesielt bra hos din virksomhet når det kommer til digital sikkerhet i deres virksomhet?
- Hvilke utfordringer møter dere på når det gjelder digital sikkerhet i virksomheten?
- Hva mener du er de svakeste faktorene når det gjelder digital sikkerhet?

Samarbeid:

- Hvordan fungerer samarbeidet om digital sikkerhet internt i virksomheten?
- Har dere samarbeid med andre organisasjoner/etater når det kommer til cybersikkerhet? Hvordan fungerer dette samarbeidet?
- Er det noen utfordringer når det kommer til samarbeid med andre?
- Hadde du ønsket mer samarbeid med andre? Hvilke, og hvorfor?

Menneskelige faktoren:

- Hva tenker du om den menneskelige faktoren når det gjelder digital sikkerhet i deres virksomhet? (altså menneskelig svikt, naivitet etc?

Ansattes ved virksomheten:

- Hvordan opplever du holdningene til de ansatte ved virksomheten når det kommer til digital sikkerhet? Går det utover den digitale sikkerheten?
- Hvordan sikrer dere at ansatte er bevisst egen og andres rolle når det kommer til digital sikkerhet?
- Hvordan jobber dere for å få en bedre bevisstgjøring og forståelse av digital sikkerhet hos de ansatte?
- Er det noen utfordringer med dette?

Ledelsen ved virksomheten:

- Hvilken betydning har ledelsen for virksomhetens digitale sikkerhet?
- Hvordan er ledelsens holdning til digital sikkerhet ved din virksomhet? Er ledelsen opptatt av digital sikkerhet? Har de fokus og strategier for digital sikkerhet?
- Hva mener du er viktig for å påvirke ledelsens holdninger til digital sikkerhet?

Beredskapsplaner, instrukser og tiltak:

- Kan du fortelle oss om beredskapsplaner, instrukser og tiltak dere har i virksomheten når det kommer til digital sikkerhet?
- Har dere beredskapsplaner for digital sikkerhet? Hvorfor/hvorfor ikke? Evnt. hvilke?

- Har dere instrukser som omfatter digital sikkerhet?
- Hvem har ansvaret for å utarbeide planer og instrukser for dette?
- Hvilke tiltak har dere i virksomheten mot digitale trusler, og hvordan evalueres disse?

Varsling

- Hvordan oppdages feil, avvik og uønskede hendelser innen digital sikkerhet i deres virksomhet?
- Er det ett system for rapportering, læring og tilbakemeldinger?
- Hvem følger opp dette, og hvordan gjøres det?
- Er det en kultur for å varsle i din virksomhet? (redd for å si ifra, flau over sin handling etc?)
- Er det fokus på læring?
- Er det noe utfordringer knyttet til dette?

Opplæring og øvelser

- Gjennomføres det opplæring i digital sikkerhet på din arbeidsplass? På hvilken måte? Hvem har ansvar for dette?
- Gjennomføres det øvelser innenfor dette feltet? Hvordan og hvilke?
- Hvordan evalueres dette? Ser dere en positiv effekt av dette?

Avsluttende spørsmål

Ut fra det vi har snakket om, er det annen informasjon, andre synspunkter eller noe du ønsker å tilføye?

Har du noen avsluttende tanker om forskningsprosjektet som du ønsker å dele?

Er det i orden om jeg kontakter deg igjen dersom jeg har oppfølgingsspørsmål eller behov for å oppklare noe?