Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk

Ingvild Kvamme

# Digital sikkerhet:

## Hvordan jobbes det fra ledelsens side med prosedyrer og bevissthet i selskapet?

Masteroppgave i Operativ Maritim Ledelse
Veileder: Marte Fanneløb Giskeødegård
Desember 2023

NTNU
Kunnskap for en bedre verden

Ingvild Kvamme

# Digital sikkerhet:

## Hvordan jobbes det fra ledelsens side med prosedyrer og bevissthet i selskapet?

Masteroppgave i Operativ Maritim Ledelse
Veileder: Marte Fanneløb Giskeødegård
Desember 2023

Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk

NTNU
Kunnskap for en bedre verden

# SAMMENDRAG

Denne masteroppgaven tar for seg hvordan det arbeides med digital sikkerhet hos et selskap i den maritime næringen. Problemstillingen tar for seg hvordan det arbeides fra ledelsens side med prosedyrer og bevissthet rundt digital sikkerhet i selskapet. Det har blitt gjennomført seks kvalitative intervju med ledere i selskapet, funnene som kommer frem blir presenter i empiri og blir i drøfting sett på opp mot den relevante teori som er blitt vektlagt i denne masteroppgaven.

For å besvare problemstillingen har det blitt tatt utgangspunkt i organisasjonsanalyse, med pentagonmodellen, for å behandle funnene. For å besvare problemstillingen har en sett på følgende forskingsspørsmål:

- Hva legges i digital sikkerhet, sett fra ledelsens perspektiv?
- Hvordan er den formelle strukturen til selskapet?
- Hvordan arbeides det med standarder og teknologi fra ledelsen sin side?
- Hvordan arbeides det med bevissthet av digital sikkerhet fra ledelsens side?
- Hvordan oppleves sikkerhetskulturen av ledelsen?

De ansatte er en viktig brikke i arbeidet med digital sikkerhet og deres bevissthet og forståelse er avgjørende for å ha en god sikkerhetskultur i selskapet. Selskapet har stort fokus på digital sikkerhet, det oppfattes å være godt etablert hos ledelsen, men nedover i organisasjonen ser en at arbeidsoppgaver som oppleves å bringe selskapet fremover prioriteres fremfor arbeid med digital sikkerhet.

Selskapet arbeider med å øke bevisstheten til de ansatte, det vises til opplæring i form av simuleringer, kurs og presentasjoner for å øke de ansattes kunnskap om digital sikkerhet slik at de er bedre rustet til å håndtere digital sikkerhet risikoer de møter i hverdagen. Blant annet ser en på simuleringer av mistenkelig e-post, som gjennomføres av selskapet, at en etter flere runder med slike tester merker at tallet på de som lar seg lure er gått ned, men at det fremdeles er en vei å gå for å komme dit en ønsker å være. En er aldri sterkere enn det svakeste ledd, og det er noe en kontinuerlig må arbeide med for å styrke.

Det kommer frem at det ikke er definerte prosedyrer i selskapet når det gjelder digital sikkerhet, men at det er retningslinjer og anbefalinger, i tillegg til at noen programvarer er med på å påvirke hvordan de ansatte forholder seg til digital sikkerhet i hverdagen.

# ABSTRACT

This master's thesis addresses how digital security is managed within a company in the maritime industry. The research question investigates how the management deals with procedures and awareness around digital security in the company. Six qualitative interviews with company leaders have been conducted, with the findings presented in the empirical data and discussed in light of the relevant theory emphasized in this thesis.

To answer the research question, organizational analysis, with the pentagon model, was used to process the findings. The following research questions were examined:

- What is understood by digital security from the management's perspective?
- What is the formal structure of the company?
- How does management work with standards and technology?
- How does management work to raise awareness of digital security?
- How is the security culture perceived by the management?

Employees play a vital role in digital security efforts, and their awareness and understanding are crucial for a robust security culture within the company. The company has a strong focus on digital security, which seems to be well-established at the management level, but further down the organization, tasks perceived as advancing the company are often prioritized over digital security efforts.

The company endeavors to increase employee awareness, pointing to training in the form of simulations, courses, and presentations to enhance their knowledge of digital security, better preparing them to handle digital security risks encountered in their daily routines. For instance, after several rounds of simulated phishing email tests conducted by the company, there has been a noticeable decrease in the number of employees who fall for these scams, though there is still progress to be made to reach the desired level of awareness. A chain is only as strong as its weakest link, and there is a constant need for work to strengthen this area.

It is revealed that there are no defined procedures in the company concerning digital security, but guidelines and recommendations exist. Additionally, some software influences how employees deal with digital security in their day-to-day activities.

# FORORD

Denne masteroppgaven er det avsluttende arbeidet i mastergradprogrammet «Operativ maritim ledelse» ved NTNU i Ålesund.

Det sitter klart i minne, det en av mine tidligere forelesere en gang sa; Når du velger tema for masteroppgaven, så er det som at du går inn i et forhold. Du velger en partner du er interessert i og som du har lyst å bli bedre kjent med. I det du går inn i forholdet vet du at dere skal tilbringe mye tid sammen, både på godt og vondt. Som alle forhold, har også denne oppgaven hatt sine opp- og nedturer, men med en spennende og dagsaktuell tematikk er det vanskelig å ikke la seg rive med. Det har vært en lærerik prosess å planlegge og gjennomføre dette studiet, og jeg legger ikke skjul på at det har vært utfordrende å kombinere studie med å være i full jobb.

Jeg ønsker å rette min takknemlighet til deltakerne som stilte til intervju og delte sine erfaringer med meg. Videre ønsker jeg å rette en stor takk til min veileder, Marte Fanneløb Giskeødegård, for støtte, gode råd og konstruktive tilbakemeldinger som har hjulpet meg på rett vei mot mål.

Da jeg startet på denne reisen i 2020, møtte jeg opp sammen med min gode venninne, Mariann. Det er gledelig at vi nå sammen krysser målstreken og jeg er utrolig takknemlig for dele dette med akkurat deg!

De du har rundt deg spiller en stor rolle i livet ditt, enten det er familie, venner eller kollegaer, så til alle dere: takk for den støtten og oppmuntringen dere har vist meg gjennom dette studiet, det har betydd mer enn dere kan tenke dere til! Ikke minst til min kjære samboer Simon, uten deg hadde det ikke gått, jeg er heldig som har deg!

Nå er det er bare å kaste seg hodestups ut i det!

God lesing!

*Ingvild Kvamme, 18.desember 2023*

*"You almost never get only get what you expect and sometimes you do not even get that. »*

*(Barley, 2020, s. 26)*

# INNHOLD

# FIGURER

# FORKORTELSER/SYMBOLER

| | |
|---|---|
| BU | Business Unit |
| CEO | Chief Executive Officer |
| CFO | Chief Financial Officer |
| HR | Chief Human Resources Officer |
| COO | Chief Operating Officer |
| HMS | Helse Miljø og Sikkerhet |
| HR | Human Resources |
| IKT | Informasjons- og kommunikasjonsteknologi. |
| IT | Informasjonsteknologi |
| NDLA | Nasjonal digital læringsarena |
| NITO | Norges ingeniør- og teknologiorganisasjon |
| NTNU | Norges teknisk-naturvitenskapelige universitet |
| SNL | Store norske leksikon |
| TQM | Total Quality Management |
| VP | Vice President |

# 1 INNLEDNING

I en tid hvor den digitale revolusjonen bringer med seg flere fordeler, observeres det samtidig at det globale trusselbildet innen digital sikkerhet har tilspisset seg betraktelig. Teknologi som forenkler hverdagen medfører en paradoksal utvikling ved at den også åpner for nye risikoer og sårbarheter. En ser til stadighet artikler med advarsler om nye svindelmetoder som hackere tar i bruk. Som et ledd i å bevisstgjøre den norske befolkningen viser det nå reklamevidoer av hvordan hackere enkelt kan ta i bruk ny teknologi for å lure en. Bak disse reklamevideoene finner en telekommunikasjons- og nettverksleverandører, som tilbyr sikkerhetsløsninger til sine kunder for å minske sannsynligheten for at det skal ramme dem. Selv om de viser til gode sikkerhetsbarrierer, må en ikke glemme menneskets rolle i det store bilde. En kan ha de beste systemene for å beskytte seg selv, som person eller selskap, men en brikke en ikke styrer er mennesket og valgene de tar.

I den årlige risikorapporten fra Nasjonal Sikkerhetsmyndighet for 2023 fremkommer det at sikkerhetslandskapet i dagens samfunn er mer uforutsigbart enn det har vært på lenge. Det vises til at denne uforutsigbarheten antagelig vil vedvare i årene fremover. Rapporten understreker sårbarheten selv godt sikrede virksomheter har gjennom underleverandørers svakheter. NSM påpeker:

> *«Selv om en virksomhet har god fysisk og digital sikkerhet, så kan trusselaktører utnytte underleverandører som er langt dårligere sikret for å få tilgang til sine egentlige mål. Dette gjør at vi også må sikre oss godt på flankene.» (Nasjonal sikkerhetsmyndighet, 2023, s. 9)*

Rapporten tar også opp de økonomiske utfordringene som rammer flere og flere, ikke bare den enkeltes privatøkonomi, men også at flere norske bedrifter merker at skoen trykker ekstra når det kommer til økonomi. I slike situasjoner risikerer en at noen selskap nedprioriterer den digitale sikkerheten, dette er sårbarheter som trusselaktører vet å utnytte.

> *«Sikkerheten vår blir ikke bedre enn det svakeste leddet i leverandørkjeden.» (Nasjonal sikkerhetsmyndighet, 2023, s. 9)*

Teknologiske sprang bidrar til effektivisering og enklere hverdagsprosesser, men medfører samtidig økt digital sårbarhet – en utvikling som trusselaktører er raske til å utnytte. Dette er en

utvikling som ingen er skjermet fra, hverken myndighet, den enkelte eller virksomheter (Nasjonal sikkerhetsmyndighet, 2023).


*Figur 1 - "Unge er dårligst på IKT-sikkerhet" - utklipp fra artikkel på nettstedet digi.no (digi, 2023).*

I forbindelse med nasjonal sikkerhetsmåned i 2022 publiserte fagorganisasjonen NITO (Norges ingeniør- og teknologiorganisasjon) en artikkel om informasjons- og kommunikasjonsteknologi (IKT) sikkerhet på sine hjemmesider med følgende overskrift «Unge er dårligst på IKT - sikkerhet» (NITO, 2022).

I februar 2023 ble denne artikkelen igjen publisert, med samme overskrift, men denne gangen på digi.no sine nettsider (digi, 2023). Digi.no er Norges største nisjepublikasjon rettet mot den norske informasjonsteknologi (IT) bransjen. I artikkelen «Unge er dårligst på IKT-sikkerhet» kommer det frem at i en undersøkelse, gjennomført av Norstat på vegne for fagorganisasjonen NITO, at omtrent halvparten av Norges befolkning ikke følger ekspertenes råd, men at verst ut er de i aldersgruppen 15-29 år, hvorav 62% ikke følger ekspertenes råd. På en annen måte kan en da si at 2 av 3 ungdommer er derfor ekstra utsatt for å få data på avveie som følger av hacking (digi, 2023). NITO sin president, Trond Markussen (Figur 1) uttaler i saken at dette er svært bekymringsfullt.

## 1.1 Problemstilling

I denne masteroppgaven blir følgende problemstilling belyst:

*Hvordan jobbes det fra ledelsens side med prosedyrer og bevissthet rundt digital sikkerhet i selskapet*?

En vil her gjøre en organisasjonsanalyse, der følgende forskningsspørsmål vil være med å belyse problemstillingen:

- Hva legges i digital sikkerhet, sett fra ledelsens side?
- Hvordan er den formelle strukturen til selskapet?
- Hvordan arbeides det med standarder og teknologi fra ledelsen sin side?
- Hvordan arbeides det med bevissthet av digital sikkerhet fra ledelsens side?
- Hvordan oppleves sikkerhetskulturen av ledelsen?

Målet er å få et helhetlig bilde av hvordan ledelsen ser på digital sikkerhet og hvordan de i hverdagen jobber med prosedyrer og bevisstgjøring. Gjennom kvalitativ datainnsamling, vil en innhente erfaringer fra seks ledere i et selskap innenfor den maritime næringen. Ønsket er at masteroppgaven vil kunne bidra til det eksisterende kunnskapsgrunnlaget om digital sikkerhet i selskapet og komme med innsikt som kva være av verdi både for selskapet som stiller opp, men også for teori og praksis innenfor feltet.

## 1.2 Avgrensninger

En har i denne masteroppgaven gjennomført en kvalitativ datainnsamling hos et selskap innenfor den maritime næringen i Norge. Med bakgrunn i at en vil se på hvordan det jobbes med prosedyrer og bevissthet rundt digital sikkerhet anses dette som en fornuftig avgrensning for å få et resultat som viser hvordan et konkret selskap jobber med dette.

En forenkling som er blitt gjort er at alle deltakerne vil henvises til som «han», men at det ikke nødvendigvis stemmer overens med identiteten til den det henvises til.

Da det både i intervju og litteratur kommer frem ulike måter å vise til digital sikkerhet, vil også begrep som datasikkerhet, IKT-sikkerhet og IT-sikkerhet brukes gjennom oppgaven.

## 1.3 Rapportens oppbygging

Rapportens oppbygging videre er som følger:

**Kapittel 1** innledning med introduksjon til oppgaven, bakgrunn for valget og dens problemstilling, samt de avgrensninger som er gjort.

**Kapittel 2** her presenteres det relevant teori; digital sikkerhet og organisasjonsanalyse

**Kapittel 3** her er valgt metode beskrevet, inkludert planlegging, utvalg mm.

**Kapittel 4** her vil de empiriske funnene bli presentert

**Kapittel 5** her drøftes de funnene som kommer frem i empiri opp mot relevant litteratur

**Kapittel 6** kortfattet oppsummering, samt tanker om masteroppgaven og veien videre

**Kapittel 7** referanser brukt i rapporten

**Kapittel 8** vedlegg til rapporten

# 2 TEORI

I dette teorikapittelet retter en blikket mot organisasjonsanalyse, med vekt på digital sikkerhet. Digital sikkerhet er ikke bare en teknisk bekymring, men er en integrert del av de strategiske beslutningene som tas og kulturelle praksiser. I dag står en ovenfor mange utfordringer knyttet til cybertrusler og teknologiske endringer. Teorien som er vektlagt her er den som knyttes til masteroppgavens problemstilling om hvordan det jobbes med digital sikkerhet, sett i lys av prosedyrer og kommunikasjon, fra ledelsen sin side. Som Barley (2020) sier om teknologisk endring:

> *«You almost never get only get what you expect and sometimes you do not even get that. » (Barley, 2020, s. 26)*

I teorien er nøkkelord: digital sikkerhet, organisasjonsanalyse, teknologi og menneske.

## 2.1 Digital sikkerhet

Noen ganger opplever en at flere forskjellige begreper, som har mer eller mindre samme betydning, brukes om det samme. Dette kan være forvirrende. I det daglige hører en gjerne følgende begreper om hverandre: cybersikkerhet, informasjonssikkerhet, datasikkerhet, IT -sikkerhet, IKT-sikkerhet og digital sikkerhet. Som Jøsang (2021) tar opp i sin bok «Informasjonssikkerhet» har tiden en lever i noe å si for hvilke begreper som er mest populær. Helt siden 1980-taller har *datasikkerhet* vært et mye brukt uttrykk, i 2010 var det *cybersikkerhet* som dukket opp med det ble den populære terminologien. I 2019 valgte norske myndigheter å skape et samlebegrep for begrepene som cybersikkerhet og datasikkerhet og det var da *digital sikkerhet* ble skapt (Jøsang, 2021). En skal nok lete lenge etter en arbeidsplass eller et hjem i dag som ikke er avhengig av IKT -systemer (Bergsjø & Windvik, 2020).

> *«Sikkerhet kan defineres som en tilstand; fravær av uønskede hendelser eller frihet fra fare og frykt. Denne tilstanden er imidlertid ikke statisk, men påvirkes av endringer i faktorer som trussel og farer, sårbarhet og verdi.» (Store norske leksikon, 2023)*

En vil i praksis ikke være helt uten uønskede hendelser, frykt og fare, men det en ønsker å oppnå er at disse er redusert til et nivå en kan si er akseptabelt (Bergsjø & Windvik, 2020).

Datasikkerhet handler om sikkerhet sett opp mot uønskede hendelser i eller gjennom datasystemer (Bergsjø & Windvik, 2018). Noen uønskede hendelser kan være at noen andre har tilsiktede handlinger som de ønsker å påføre virksomheten, da i all hovedsak med negativ konsekvens. Eksempler på dette kan oppsummeres med fire S'er: sabotasje, svindel, spionasje eller sverting (Bergsjø & Windvik, 2018).

I boken «Datasikkerhet for ledere – hvordan beskytte din virksomhet» av Bergsjø og Windvik (2018) beskriver de hvorfor de ønsket å skrive en bok om datasikkerhet for ledere. En av årsakene er at nøkkelen til god datasikkerhet ligger i styringen og gjennomføringen av sikkerhetsarbeidet. Med referanse til NSM sin risikorapport fra 2017 viser de til at det i flere år har vært manglende planlegging, styring og gjennomføring av sikkerhetsarbeid i norske virksomheter. Bergsjø og Windvik (2018) forklarer at for å ha god styring og gjennomføring så må det være forankret i ledelsen og styret. De mener et viktig steg på veien for å bedre dette er bevisstgjøring og handling.

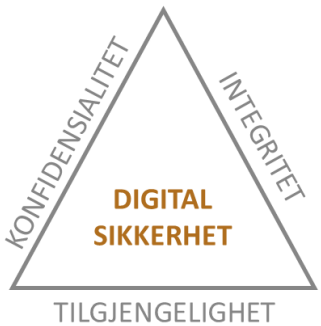
Bjørnsen (2012) omtaler ulike tidsepoker når det kommer til IKT og hvordan tilstedeværelsen fra ledere og styre i selskaper har vært i de ulike epokene. Han viser til at i noen perioder så har ikke ledelsen deltatt aktivt i det som angår IKT og latt IT-driften ta seg av dette. Han viser til at en, altså i 2012 da boken var utgitt, var inne i det tredje tideverv og at det er igjen viktig at toppledelsen og eventuelt styre er med å ha kontroll. Han så fremdeles en god del ledere og styremedlemmer som ikke så behovet for at dette skulle løftes høyere på agendaen. Årsaken til at han mener dette er viktig nå er det faktum at informasjon kan komme på avveie og ruinere en virksomhet og at dette kan skyldes ubetenksomhet ho en enkelt ansatt, eller at det kan være en bevisst handling. Innen ledelse for datasikkerhet viser også Bergsjø og Windvik (2018) til at det ikke lenger er tilstrekkelig med egne sikkerhetsavdelinger som jobber med temaet. De viser til at de som i det daglige jobber med medarbeiderne må ta hovedansvaret for å forebygge og avdekke innsidetrusler, i dette tilfelle vil det si avdelingsledere.

For å kunne mene noe om risiko rundt digital sikkerhet trenger en å ha noe kunnskap i bunn. Bergsjø og Windvik (2020) viser til følgende komponenter er knyttet sammen: kompetanse, læring og risikooppfattelse. Som ansatt må en ha mulig kompetanse om digital sikkerhet for å forstå de mulige risikoene en utsettes for. For hackere er en av de viktigste kanalene for å komme inn på datamaskiner på norske arbeidsplasser gjennom ondsinnede vedlegg eller lenker i e-poster. Det er ikke nok å bare vite om risikoen, en må ha forståelse for hvor ofte slike e-poster prøver å gjøre skade og hva det er som kjennetegner disse. Dette for at de ansatte skal

kunne gjøre de nødvendige vurderingene, her vist til som de riktige vurderingene. De legger også til at ens væremåte også er med på å påvirke oppfattelsen. Det kan være selskap har ansatte som har vært gjennom noe lignende tidligere i arbeidslivet og av den grunn er mer observant og utøver større forsiktighet. Noen personer er forsiktige av natur, mens andre er spenningssøkere, sistnevnte kan gjerne tenke at det meste går bra eller at «det skjer ikke meg». Andre kan mene at grunnet høy interesse og kompetanse på området så er det lite sannsynlig at de selv går i fellen. I boken «Digital sikkerhet – en innføring» viser Bergsjø og Windvik (2020) til en studie gjort i 1995, av Kreuter & Stecher, som legger frem at det hos mennesker som man mener har mye kompetanse eller ferdigheter finners en økt risikoatferd.

En har de siste årene sett at direktørsvindel er noe som har hatt en økning. Med direktørsvindel sikter en til hackere som utgir seg for være direktør i selskapet. Da dette startet var det gjerne en e-post på engelsk eller dårlig norsk som ble sendt til økonomiansvarlig. En slik e-post var laget slik at det skulle se ut som det tilsynelatende kom fra direktøren, altså noen med autoritet, der den såkalte direktøren ber om en hasteoverføring eller at en regning måtte betales. Selv om språk og betalingskonto i utlandet gjorde at en lærte seg at dette var svindel, var det likevel noen som ble lurt. Hackerne blir også smartere, og direktørsvindel finnes enda. Nå er e-posten på godt norsk, enten fordi det er nordmenn som står bak eller at det er noen som er god i språket og de har norske utbetalingskontoer. Disse kontoene er enten til et falskt firma eller til en norsk person. Hackerne vet nå å utnytte de naive eller de som trenger raske penger, og kan derfor bruke norske kontoer og få noen av disse til å gjøre overføringen til utlandet. Med dette utsetter ikke hackeren seg selv for noen risiko, men sette andre i den i stedet da det å flytte penger uten å vite hvor de kommer fra eller hva de er for er en ulovlig aktivitet (Bergsjø & Windvik, 2020).

Innenfor datasikkerhet er det tre prinsipper som vektlegges; konfidensialitet, integritet og tilgjengelighet. Disse oppsummeres i KIT trekanten (Jøsang, 2021), gjengitt i Figur 2. Når en ser til informasjonssikkerhet, er noe av det første en tenker konfidensialitet. Dette er noe både selskap og privatpersoner er opptatt av. I ISO/IEC 27000 finner en følgende definisjon på konfidensialitet:



*Figur 2 KIT trekanten (Jøsang, 2021)*

> *«Property that information is not made available or disclosed to unauthorized individuals, entities or processes» (Standard Norge, 2018, s. 3.10)*

Begrepet konfidensielt blir meningsløst dersom det er uklart hvem det er som er autorisert eller ikke. Det er derfor verdt å merke seg spesifiseringen av «uautoriserte» i det overnevnte sitatet.

Det er ikke bare forretningshemmeligheter som er konfidensielle; all data som ikke er offentlig tilgjengelig er konfidensiell. Hvis en aktør er interessert i hvilke mulige prosjekt et selskap jobber med, kan det være aktøren ønsker å spionere for å sabotere, det er nemlig mulig aktøren ønsker å vinne kontrakten selv. En annen måte spionasje kan være skadelig på, er dersom aktøren får innsikt i hvordan virksomhetens viktigste maskin opereres. Dersom aktøren kan tukle med hvordan maskinen jobber, vil det kunne sette virksomheten ut av drift til de klarer å rette opp i feilen (Bergsjø & Windvik, 2018).

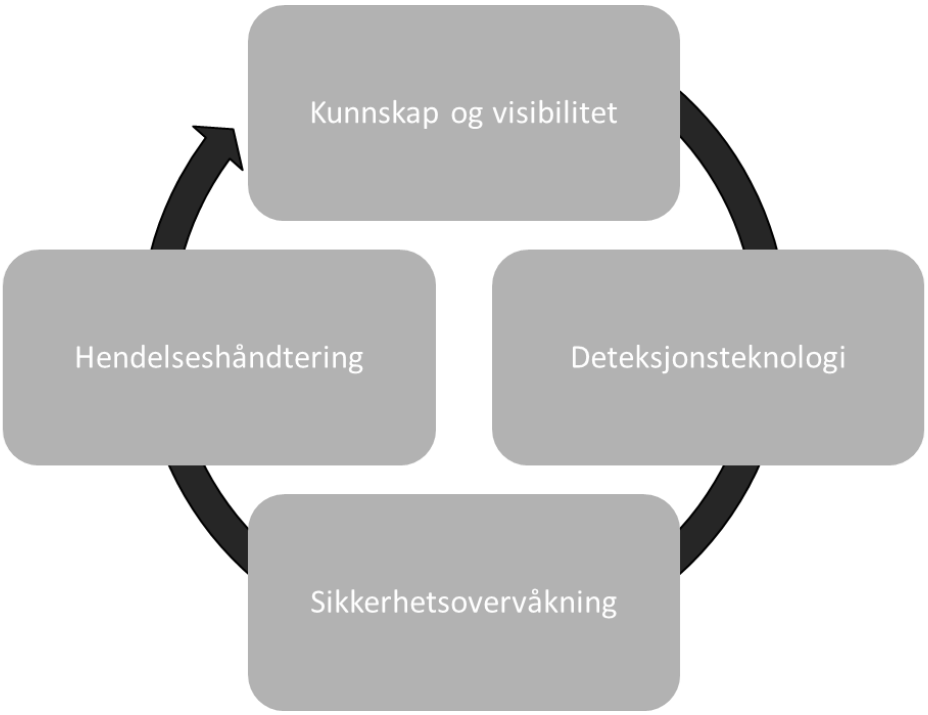
Ser en videre på sabotasje kommer en også inn på selskapets integritet, da hackerne må klare å komme seg forbi systemets sikkerhetsbarrierer. Innen digital sikkerhet viser integritet til at data er beskyttet mot uautoriserte endringer eller manipulasjon. Dataintegritet sikrer at data forblir nøyaktig, hel og uendret. Integritet omhandler alle typer data. Sabotasje i form av integritet krever stort sett inngående kjennskap til virksomhetens sine systemer, for eksempel så kan personer med uautorisert tilgang endre på anbud eller innkomne e-poster (Bergsjø & Windvik, 2018).

I de senere årene har det vært flere saker om virksomheter som har mistet tilgang til sine data som et direkte resultat av dataangrep. Enten ved at dokumenter er slettet eller blitt kryptert. I noen tilfeller kan en få tilbake data etter en har betalt løsepenger, men det er dessverre ikke alltid en får filene tilbake selv om en betaler løsepenger. Det er flere metoder på markedet som gjør at filer som er kryptert ikke kan dekrypteres etterpå, de er da altså tapt. Metoder som dette er hvorfor det er viktig, for privatpersoner og virksomheter, å ha sikkerhetskopier av viktige dokumenter, slik at de ikke går tapt for alltid dersom en skulle bli utsatt for et dataangrep. Ved å ha sikkerhetskopi, er det større mulighet for å få dokumentene tilbake et slikt angrep, enn om ikke (Bergsjø & Windvik, 2018).

> *«Arbeidet med sikkerhet handler om å beskytte noe som er verdifullt. Tap av disse kan gi negative konsekvenser, ikke bare for virksomheten selv, men også andre interessenter.» (Nasjonal Sikkerhetsmyndighet, 2020)*

En måte å jobbe med digital sikkerhet er gjennom å overvåke trafikk. Bergsjø og Windvik (2020) viser til sikkerhetshjulet når de snakker om hvordan en må overvåke verdiene for å kunne ha en hendelse å håndtere (Figur 3). For å kunne drive med overvåkning er en avhengig

av deteksjonsteknologi som gjør dette mulig. Det å ha kunnskap om de aktuelle truslene, sårbarhetene, samt en klar definisjon av selskapets digitale verdier, er avgjørende for å kunne velge rett teknologi. Sirkelen er en evig syklus, der en vil få mer kunnskap og visibilitet, til å for eksempel velge rett teknologi, ved å ta til seg kunnskap av de hendelsene som har blitt håndtert.

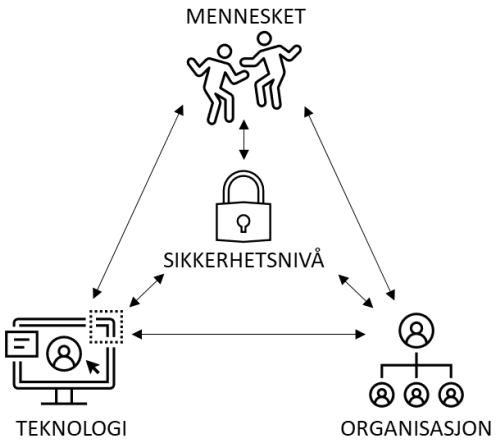



*Figur 3 Sikkerhetshjulet (Bergsjø & Windvik, 2020)*

Ikke alle delene i sikkerhetshjulet vil bli belyst, men temaer som sikkerhetsovervåkning og deteksjon av uautorisert tilgang er relevant å ta med videre. Bergsjø og Windvik (2020) viser til at med sikkerhetsovervåkning kommer det også utfordringer. Det at alarmer går av er kun en indikasjon på at det er et datainnbrudd, men det gir ikke det fullstendige bilde over situasjonen. Noen datainnbrudd kan være umiddelbart gjenkjennelige, mens andre kan være så små og kompleks at det kreves spisskompetanse innen feltet for å kunne oppdage den. I tillegg så kan informasjonen en får ut være både mangelfull og feilaktig, noe som ytterligere vanskeliggjør prosessen med å avdekke inntrengningen.  Det er mange årsaker til at alarmen kan gå av, deriblant finner en også de som skyldes helt andre ting enn et datainnbrudd. Det kan være konfigurasjonsfeil eller andre driftsproblemer som utløser alarmen, og det er nettopp slike indikatorer som skaper støy og gjør det vanskelig å drive med sikkerhetsovervåkning.

## 2.2 Organisasjonsanalyse

Det å forstå organisasjoner er interessant for mange. Det er interessant både for de som har lederroller, men også de som har andre roller i organisasjonen. I tillegg kan det også være av interesse til de som er rundt organisasjonen. For å lykkes med organisasjonsutvikling er det essensielt å ha inngående kunnskap om hvordan organisasjoner fungerer, ettersom forståelsen er grunnlaget for å forbedre utnyttelsen av ressurser og prestasjoner (Schiefloe, 2021).




*Figur 4 - MTO - Mennesket, teknologi og organisasjon, sammenhengene illustrert basert på Schiefloe (2017)*

Et begrep som favner om både tekniske, menneskelige og organisatoriske faktorer er sikkerhetsledelse. Alle disse faktorene er med relevant når en ser på sikkerhet, som illustrert i Figur 4 (Schiefloe, 2017).

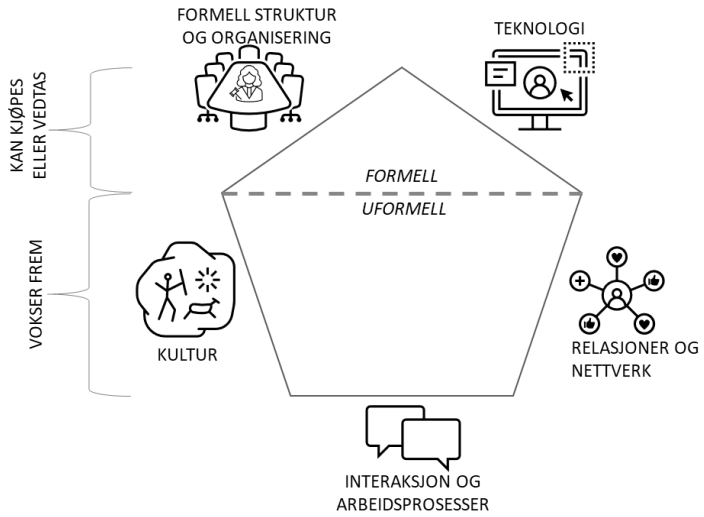
Om en starter med å se på teknologi, så kan en vise til minst to grunner til at dette er viktig. Den første er at en er avhengig av å ha teknologi som er pålitelig, da både som barrierer, men også for den operasjonelle driften av organisasjonen. Det at teknologien er pålitelig er noe som er avgjørende. Dette innebærer også at en har tilstrekkelig kapasitet og at systemet er satt opp slik at en har redundans for de systemene som har kritiske funksjoner. For det andre må teknologien gi de ansatte sikkerhet (Schiefloe, 2017). Dersom det skjer en teknologisk svikt, kan det føre til svært alvorlige hendelser. Schiefloe (2017) viser til at selv om teknologien kan svikte, så er det ytterst få ganger at det er den eneste forklaringen til hvorfor ulykken oppstod.

Dette fører diskusjonen over på den neste faktoren, mennesket. Schiefloe (2017) viser til at i de aller fleste granskninger av ulykker trekkes menneskelig svikt frem som en av de viktigste, om ikke den eneste, medvirkende årsakene til hendelsene. For å oppnå tilstrekkelig med sikkerhet spiller mennesket inn, med tanke på hvordan de opererer, handler eller forholder seg til situasjoner. En sier at menneskelig svikt kan oppsummeres i fire hovedtyper: feilvurdering, feilhandling, utelatelser eller koordineringsfeil. Til tross for at hvordan mennesket handler, eller ikke handler, kan være den siste og utløsende faktoren for uønskede hendelser, så vises det til at det som oftest er andre bakenforliggende forklaringer på hvordan en slik menneskelig svikt kunne skje. Det som da kommer frem, kan være forhold som går på konteksten handlingene skjer innenfor og en ser da mot funksjonen til organisasjonen (Schiefloe, 2017).

Når en skal gjøre en organisasjonsanalyse, kommer det godt med at det finnes analytiske hjelpemiddel for å sortere og tolke data. Disse vil nå bli sett nærmere på.

### 2.2.1 Pentagonmodellen

Ofte kan problemstillinger en står ovenfor i en organisasjon være sammensatte og uoversiktlige. Gassutblåsningen som var på Snorre A i 2004 er et eksempel som trekkes frem innen organisasjonsanalyse. I etterkant av gassutblåsningen var det behov for omfattende datainnsamling og det ble da klart at det ikke var noen enkeltfaktorer som alene forklarte hva som var årsaken til at denne gassutblåsningen skjedde. Det var små marginer om å gjøre for at denne hendelsen kunne endt med en omfattende menneskelig, økonomisk og miljømessig katastrofe (Schiefloe, 2021). Da de i etterkant jobbet med datainnsamlingen kom det frem at det var nødvendig å utvikle en modell for å kunne forstå, samt formidle, alle faktorene som ikke bare spilte inn, men som spilte sammen. Det var denne gassutblåsningen som la grunnlaget for det en i dag kjenner som pentagonmodellen. Faktorene som spilte inn på Snorre A gassutblåsningen var: organisatoriske endringer, arbeidsvaner, ledelse, kultur, relasjoner, tidspress og teknisk tilstand (Schiefloe, 2021).



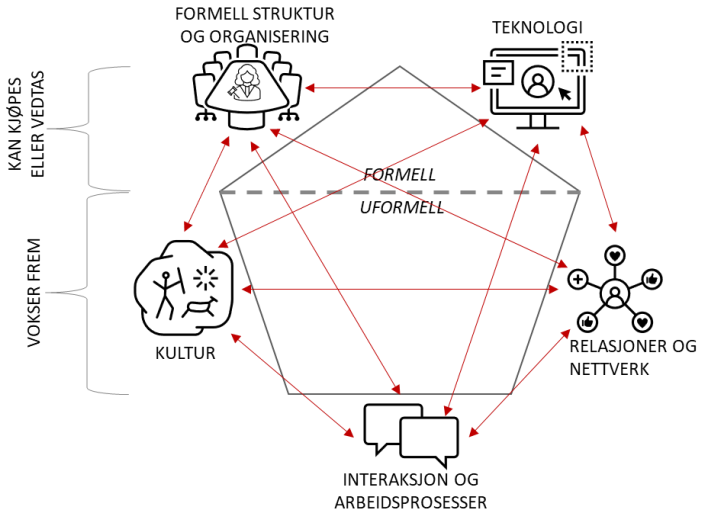

*Figur 5 Pentagonmodellen, illustrert basert på beskrivelsene til Schiefloe (2021)*

Pentagonmodellen (Figur 5), som av navnet er utformet som en pentagon, er bestående av fem like sider og fem like vinkler, hvor hver side representerer en av de fem hovedkategoriene: formell struktur, teknologi, kultur, interaksjon og relasjoner. Basert på forskingsresultat er det disse fem hovedkategoriene som har vist seg å være sentrale forklaringsfaktorer (Schiefloe, 2021). Pentagonmodellen kan også deles i det som kan kjøpes/vedtas og det som vokser frem. På en enklere måte kan en si det formelle og det uformelle. Det er viktig å presisere at

pentagonmodellen er ikke en teori, det er derimot et analytisk hjelpemiddel for å analysere organisasjoner som et system. Ved bruk av de fem hovedkategoriene kan pentagonmodellen brukes til å sortere og klassifisere data, og en kan trekke linjer mellom de ulike kategoriene (Schiefloe, 2021)

Det å se ulike perspektiv handler kan en trekke mot innramming og meningsdanning. En kan si at innramming er de begreper og antagelser som personer benytter seg av for å forstå, beskrive og kommunisere rundt en bestemt virkelighet, dette basert på hva personen selv ser som relevant når en må forholde seg til store mengder med informasjon, sanseinntrykk og observasjoner som er rundt oss. Meningsdanning kan kort oppsummeres som prosess der en bruker det en har erfart tidligere til å lage prognoser og meninger om det som kommer. Alle mennesker danner seg et rammeverk basert på erfaringer for å kunne forstå, forklare eller forutsi. Med dette settes det en hører, leser og observerer inn en sammenheng. En kan si at meningsdanning som en prosess er både framoverskuende, men også tilbakeskuende. En kan oppsummere innramming og meningsdanning som at innramming bestemmer hva som er viktig og hvordan informasjonen en har skal tolkes. Meningsdanning setter den spesifikke informasjonen inn i den aktuelle rammen (Schiefloe, 2021).

Når en ser på en organisasjons egenskaper, beveger en seg inn i de interne forholdene. Innenfor de interne forholdene har en to viktige skiller: det formelle og det uformelle. Det formelle viser en gjerne til som det en kan kjøpe eller designe. En deler det formelle inn i to kategorier. Den første er organisasjonens formelle struktur. Her finner en blant annet prosedyrer, regler og organisasjonskart. I den andre finner en organisasjonens teknologi, herunder finner en digitale systemer og materiell infrastruktur. Ser en videre til de forholdene som ikke kan kjøpes, men som vokser frem i en organisasjon ser en til det uformelle. Her finner en organisasjonens kultur, relasjoner og interaksjoner. I organisasjonens kultur finner en blant annet normer, grunnleggende antagelser, væremåter og praksiser. Ser en videre til relasjoner, ser en på relasjoner mellom de ansatte i organisasjonen, både personrelasjoner og gruppedannelse. Generelt sosiale nettverk. Til slutt har en interaksjon, der en ser på interaksjon mellom de ansatte, hvordan de kommuniserer og samarbeider. Herunder kommer også styring og ledelse. I Figur 6 er det illustrert hvordan de fem faktorene er med å påvirke hverandre.




*Figur 6 Pentagonmodellen, hvordan de fem faktorene er med på å påvirke hverandre*

#### *2.2.1.1 Formell struktur*

En organisasjons formelle struktur kommer frem basert på flere elementer, blant annet organisasjonskart og regler, men også via fastsatte ordninger og system for kontroll. Schiefloe (2021) viser til Mintzberg (1983:2) sin definisjon av organisasjonsstruktur, at når en ser på oppdeling av arbeid, så er det måten disse er delt opp i deloppgaver og hvordan de koordineres. For å si det på en enklere måte: et rammeverk bestående av roller og prosedyrer. Schiefloe (2021) trekker frem Mintzberg (1983) når han videre tar for seg fem måter en kan koordinere i en organisasjon: gjensidig tilpasning, direkte overvåkning, standardisering av arbeidsprosesser, standardisering av produkter og standardisering av ferdigheter.

Organisasjonskart brukes ofte for å illustrere strukturen i en organisasjon. Oppbyggingen av organisasjonskart er ofte gjort på en hierarkisk måte og viser til ulike funksjonsområder og hvordan oppgavene mellom dem er delt. Dette blir også betegnet som organisasjonsdesign. Når en setter opp organisasjonsstrukturen viser Schiefloe (2021) til noen grunnleggende krav som bør fremheves. Tre av punktene han viser til, omhandler struktur. Det første er at strukturen må kunne fungere og være tilpasset i forhold til de eksterne omgivelsene organisasjonen har. Det andre punktet relatert til struktur er at den må gi grunnlag for å kunne ha kvalitet, produktivitet og effektiv ressursutnytting. Det siste han trekker frem er at det må legges til rette for, både vertikalt og horisontalt, å ha nødvendig informasjonsdeling og kommunikasjon. På listen viser han til to andre krav, det ene er at en for å unngå byråkratiske dysfunksjoner må ha utformet de administrative systemene slik at det unngås. Det siste punktet er å sikre at de ansatte bidrar til

organisasjonens måloppnåelse, dette ved å la de ansatte få arbeidsoppgaver hvor de får utnytte sin kompetanse. Dette må gjøres gjennom rollebeskrivelser og regelverk.

Størrelsen på en organisasjon er med å påvirke hvorvidt det er enkelt å utforme en velfungerende struktur. En ser gjerne at i store organisasjoner må det omfattende omorganiseringer til for å kunne sette opp et nytt organisasjonskart hvor roller og oppgaver flyttes rundt på. Ved utforming av organisasjonsdesign er det fem dimensjoner som fremheves som særlig viktig: funksjonsdeling, sentralisering, regelverk, rolleutforming og kontrollsystemer og intensiver (Schiefloe, 2021).

Uten å gå i dybden på alle de nevnte dimensjonene, er det likevel noen aspekter en vil se nærmere på. Om en ser på regelverk så er det de styrende dokumentene, som sier noe om hvilke regler en skal forholde seg til og hvordan en skal utføre ulike arbeidsoppgaver. Organisasjonskartet på sin side beskriver hvordan fordeling av makt, ansvar og myndighet er, samt arbeidsdeling. Hvordan regelverk er utformet har mye å si, noen utforminger gjør at arbeidet vil ta lang tid fordi regelverket beskriver en tungvint måte å gjøre dette på. I noen tilfeller er det da ansatte som velger å følge regelverket til punkt og prikke, og på den måten vise at effektiviteten går ned av å ha reglene utformet som de er. Et siste poeng som Schiefloe (2021) tar opp er at det er blitt ganske vanlig at en «skriver seg ut av problemene» ved at en møter et problem med å formulere nye regler.

Dersom en ser til Barley (2020), ser en at ved å anvende en rollebasert tilnærming til teknologisk endring, blir tre nøkkelkonsepter fremhevet: posisjon, rolle og rolleforhold. Posisjon refererer til en persons status, mens rolle beskriver de aktivitetene som knyttes til denne statusen. Kritisk er også rolleforhold, som definerer hvordan personer med ulike posisjoner samhandler, hvem de samhandler med, og hvordan disse samhandlingene struktureres i dagliglivet. Dette komplekse samspillet mellom posisjon, rolle og rolleforhold utgjør kjernen i teknologisk endring, da det ikke bare påvirker individuell oppførsel, men også organisasjonens struktur og kultur.

#### *2.2.1.2 Teknologi*

Hverdagen er fylt med teknologi, og den er å finne overalt i dagens selskaper. Med teknologi er det lett å tenke internett, datamaskiner, mobiltelefon, generelt sett de maskiner, utstyr og IT-system som arbeidstagerne er avhengig av i hverdagen for å gå gjennomført arbeidsoppgavene sine. Ser en vidt på det, finner en under teknologi også det en kan kategorisere som fysisk infrastruktur, også kallet materialitet. Kontoret er et eksempel på dette, med arbeidsplasser,

kantine, kaffemaskin og møteplasser. Fysisk infrastruktur/materialitet er ikke bare nødvendig for å ha en plass å gjennomføre arbeidet, det spiller også en essensiell rolle inn mot det kollegiale. Hvordan infrastrukturen er i selskapet er med på å påvirke hvordan de sosiale systemene er og hvordan relasjonsbygging skjer innen det kollegiale. Nøkkelord her er kommunikasjon, samarbeid og tilgjengelighet. Når det reflekteres over diskusjonene omkring åpent kontorlandskap, vil disse nøkkelordene raskt bli gjenkjent. Ved å sitte adskilt reduseres et spontant og frivillig samarbeid, noe som kan betegnes som uformell kontakt. Dette fører til at det er vanskeligere å ta felles initiativ, samt dele erfaringer på tvers mellom kollegaer (Schiefloe, 2021).

I 2009 synliggjorde Orlikowski (2009) at det i de siste tiårene har vært et tydelig fravær av teknologi i litteratur som omhandler ledelse. Det er spesielt tre perspektiv som poengteres: «absent presence», «exogenous force» og «emergent process». Disse perspektivene har Schiefloe (2021) oversatt til følgende tre tilnærminger: «fraværende tilstedeværelse», «ytre kraft» og «utviklingsprosess». I «fraværende tilstedeværelse» legger Orlikowski (2009) at teknologi ikke er blitt anerkjent av forskere som jobber med organisasjonslitteratur, og at det er grunnen til at det ikke er inkludert i litteraturen. Med «ytre kraft» mener Orlikowski (2009) at teknologi er en pådriver som har en avgjørende innvirkning på organisasjoner, Schiefloe (2021) viser til at teknologi her er med på å drive frem en organisatorisk tilpasning eller endring. For den tredje tilnærmingen til Orlikowski (2009) ser en til Schiefloe (2021), han viser til at teknologi også kan tolkes som sosialt definert og som et sosialt produkt da en ser at bruken av teknologi, samt ens betydning, er et resultat av samspill mellom atferd, institusjonelle og narrative kontekster.

Et annet relevant aspekt innenfor teknologi når en ser på pentagonmodellen er «human factors», eller menneskeligfaktor på norsk. Menneskeligfaktor ser på forholdet mellom mennesket og de redskap og systemer som de bruker og integreres med, samt de omgivelsene en arbeider i. Med menneskeligfaktor vinkler en lyset på det fysiske arbeidsmiljøet og utstyr og ser på hvordan de materielle faktorene spiller en rolle i utføring av arbeidet og på samme måte de resultatene som oppnås av dette arbeidet (Schiefloe, 2021).

En sentral observasjon ved implementering av ny teknologi i organisasjoner er at endringene ofte starter ved å modifisere arbeidspraksis, både i hva folk gjør og hvordan de gjør det. Dersom disse endringene stopper ved arbeidspraksisen, kan teknologien ha begrenset innvirkning på organisasjonen som helhet, selv om den kan være betydningsfull for individuelle brukere.

Imidlertid, når endringene i arbeidspraksis påvirker interaksjoner og relasjoner mellom ansatte, krysser teknologien en kritisk grense. Dette markerer begynnelsen på endringer i roller, rolleforhold og sosiale nettverk, noe som i sin tur kan medføre dypere strukturelle endringer i organisasjonens arbeidsdeling (Barley, 2020).

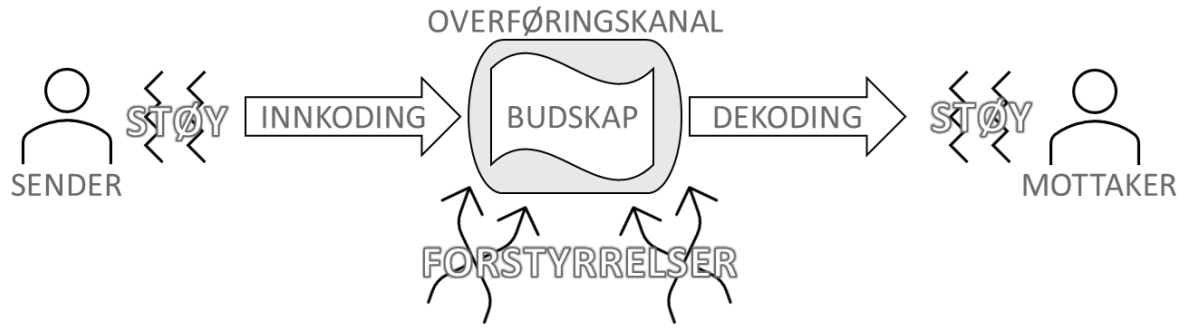
#### *2.2.1.3 Interaksjon*

Om en ser tilbake til kapittelet om formell struktur ser en at all organisering bygger på arbeidsdeling og koordinering. Med andre ord vil det si at det handler om interaksjon, om at mennesker deler på ansvar og oppgaver og samordner resultatene av innsatsen. Med interaksjon menes at mennesker aktivt forholder seg til hverandre, at de reagerer på væremåter, at de kommuniserer eller at de utforsker ting sammen. Interaksjon er derfor essensielt i et selskap da det gir selskapet grunnlag for utvikling. Det er fem former for interaksjon som er av høyere interesse; kommunikasjon, koordinering, samarbeid, ledelse og styring (Schiefloe, 2021). Innenfor interaksjonsanalyse kan disse fem formene deles inn i to hovedgrupper, samhandling og ledelse. Der en under samhandling finner samarbeid, kommunikasjon og koordinering, mens under ledelse finner en styring og lederskap.

«*Å gjøre felles*» er den norske oversettelsen av latinske «*communicare*» som kommunikasjon kommer fra. Kommunikasjon er det som gjør det mulig for mennesker å dele tanker, meninger og følelser med hverandre og som rett og slett binder mennesker sammen (Hårberg, 2020). Kommunikasjon er blant annet en viktig del av samarbeid. For at selskapet skal oppnå det de ønsker er samarbeidet mellom de ansatte av stor betydning. Samarbeid er nå to eller flere jobber sammen for å produsere noe eller oppnå et mål. For å nå målene er kvaliteten og effektiviteten til samarbeidet det som viser hva samarbeidet er i stand til å oppnå (Schiefloe, 2021).

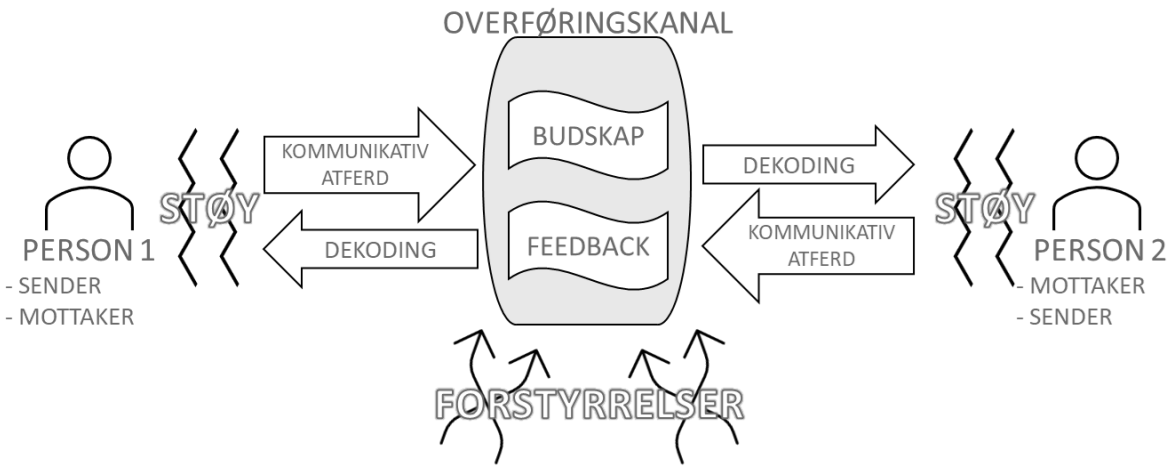
Figur 7 illustrerer den lineære kommunikasjonsmodellen som brukes av Schiefloe (2021). Bakgrunnen for modellen stammer fra Shannon og Weaver, som i 1948 presenterte en matematisk kommunikasjonsteori (Dahl & Baker, 2020). Askehave (2006) viser til at modellen til Shannon og Weaver (1949) var mer opptatt av kommunikasjonskanalen fremfor de menneskelige aspektene ved kommunikasjon. Hva som var selve budskapet, og hvor meningsutvekslingen tok sted ble sett på som irrelevant i forskningen de gjorde. Selv om dette ble neglisjert tok mange med seg modellen videre, og moderniserte den, slik som Schiefloe (2021) gjør her. Modellen til Schiefloe (2021) illustrerer kommunikasjon som en enveisprosess, hvor senderen har som mål å formidle et budskap. Første steget er å innkode budskapet, som oftest via ord, før det blir formidlet videre i en overføringskanal. En overføringskanal kan være

så mangt, blant annet er det å si det ansikt til ansikt en overføringskanal, men det kan også være noe som skjer skriftlig. Det kan også være via e-post, telefon eller sosiale medier. Veien videre fra overføringskanalen er til mottaker, der det må dekodes og mottaker tolker budskapet. Et eksempel på lineær kommunikasjonsmodell kan være at CEO (Chief Executive Officer) holder en tale i et allmannamøte. CEO er da sender og de ansatte er mottaker, mens overføringskanalen er allmannamøte. Det er ikke alltid at budskapet når frem til mottaker slik som sender initierte at det skulle, det kan være flere grunner til dette, det kan være at mottaker mistolker informasjonen som er sendt, eller at det er noe mangelfull og/eller utydelig innkoding eller dekoding (Schiefloe, 2021). Et annet moment er forstyrrelser eller støy som illustreres i Figur 7.




*Figur 7 Lineær kommunikasjonsmodell (Schiefloe, 2021)*

I betraktning av kommunikasjon mellom medarbeidere, rettes oppmerksomheten mot dialogen mellom kollegaer som gjerne kjenner til hverandre og reagerer på det som blir sagt. Da er ikke den lineære kommunikasjonsmodellen like relevant. En ser derfor på interaktiv modell når det er snakk om kommunikasjon mellom medarbeidere. I den interaktive modellen tar en høyde for flere forhold. For det første må en huske at det er ikke bare det som er tilsiktet med budskapet som kan oppfattes, men det kan også oppfattes ting som ikke var tilsiktet (Schiefloe, 2021). I og med at en kan formidle budskapet både med verbale og nonverbale signal så dekker ikke innkoding alt, en ser heller derfor på det som kommunikativ atferd som illustrert i Figur 8.



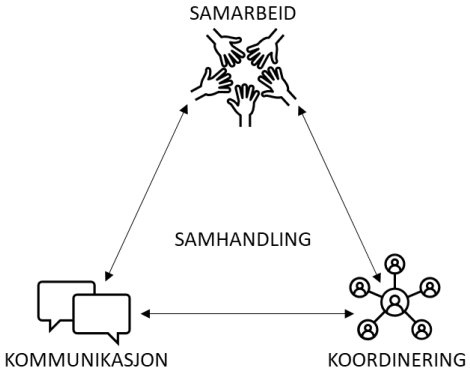

*Figur 8 Interaktiv kommunikasjons modell (Schiefloe, 2021)*

I en samtale mellom to medarbeidere er det også normalt å gi hverandre noen form for indikasjon på at du følger med, enten via tegn eller å uttrykke deg verbalt. Dette betyr at den som sender budskap også mottar budskap som sender da tolker og tilpasser seg til. Ut fra situasjon og sammenheng kan et ord og en setning bety flere forskjellige ting, i tillegg til at de har noe å si hvem som sier det og hvem som mottar. En kan oppsummert si at relasjoner og erfaringer spiller inn og det er da nyttig at den som sender også kan motta budskap for å være mer sikker på at budskapet oppfattes slik en ønsker og får anledning til å rette opp i eventuelle misforståelser. Det at partene i kommunikasjonen har en del til felles gjør det mer sannsynlig at kommunikasjonen vil være effektiv, samt at misforståelser og feiltolkninger vil være minimal (Schiefloe, 2021). Askehave (2006) viser til det å dele informasjon, ikke sende informasjon, at kommunikasjon er et samarbeid mellom partene for å skape en felles forståelse.

Her deler Schiefloe (2021) ledelse opp i lederskap og styring, dette for å dekke de funksjonene ledelse har. Lederskap har som formål å lede, altså få andre med seg og sammen oppnå gode resultat. Innenfor lederskap er det essensielt å kunne motivere andre og være i posisjon til å få de en leder til å yte sitt beste for å nå de mål som er satt. Styring på sin side er mer kontrollerende, den kommer med makt og innebærer å planlegge, deriblant bemanning, økonomi og løsninger på problemer. Det innebærer da å måtte ta beslutninger som andre må føye seg til. Det er ikke nødvendigvis slik at det er en og samme person som sitter med både styring og lederskap, flere av aktivistene som kommer med rollene kan fordeles på flere, som for eksempel innad i et lederteam. Utfordringen er å balansere disse to funksjonene på en god måte (Schiefloe, 2021).

Kommunikasjon, koordinering og samarbeid er det som må til for å få en effektiv samhandling (Figur 9). Helseinnovasjonssenteret har oppsummert deres forståelse av begrepet samhandling på en god måte:

> *«Samhandling er koordinerte aktiviteter i en prosess, der aktørene engasjerer og forplikter seg mot et felles mål, og handler og beslutter sammen som likeverdige parter på tvers av roller, nivå, fag og sektorer.» (Helseinnovasjonssenteret, 2023)*




*Figur 9 Samhandlingstriangel (Schiefloe, 2021)*

Når en snakker om koordinering er det fornuftig å skille mellom det som kan løses med prosedyrer og regelverk og det som trenger tilpassing. Grunnlaget for koordinering kan dekkes med prosedyrer og regelverk dersom det er kjente oppgaver og løsninger som skal gjennomføres, mens dersom oppgavene varierer må en koordinere ut fra situasjonen (Shiefloe, 2021).

#### *2.2.1.4 Relasjoner*

Med relasjoner menes her en sosial relasjon, som når to personer på grunnlag av gjentatt interaksjon og gjensidig forventning blir knyttet til hverandre. Det finnes både formelle og uformelle relasjoner. Et eksempel på formell relasjon kan være mellom deg og lederen din, eller mellom deg og kollegaer. De aller fleste relasjoner er likevel av den uformelle sorten, altså de som oppstår uoppfordret. Typiske egenskaper ved relasjoner er blant annet opplevd forpliktelse, nærhet og styrke. I mange tilfeller opplever en relasjoner som positivt, men da det ikke er alle relasjoner en styrer over er det noen som kan oppleves negativt. Et eksempel kan være en relasjon med en kollega, der en misliker eller har mistro til kollegaen sin, men likevel må jobbe sammen (Schiefloe, 2021).

Innenfor relasjoner ser en på sosiale nettverk, dette er uformelle relasjoner mellom mennesker. Når flere relasjoner kobles sammen dannes det et nettverk som knytter en sammen. Hvordan et selskap fungerer er et utfall av hvordan de uformelle relasjonene og nettverkene er. Ved å gjøre en nettverksanalyse kan en avdekke dersom selskapet har sårbarheter eller svakheter i hvordan selskapet fungerer i det daglige. I en analyse rettet mot relasjoner er det ofte kvantitative metoder som blir brukt, da en ønsker å finne frem til viktige og kritiske relasjoner (Schiefloe, 2021). Det er likevel fornuftig å ha med seg kunnskapen om relasjoner inn i organisasjonsanalyse når en skal drøfte resultatene som kommer frem.

Sosial kapital refererer til de ressursene som oppstår både direkte og indirekte som et resultat av at aktører aktivt deltar og forplikter seg i ulike sosiale nettverk. Ser en på selskapets sosiale kapital så kan en si at det er en resurs som reflekterer selskapets egenskaper ved de sosiale relasjonene. Den sosiale kapitalen i et selskap kan deles inn i to komponenter: «associability» og tillit. Med «associability» menes deltakernes vilje og evne til å sette det kollektive fremfor det individuelle når det kommer til mål og handlinger. Mens en robust og varig tillit blir sett på som en forutsetning for sosial kapital (Schiefloe, 2021).

Schiefloe (2021) bruker Leana & van Buren (1999) i sin diskusjon rundt sosial kapital. Blant annet ved å vise til at sosial kapital har fire måter den kan gi avkastning på til et selskap. Den første av disse ser på hvordan et høyt nivå av sosial kapital spiller inn på hvordan den ansatte setter de mål som er felles fremfor sine egne mål. Når ansatte føler de bidrar til fellesskapet, vil egne interesser bli lavere prioritert. Som nummer to ser en på økt fleksibilitet og tilpasningsevne. Relatert til dette er den tredje effekten, som har med transaksjonskostnader og koordinering å gjøre. I et selskap med en grunnleggende solid sosial kapital blir behovet for prosedyrer mindre, da de ansatte i selskapet deler en grunnleggende forståelse av selskapet, samt at de har tillit til hverandre og derfor kan jobbe effektivt sammen. Den siste måten viser til at det er lettere å dele informasjon og kunnskap om en et tilgjengelig for hverandre. Dette ved å utnytte de intellektuelle ressursene en har (Schiefloe, 2021).

#### *2.2.1.5 Kultur*

I organisasjonsanalyse beskrives kultur som noe felles, velkjent og tydelig (Schiefloe, 2021). Kultur er noe som flyter mellom mennesket, det både binder mennesket sammen og skiller mennesket fra hverandre, men hvordan, når og hvorfor er basert på ulike grunnlag (Holliday, 2009). Forklaringen til Eriksen og Sajjad (2015) om hvordan kultur kan betraktes er en av de bedre.

> *«Kultur kan […] betraktes som en slags mental matrise for handling; summen av alle de erfaringer, kunnskaper og verdier vi bærer med oss, og som vi handler på grunnlag av. Men det går ingen skarpe grenser mellom kulturer, og det er ikke nok å «kjenne til en kultur» for å forstå hvorfor folk gjør som de gjør.» (Eriksen & Sajjad, 2015, s. 41)*

En kan ikke ta for gitt at kulturen i et selskap er felles, med det menes det at det er ikke gitt at alle de ansatte opplever kulturen likt. Det er ikke alle kulturer som kommer som «one size, fits all», et eksempel på dette er nasjonale kulturer. Et eksempel på nasjonale kulturer er at en gjerne

beskriver en nordmann som en person i bunad, med ski på beina og brunost på skiva. Nasjonale kulturer sier en består av mange subkulturer, der alder, geografi, kjønn, interesser med mer spiller inn. Et eksempel på en subkultur er en digital sikkerhetskultur (Bergsjø & Windvik, 2020).

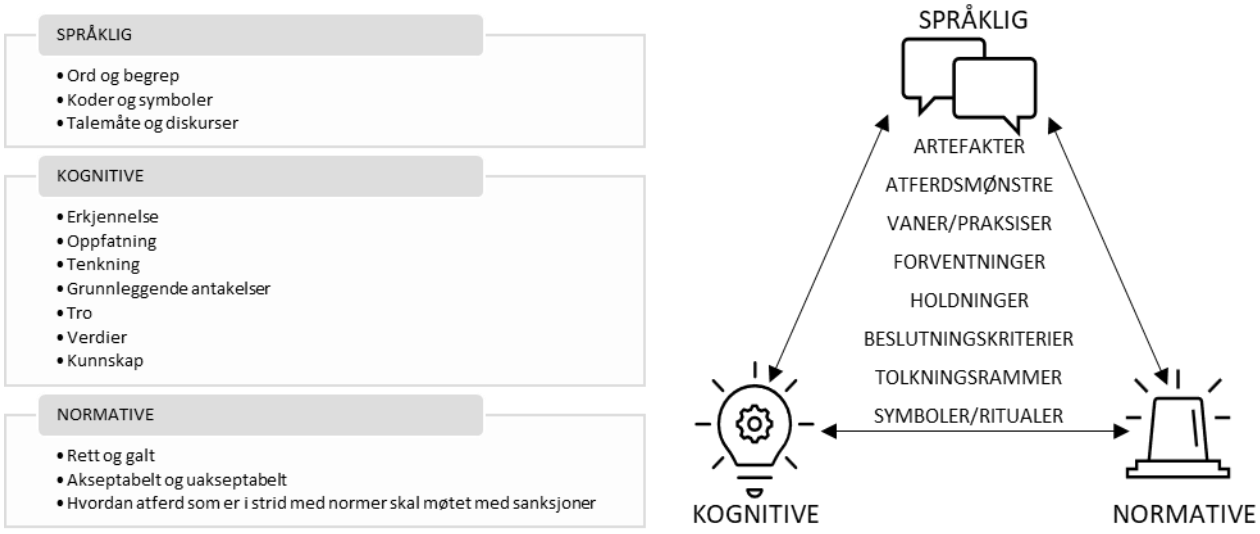
Dette er spesielt merkbart i større selskap, hvor det observeres at kulturen er differensiert og fragmentert. I et selskap kan det være flere subkulturer, hvor noen eksisterer harmonisk, mens andre kan være konkurrerende eller i konflikt. De kan også være helt uavhengige av hverandre. Et eksempel på en subkultur kan være en enhet eller et team. Ser en til selskapet som denne masteroppgaven tar utgangspunkt i, så er selskapet fordelt på tre ulike lokasjoner. Det gjør det naturlig å tenke at hver lokasjon kan være en subkultur. Innenfor hver subkultur kan en igjen finne en ny subkultur, for eksempel innenfor faggrupper, roller eller kjønn. Dersom kulturen i selskapet fremstår som fragmentert vil det si at det ikke er helt klare kulturelle retningslinjer, det vil si at de ansatte ikke har en felles oppfatning av at «sånn gjør vi det i dette selskapet» (Schiefloe, 2021).

Det som er viktig å få frem når det kommer til kultur, er at denne ikke kan vedtas eller styres; den vokser frem av seg selv. Kultur kan i noen tilfeller påvirkes, utvikles og endres gjennom aktiv medvirkning, signaler og lokale prosesser. Hvordan og hvor mye kultur spiller inn i selskap er ulikt fra selskap til selskap (Schiefloe, 2021). Noe en må ha i bakhode er at det er de ansatte som skaper kulturen og det er også de som blir påvirket av den (Bergsjø & Windvik, 2020). For å få en god sikkerhetskultur er det derfor viktig at sikkerheten er mulig for de ansatte å forstå. Ledelsen må sørge for at de ansatte har relevant kompetanse for å møte forventningene knyttet til digital sikkerhet, og dette innebærer å utstyre de ansatte med den kunnskapen som trengs samt jobbe med å vedlikeholde kunnskapen. Ved å opprettholde opplæring og bevissthet hos de ansatte styrkes deres evne til å foreta sikre valg angående digital sikkerhet. Når en skal jobbe med digital sikkerhetskultur kan det være hensiktsmessig å gjøre en form for kartlegging, slik at en får et overblikk av hvordan de ansatte lærer om temaet. Det er ikke slik at alle lærer på samme måte og det kan derfor være fornuftig å se på hvilke metoder det kommer frem at ansatte lærer av (Bergsjø & Windvik, 2020). I noen selskap er det tydelige kulturer, det er for eksempel noen etablerte vaner, praksiser, typiske atferdsmønstre, forventninger og holdninger.

Innenfor organisasjonsanalyse kan en splitte kulturelle fundamenter opp i tre grupper. Disse gruppene er språklige, kognitive og normative elementer, hva som ligges i de enkelte og hvordan de henger sammen og påvirker hverandre er illustrert i Figur 10 (Schiefloe, 2021).

Samfunnet er i stadig utvikling og mer blir digitalisert. Bergsjø og Windvik (2020) tar opp at det er fristende å slå fast at interessen til de ansatte når det kommer til IT og teknologi er en fordel som de uten interessen ikke har. Interesser bidrar til å forme, både når det kommer til ferdigheter, holdninger og kunnskap. Med interessen kommer også en økt bevissthet og det påvirker hvem en lytter til, hvem en omgås og det stimulerer nysgjerrigheten.

Ser en tilbake på forordet i denne masteroppgaven, ser en at «det er bare å kaste seg hodestups ut i det», noe som er en metafor på at en setter i gang med noe uten å vite hvordan det går. En metafor er nemlig en sammenligning, men uten sammenligningsord. Det er ord eller uttrykk som brukes i billedlig betydning, som her, eller i overført betydning. Metaforer er med på å styre hva, hvilke og hvordan: hva legger en merke til, hvilke data ses som relevante og hvordan tolke det virkelighetsbildet som da dannes. Nettopp fordi de er med på å gjøre det lettere for den enkelte å forstå fenomener, betyr det også at metaforer har med seg noen begrensninger (Schiefloe, 2021).




*Figur 10 De tre kulturelle fundamenter (Schiefloe, 2021)*

Alt som foregår i et selskap, har enten direkte eller indirekte påvirkning fra kulturen. Kultur virker sammen med de fire andre hoveddimensjonene i pentagonmodellen (Schiefloe, 2021). Andersen (2001) kommentere i sin bok «Den meningsskapte organisasjon» at det forholdet som har med sosiale strukturer og makt lett kan undervurderes om en fokuserer på kulturen, noe som er fornuftig å ha i bakhode når en ser på resultatene fra undersøkelsene som er gjort i denne masteroppgaven.

I dag består hverdagen av mye teknologi og tekniske tjenester, og det settes forventinger av samfunnet at en skal ha en viss form for grunnleggende kompetanse innenfor det digitale, nettopp for å kunne ta del i det digitale samfunnet. På noen arbeidsplasser legges det opp til opplæring av de ansatte, mens det andre steder forventes at de ansatte tilegner seg nødvendig kunnskap på egen hånd uten tilbud om formell opplæring. Det er ikke mange år tilbake i tid en skal reise for at problemstillingen «minnepenn på bakken» var et scenario som var særs aktuelt for å forklare datasikkerhet. Da tok en den gjerne med seg og plugget den inn i datamaskinen sin, hovedsakelig for å identifisere eieren og deretter returnere den. Dette var en metode hackere brukte for å få tilgang til systemene, men bevisstgjøring og opplæring har bidratt til en uskreven regel om at en ikke skal plugge i en minnepenn uten kjennskap til innholdet. Faremomentene med dette er blitt allment kjent og de aller fleste vet at dette er noe de ikke skal gjøre. Slike uskrevne regler kalles også for sosiale normer. Sosiale normer er uskrevne regler som regulerer hvordan vi skal oppføre oss i ulike situasjoner. På en arbeidsplass vil en finne flere slike sosiale normer og når en ser på sosiale normer i en gruppe, vil en da si at gruppen har en kultur hvor de sosiale normene er en retningslinje (Bergsjø & Windvik, 2020).

# 3 METODE

Problemstillingen er selve startstreken for forskning, dette fordi en må ha noe en ønsker å finne ut mer om, der målet er å finne forskningsdata som kan drøftes med utgangspunkt i problemstillingen opp mot relevant litteratur.

Kvale og Brinkmann (2015) viser til at «veien til mål» er den opprinnelige betydningen av ordet metode. Hvilken vei en velger blir påvirket av flere ting, spesielt hvordan problemstillingen er utformet. Noen ganger kan problemstillinger egne seg til både kvalitativ og kvantitative undersøkelser, men det er ikke alltid slik. Det å utforske komplekse aspekter av menneskelige opplevelser og perspektiver krever ofte mer enn tall og statistikk. Problemstillinger med spørreord som hvordan, hvilke eller hvorfor åpner for mer utdypende svar enn «ja» og «nei» (Larsen, 2017). Når en ønsker å komme i dybden, fange opp meninger og opplevelser så er ikke den kvantitative metoden med spørreundersøkelser veien å gå. Når en her ønsker å se på hvordan det jobbes med digital sikkerhet og hvordan forholdet er mellom teknologi, mennesket og organisasjon så vil en kunne hente ut mer detaljert data fra et dybdeintervju enn en ville fått av et skjema der ansatte skal krysse av.

## 3.1 Kvalitativt forskning

Hvordan noe oppleves og hvordan noe skjer, er det kvalitativ metode handler om (Kvale & Brinkmann, 2015). I denne masteroppgaven vil den kvalitative forskningen bli gjort gjennom intervju. Ved intervju ønsker en å få nyanserte beskrivelser fra deltakerne gjennom ord. Under intervjuet må en lytte til deltakernes beskrivelser og meningene de uttrykker, men en må også lytte til de tingene som blir «sagt mellom linjene». Når en hører noe bli sagt mellom linjene i et intervju, kan en spille det tilbake til deltakeren for å få bekreftelse på om en har tolket det som ble sagt riktig, eller om en har misforstått slik at deltakeren får mulighet til å oppklare (Kvale & Brinkmann, 2015).

Som oftest er intervju ansikt til ansikt, det gjør at en også kan observere den en intervjuer samtidig som en lytter til det som blir sagt. Dette er også noe en tar med seg når en tolker svarene, både på godt og vondt. En fallgruve er om den som blir intervjuet sier noe med ironi, men det blir oppfattet reelt, eller vis-e-versa. Fordelen er her, på samme måte som med det som blir «sagt mellom linjene» at i slike situasjoner kan en få det oppklart i intervjuene dersom en

stiller oppfølgingsspørsmål for å klarere at tolkningen en har gjort stemmer. Siden det kan stilles utdypende og flere spørsmål, samt at den som blir intervjuet kan snakke fritt, gir det god validitet. Spesielt siden en kan få ryddet unna eventuelle misforståelser ved å stille oppfølgingsspørsmål.

Det at en avtaler å gjennomføre intervju, mot at en sender ut spørreundersøkelser til en større gruppe, blir sett på som en metode en har mindre frafall fra. Når en har avtalt å delta i et intervju skjer det sjeldent at folk dropper å møte opp. Dersom de skulle bli forhindret fra å møte opp gir de ofte beskjed om dette i forkant og avtaler nytt tidspunkt. I intervjuprosessen som ble gjennomført i denne oppgaven skjedde nettopp det, noen ble forhindret i å møte til avtalt tid, men kom med forslag om nytt tidspunkt.

Noen utfordringer som kommer med intervju som metode, er at det kan være den du intervjuer ikke ønsker å svare det de egentlig mener. Dette kan være flere grunner til, en av de kan være at deltakeren tror at det han sier er det en forventer skal bli sagt eller at det er det en ønsker å høre, eller ønsker å fremstå på en annen måte på grunn av situasjonen en sitter i. Selv om intervjuene er anonyme og funnene ikke skal kunne spores tilbake til den som blir intervjuet så er det lettere å være ærlig i et spørreskjema enn når du sitter rett fremfor noen. Unntaket ved intervju er dersom den en intervjuer lar seg sitere. Det er viktig å tenke gjennom hvordan oppbyggingen av intervju blir gjort, en ønsker at den som deltar skal føle seg trygg og ikke bli ledet av spørsmålene som stilles.

All forskning krever et grundig forarbeid før en kan starte å innhente informasjon. Her vil de ulike prosessene som har blitt gjennomført før selve intervjuet bli belyst, hvilke valg som er tatt, hvorfor disse valgene er tatt og hvordan prosessen har gått for seg.

I intervju er det ikke bare svarene til de som deltar en får, en får også observere de under samtalen. Og en har mulighet til å rette opp i eventuelle misforståelser, samt stille oppfølgingsspørsmål, noe en ikke har mulighet til i den kvantitative metoden

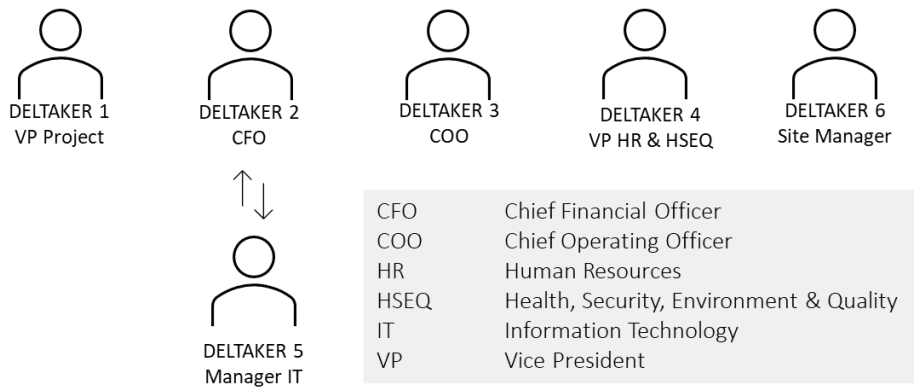
## 3.2 Utvalget

Når en skulle finne deltakere til intervjuene var det noen kriterier som ble bestemt. Det første var at en kun ville se på et selskap og at dette selskapet måtte være innenfor den maritime sektoren.

Selskapet som stilte opp, er et selskap innen den maritime sektoren som har flere lokasjoner i Norge og som består av både fabrikkvirksomhet og kontorvirksomhet. Da problemstillingen tar

for seg hvordan det formelt og uformelt jobbes med digital sikkerhet ble det valgt å bruke en skjønnsmessig utvelging. Med en skjønnsmessig utvelging menes det at deltakerne er valgt ut fra ulike kriterier, som blant annet kjønn, alder og utdanning. Denne utvelgings metoden er mye brukt innenfor kvalitativ forskningsmetode. Skjønnsmessig utvelging er en del av det som kjennetegnes som strategisk utvelgelse, kort oppsummert at den som skal gjennomføre undersøkelsen selv bevisst velger hvem som skal delta (Larsen, 2017). I dette tilfelle er kriteriene hverken kjønn eller alder, men rollen deltakerne har i selskapet. For denne masteroppgaven ble det lagt vekt på at en ønsket lederroller, gjerne fordelt på selskapets lokasjoner, samt noen med fagkunnskap innenfor digital sikkerhet.

Innenfor forskningen er det variert hvor mange deltakere det anbefales å ha, Larsen sier selv at det ikke er noen fasit på dette (Larsen, 2017). Ser en til Kvale og Brinkmann (2015) viser de til at det har en tendens til å enten være for mange eller for få, dersom en har for få deltakere vil det blant annet være vanskelig å generalisere. Dersom en har for mange deltakere derimot, så vil tiden mest sannsynlig ikke strekke til for å få gjort en dyptgående analyse av intervjuene. Videre legger de frem at vanlige intervjuundersøkelser ligger rundt 15 deltakere, men at det er med en margin på +/- 10 deltakere, noe som vil si det er et sted mellom 5 og 25 deltakere. Det kommer også frem at inntrykket er at i nyere intervjuundersøkelser er det ofte en fordel å ha et lavere antall deltakere, dette for å fordele tiden mer på forberedelser og analyse (Kvale & Brinkmann, 2015). For denne masteroppgaven ble det sendt ut forespørsel til syv ledere i selskapet, der noen også har fagkompetanse på digital sikkerhet. Av de syv som ble kontaktet hos selskapet svarte seks av de ja til å delta i et dybdeintervju om digital sikkerhet og hvordan dette jobbes med i selskapet. Den siste som ble forespurt var på daværende tidspunkt ikke tilgjengelig for å kunne delta i intervjuene. Utvalget er presentert i Figur 11.




*Figur 11 Utvalget, med beskrivelse av forkortelser*

Utvalget vil heretter bli henvist til som: VP Project, CFO, COO, HR, Site Manager og IT-ansvarlig. Av hensyn til deltakerne og selskapet, så har alle navn, både på personer og selskap, blitt anonymisert ved å henvise henholdsvis til rolle og type selskap. Dersom noen har henvist til IT-ansvarlig ved navn i sine intervju, så vil vedkommende da omtales som IT-ansvarlig i et eventuelt sitat. Da kjønn ikke er blant de kriterier som vektlegges i denne masteroppgaven, så sees kjønn på som ikke-relevant, derfor vil alle bli henvist til som «han», dette til informasjon.

## 3.3 Intervjuguide

For intervjuet ønskes en god atmosfære der deltakerne føler de kan komme med de meningene de har, det skal føles som at det er et intervju og ikke et avhør. Det er en av grunnene til at en skal ha en intervjuguide forberedt i forkant av intervjuet, en annen grunn er å sikre at en får stilt spørsmål om de emnene som er relevant for undersøkelsen en gjør. Med bakgrunn i organisasjonsanalyse og digital sikkerhet, er intervjuguiden her bygget opp rundt de fem hovedmomentene i Schiefloe (2021) sin pentagonmodell formell struktur, teknologi, relasjoner, interaksjon og kultur (Figur 5)

Det finnes flere metoder for hvordan en legger opp intervjuguiden. Schiefloe (2021) viser til to metoder for kvalitative organisasjonsstudier der pentagontilnærmingen brukes. Den føreste er å benytte de fem hovedgruppene av faktorer som redskap for kategorisering av den informasjonen som skal samles inn. Etter intervjuet vil forskeren da ta med seg svarene og sette det inn i et analyseskjema som var laget i forkant av intervjuene. Den andre metoden er gjennom en mer strukturert tilnærming, der en benytter en intervjuguide som sikrer at alle de fem hovedkategoriene dekkes. I denne metoden viser Schiefloe (2021) til forslag på problemstilling med sterke og svake sider ved IT-sikkerheten, der en kan stille spørsmål både om betydning av formell struktur, teknologi, kultur, interaksjon og relasjoner. Selv om en har en strukturert tilnærming må en være åpen for at informanten kommer med innspill om andre forhold enn de som var listet opp i intervjuguiden. Avslutningsvis nevner Schiefloe (2021) at en kan bruke en mellomvariant av disse to metodene, der en stiller relativt åpne spørsmål, men som hjelpemiddel har en med seg en stikkordsliste med temaer som en går ut fra er viktig som en kan dra frem om informanten ikke kommer innom disse temaene selv.

Intervjuguiden som er laget for denne masteroppgaven er av den typen som Schiefloe (2021) ville kallet en mellomvariant. Utformingen av intervjuguiden (vedlegg 1) gjort med åpne spørsmål som bygger på de fem hovedkategoriene i pentagonmodellen, da innenfor digital sikkerhet. Til hvert av spørsmålene ble det notert stikkord tema en ønsket deltagerne skulle si

noe rundt. Disse stikkordene fungerte også som et hjelpemiddel for å føre samtalen tilbake til på rett spor om en skulle snakke seg for langt unna formålet med intervjuet. Dette er en sikkerhet for å vite at deltakerne har fått mulighet til å komme med sine erfaringer og meninger innenfor de forhåndsplanlagte temaene. Det er ikke alltid alle temaene er like aktuelle for alle deltakerne, men da får de muligheten til å velge om de har noe de vil tilføye (Schiefloe, 2021).

## 3.4 Samtykke og søknader

Med både intervjuguide og utvalg på plass, er det bare noen formaliteter som gjenstår før en kan sette i gang med intervjuene. Det første er å melde forskningsprosjektet inn til Norsk senter for forskningsdata (heretter omtalt som NSD). På NSD sine nettsider finner en lenke for søknad. Her må en fylle inn en søknad som får et eget referansenummer, denne masteroppgaven er gitt referansenummer 496671. I tillegg til å fylle ut et søknadsskjema så må en laste opp intervjuguide, samt til et informasjonsskriv. Dette informasjonsskrivet er laget for å gi deltakerne den informasjonen de trenger i forkant av intervjuet. Innholdet i skrivet er blant annet informasjon om masteroppgaven, som formål, hva det innebærer å delta, hvordan opplysninger vil bli behandlet og hva som skjer med opplysningene i etterkant av masteroppgaven. Informasjonsskrivet som ble sendt ut finner en under vedlegg 2. Informasjonsskrivet avsluttes med en samtykkeerklæring om at en ønsker å delta i dette forskningsprosjektet og at de godtok at samtalen ville bli tatt opp. Med klarsignal fra NSD og samtykkene fra deltakerne, ble det avtalt tidspunkt for gjennomføring av intervju med hver enkelt deltaker.

Til informasjon så ligger det to vedlegg fra NSD ved denne oppgaven (vedlegg 3 og 4), dette da forskningsprosjektet ble forlenget grunnet personlige årsaker og søknaden måtte derfor fornyes.

## 3.5 Veien til mål

En vil her se på hvilke valg som ble gjort for intervjuoppsettet og beskrivelse av hvordan gjennomføringen av selve intervjuene.

### 3.5.1 Intervjuoppsett

For intervjuene ønsket en at det skulle være like rammer for alle deltakerne. Grunnet ulike lokasjoner ble det derfor besluttet at alle intervjuene skulle gjennomføres via videosamtale med Microsoft Teams. Det å gjennomføre intervjuene digitalt ble vurdert til å være et godt valg, i tillegg ville det gi muligheter til å vie full oppmerksomhet til deltakerne da et videopptak ville gjøre at en ikke må notere ned observasjoner underveis.

En ville at deltakerne skulle føle de hadde nok tid til å ta seg tid til å resonere der det skulle være aktuelt, samtidig ville en ikke sette av så mye tid at deltakerne skulle føle det som en byrde. Det ble derfor satt av en hel klokketime til hver deltaker, med beskjed om at tiden som satt opp var for å sikre at det skulle være tilstrekkelig med tid avsatt.

### 3.5.2 Gjennomføring av intervju

I en hektisk hverdag er det vanskelig å få det til å passe for alle, men intervjuene ble gjennomført innenfor en tidsramme på to uker i første kvartal i 2023. Som avtalt med deltakerne var det avsatt en klokketime til å gjennomføre intervjuet. Selv med denne avklaringen på forhånd, var det en deltaker som informerte i staten av intervjuet om at det hadde kommet noe i veien og vedkommende ikke hadde mulighet til å delta i mer enn en halvtime. Selv med mindre tid til rådighet var opplevelsen at tiden ikke påvirket intervjuet. Dette var inntrykket en satt igjen med for alle intervjuene, det virket til at samtlige tok seg tid til å reflektere over de spørsmål som ble stilt. For utvalget lå intervjutidene et sted mellom 25 og 45 minutter.

Innledningsvis i intervjuene ble noe av informasjonen fra informasjonsskrivet gjentatt, det ble kontrollert at samtykket fremdeles stod ved lag, samt en åpnet for om det var spørsmål utover den informasjonen som ble sendt ut. Da dette var gjennomgått, ble opptak av videosamtalen startet.

Innledningsvis startet en med spørsmål om deltakeren, der de fikk fortelle hvem de er, hva de arbeider med og hvilke arbeidserfaringer de har. Av informasjonen som kom frem viser noen blant annet til tidligere arbeidserfaring knyttet til digital sikkerhet. En annen ting som kom frem var hvilke roller de har hatt tidligere, både i dette selskapet og andre selskap.

En ting som har kommet frem gjennom studieløpet er at ikke alle sitter med de samme rammene og at dette kan påvirke ens oppfatning. Det en legger i et begrep trenger ikke være det samme deltakeren legger i det, det ble derfor stilt spørsmål om hva deltakerne tenkte når de hørte digital sikkerhet.

Under intervjuene lå intervjuguiden fremme. Flyten i intervjuene gikk naturlig og det var sjeldent det ble behov for å se til nøkkelordene som hadde blitt notert. Intervjuguiden tok utgangspunkt i hovedspørsmålene og ble ellers brukt som en sjekkliste på at temaene hadde vært dekket og om det var tema som ikke hadde blitt nevnt ble de så tatt opp.

Siden intervjuene ble tatt opp, med både video og lyd, ble det ikke tatt notater under intervjuene. Dette var med på å sikre en god flyt for begge parter, det var full oppmerksomhet på deltakeren

og på hva den la frem. Dette gjorde at en fikk stilt oppfølgingsspørsmål som under intervjuet der det ble aktuelt.

Det at intervjuene ble gjennomført digitalt opplevdes ikke som noen form for hindring. En sitter igjen med følelsen av at det var like hverdagslig som å sitte ovenfor hverandre. Dette kan nok skyldes at det å gjennomføre møter via Microsoft Teams, eller andre tilsvarende program, er blitt en hverdagslig ting for de fleste og påvirket nok derfor ikke atmosfæren i intervjuene. En opplevde at deltakerne følte seg bekvem i situasjonen. I tillegg spilte teknologien på lag, noe som gjorde det hele til en god opplevelse.

### 3.5.3 Transkripsjon

Ved å transkribere intervju så omgjør en de fra å være muntlig til å være skriftlig, dette for at intervjuene skal være mer egnet for å analyseres. Når en får det strukturert ned på papir så kommer oversikten tydeligere frem.

Det å transkribere er en tidkrevende jobb. Kvale og Brinkmann (2015) viser til et bestemt karakterstudiet i sin bok «Det kvalitative forskningsintervju», hvor en erfaren skriver brukte rundt fem timer på å transkribere et intervju ordrett, dette var da et intervju med varighet på en time. Alt etter hvor mye tale som er i et slikt intervju kommer det på ca. 20-25 sider, det skal nevnes at dette var med enkel linjeavstand. Intervjuene i denne oppgaven var som nevnt tidligere på mellom 25 og 45 minutter, transkripsjonene er på mellom 7 og 12 sider, med skriftstørrelse 11 og 1,15 i linjeavstand. Tiden brukt på dette kan oppsummeres som veldig lang. Selv om det i dag finnes mange programmer som kunne gjort transkripsjon for en, så ble det her valgt å gjøre jobben selv. Selv om det er en tidkrevende jobb, så ble det vurdert som en investering i å bli godt kjent med materialet en skal jobbe videre med.

Transkripsjonen ble gjort ordrett så godt som det lar seg gjøre. For å kunne gjøre det på en så effektiv måte som mulig ble det brukt bokstaver for å indikere om det var noe som deltakeren sa eller om det var intervjueren som sa noe. Det var noen få ganger det ble en del mumling, eller at deltakerne stoppet opp midt i en setning og fortsatte på noe annet. Alt ble notert ned, så en kan se hvor en har «tenkt høyt». Videre har det også blitt notert ned der deltakerne tar seg en tenkepause, der de leter opp informasjon mens de snakker, blir forstyrret av at noen kommer inn eller om de ler og smiler mens de forteller om situasjoner.

## 3.6 Analyse av data

Når transkripsjon av intervjuene var gjort var det mye informasjon innhentet fra deltakerne. Når en skal analysere de funnen som kommer frem er det lurt å gå gjennom transkripsjonene flere ganger. Larsen (2017) viser til forskjellige måter å gå gjennom transkripsjonene på, med å lese, notere og planlegge for koding. Transkripsjonene ble lest mange ganger, en startet med å lese gjennom for å danne seg et helhetsinntrykk, før en gikk gjennom transkripsjonene igjen og noterte i margen de tanker som kom mens en leser, deriblant ideer om koding.

Når en analyserer de data som er innhenter, forsøker en å finne sammenhenger og se mønstre. For å kode data som kom frem av transkripsjonene ble det for denne masteroppgaven sett på flere måter å kode data. Det å kode transkripsjonene var ikke så enkelt som en hadde tenkt og valget av metode for koding var vanskelig. Til slutt ble det besluttet å se på et enkelt «kodetre», der hver gren av treet representerte de fem kategoriene i pentagonmodellen. Under hver gren ble relevante kategorier hentet ut fra teorien om hva som ligger under formell struktur, teknologi, interaksjon, relasjoner og kultur. Til å sette opp «kodetre» ble Excel brukt for å lage en slags matrise der en fikk overblikk hva de ulike deltakerne hadde sagt innenfor de ulike kodene. En utfordring en merket tidlig var når flere elementer fra intervjuene passet i flere av kategoriene, dette kom tydelig frem i «kodetreet». Det er i empirien og drøfting forsøkt løst ved å sette sammen flere kategorier for å trekke linjene mellom disse.

## 3.7 Validitet

Allerede tidlig i arbeidet med masteroppgaven må en ta høyde for validitet. Innenfor kvalitative studier handler det blant annet om den dataen en innhenter er relevant for problemstillingen en har for at de slutningene som trekkes er valide. En må derfor ta høyde for validitet i det en ser på utvalg og intervjuguide, at de en intervjuer og de spørsmålene de får er relevant for problemstillingen en jobber med (Larsen, 2017). I tillegg må en tenke over hvordan en formulerer spørsmålene, for denne oppgaven var fokuset å ha åpne spørsmål for å la deltakerne selv styre retningen og deretter bruke intervjuguiden til å navigere tilbake til de temaene en ønsket å dekke. Under intervju var det mulighet for å stille oppfølgingsspørsmål dersom noe skulle være utydelig, eller gjøre korreksjoner dersom det kommer frem informasjon i intervjuet en i utgangspunktet ikke hadde tenkt var viktig når en jobbet med problemstillingen. Dette er også med på å øke validiteten.

En har i denne masteroppgaven et utvalg der alle er hentet fra samme selskap innenfor den maritime bransjen der alle har lederroller, noen også med fagkompetanse om digital sikkerhet. Videre ble det valgt å ikke gjennomføre noe pilotundersøkelse, en hadde i stedet en nøye gjennomgang av intervjuguide og utvalg sammen med veileder. Dette for å sikre at en ville dekke de områdene en ønsket å innhente data om. Det at en har tatt høyde for dette er grunnleggende for at en skal kunne bekrefte de funn som kommer frem av forskningen og eventuelt de slutningene en trekker. En må også tenke på om de fortolkningene en gjør er troverdige (Larsen, 2017) .

Larsen (2017) kommer med et råd når det kommer til å være kritisk i forskningsprosessen. Det er å tenke igjennom alle slutninger en foretar i drøftingene og tolkningene og stille seg selv spørsmål om en har grunnlag fra datagrunnlaget til å trekke denne slutningen.

## 3.8 Reliabilitet

Med reliabilitet viser en til om nøyaktighet har ligget til grunn gjennom hele prosessen. Å sikre høy reliabilitet innenfor kvalitative studier, da gjennom både intervju og observasjon der flere momenter spiller inn. I intervju er det muligheter for at informasjonen som kommer frem påvirkes av intervjueren og av situasjonen, det er ingen garanti for at deltakerne ville sagt det samme om intervjuet ble gjennomført tre måneder senere, enten av samme intervjuer eller en annen. Selv dagen etter kunne svarene vært annerledes enn de var da intervjuet ble gjennomført. En viser til troverdighet i reliabilitet også, at de empiriske funnene som presenteres er det som faktisk kommer frem av funnene fra intervjuene. For å sikre reliabilitet kan en ta en kritisk gjennomgang av datamaterialet på ulike tidspunkt. Dette kan blant annet gjøres ved å gå gjennom datainnsamling å se at spørsmål ikke er ledende og at de er tydelig. At transkripsjonen gjøres nøyaktig er også med på å sikre reliabilitet, samt at en er nøyaktig i kodingen av tekst (Larsen, 2017). I denne masteroppgaven har det i de tilfeller sitat skal brukes, blitt hentet direkte fra transkripsjonene og ikke fra dokument med koding, dette for å være sikker på at det som siteres er i henhold til det transkripsjonen viser at deltakerne sa.

## 3.9 Egen forståelse

Om objektivitet sier Larsen (2017) følgende:

> *«Kunnskapssyn, erfaringer og verdier kan ha betydning for hvilken tilnærmingsmåte en velger i sin forskning, hvordan en formulerer sine problemstillinger, hvilke begreper og teorier en velger å bruke, og det vil*

> *også til en viss grad påvirke hvordan vi tolker svarene. Det vil altså være umulig å være helt objektiv når en driver med forskning. Det er viktig i forskningen at en etterstreber å være åpen om hvordan en har gått frem i forskningen, at en er redelig og nøyaktig.» (Larsen, 2017, s. 14)*

Det er i alle forskingsprosjekt viktig å se på ens egen forståelse, denne masteroppgaven er intet unntak. Valg av masteroppgave bygger på hvilken interesse en har, og hva en ønsker å studere nærmere. Gjennom både arbeidsliv og studieløpet har tema som kulturforståelse og maritim digital sikkerhet vært med på å påvirke både hvordan en tenker og handler, og digital sikkerhet sees på som en interesse.

Etter å ha både arbeidet og deltatt aktivt på arrangement innenfor den maritime næringen i flere år, blir en kjent med folk og selskap som arbeider innenfor næringen. Selskapet som har stilt opp for oppgaven er et en har kjennskap til, gjennom aktiv deltakelse i den maritime næringen. Gjennom hele prosessen har en satt sin egne forståelse og perspektiv til side etter beste evne.

# 4 EMPIRI

Formålet med empiri kapittelet er å skape en mening bak de funnene som er gjort i analysen. I analysen så en på de mønstrene og sammenhengene som kommer frem i dybdeintervjuene. Gjennom intervjuene med deltakerne blir det dykket ned i deres oppfatninger, erfaringer og eventuelle bekymringer knyttet til digital sikkerhet. Det er dette som danner grunnlaget for å utforske de ulike aspektene ved digital sikkerhet, fra hvordan samspillet mellom mennesker, teknologi og organisasjon er, samt hvordan selskapet og de ansatte jobber med digital sikkerhet i hverdagen. De perspektivene og utfordringene som kommer frem i analysen, vil brukes til å få frem et helhetlig bilde av digital sikkerhet i selskapet og hvordan det jobbes med dette både formelt og uformelt.

Empiri kapittelet er delt i flere deler. Den første delen vil ta for seg hvordan deltakerne resonnerer rundt begrepet digital sikkerhet og hvilke trusler de ser. Nøkkelord for empirien er selskapets struktur, standarder, sanksjoner, teknologi, kommunikasjon, kunnskap, bevissthet, holdninger og kultur.

## 4.1 Hva legger lederene i «digital sikkerhet»?

Innenfor litteraturen finnes det flere begrep som betyr mer eller mindre det samme som digital sikkerhet. Det er derfor naturlig å starte empirien med å forstå hva deltakerne legger i terminologien digital sikkerhet.

> *«Visst du sier digital sikkerhet da tenker jeg jo bevisstheten som vi har rundt alt vi gjør i jobb sammenheng digitalt, for så vidt også privat. Det å passe seg for å ikke bli lurt på digitale plattformer og være nøye med å sjekke hvilke vedlegg du åpner, hvilke eposter du åpner. Slette alt som er mistenkelig, ser mistenkelig ut. Også informere internt i organisasjonen når det er noe som er mistenkelig.» (Deltaker 3)*

Dette sitatet oppsummerer mye av det deltakerne tok opp. HR viser her til at digital sikkerhet er noe som en må være bevisst på både på jobb og privat, det at en tar inn over seg hva som kommer inn av e-post og tenker over det før en gjør noe med eventuelle vedlegg og lenker.

> *«Det er den største risikoen, at vi gjør noe vi blir manipulert til å trykke på.» (Deltaker 2)*

CFO bemerker at den største risikoen er at en skal bli manipulert til å trykke på noe en ikke burde. Selv sier han at det kommer mange spam e-poster, deriblant der avsender angivelig skal være fra CEO i selskapet som ber om utbetaling. For å jobbe med bevisstheten til de ansatte kommer det frem at simuleringer av slik type e-post er blant de tingene selskapet aktivt trener på. Det er nemlig ikke er bare CFO som mottar slike e-poster, enten de kommer fra simulering eller er ekte, så påpeker COO:

> *«[…] det er fryktelig mange som lar seg lure av falske e-poster eller det som er[…] trykke på lenker og det som hører til.» (Deltaker 4)*

HR resonnerte også rundt hva han ser som er den eksterne og den interne trusselen, der han viser til at den eksterne trusselen er de profesjonelle aktørene, hackerne. Mens den interne trusselen er bevisstheten til de ansatte. Selv sier COO at han er bekymret for naiviteten til enkelte:

> *«Naiviteten til veldig mange er vel min største frykt med tanke på digital sikkerhet. Det er veldig mange som er alt for naive og som ikke tenker seg om før de trykker på noe. Og da er risikoen for at noen kommer seg inn i systemet vårt relativt stor dersom vi ikke har fokus på det da» (Deltaker 4)*

Samtlige nevner mennesket på en eller annen måte i sine tanker rundt digital sikkerhet og hvilke trusler de ser, og med menneske henviser de til de ansatte i selskapet. Det er spesielt de ansattes bevissthet og væremåte som kommer frem i disse intervjuene. Hva det angår de ansattes rolle innenfor arbeidet med digital sikkerhet er IT-ansvarlig helt tydelig på hva han mener:

> *«Jeg tror du skal lete lenge etter en sikkerhetsansvarlig, eller hva som helst, som sier det at: mennesket er ikke de viktigste komponentene. Fordi, alt annet har vi kontroll på, altså har vi så god kontroll på som vi kan ha.» (Deltaker 5)*

Han nevner at mennesket er en viktig komponent, også på et annet tidspunkt viser han til at de er en viktig brikke, da det er de ansatte som kan stille seg de kritiske spørsmålene og vurdere situasjonen de står i.

Et annet poeng som blir tatt opp når en snakker om hva som legges i digital sikkerhet, er det å være bevisst på hvilken informasjon en gir fra seg. Hva en deler, og med hvem, er noe som både Site manager, COO og VP Project kommer inn på, men med ulike vinklinger. Site Manager bemerker viktigheten med sporfjerning, både digitalt og analogt. Han viser til at som selskap er det viktig å ta vare på sine bedriftshemmeligheter enten det er arbeidstegninger eller hvem som er leverandører av ulike deler.

> *«Jeg tror det er den plassen vi må være mest forsiktig. Det er litt analogt i forhold til det digitale du spør om. Men det å fjerne klistremerker, altså sporfjerning er en fin sånn forsvarsting som jeg er ganske god på.» (Deltaker 6)*

Site Manager mener han selv er ganske god på dette og legger til at mye kan gjøres selv for å sikre seg at en fjerner spor, enten det er klistremerker, som han viser til over, eller digitalt. Han tar opp problematikken med at kunder gjerne spør om informasjon om produktene som selges. Han viser til at dersom du videresender en pakkseddel fra din leverandør til kunden har du da også sannsynligvis gitt fra deg informasjonen om hvor du handler. Et eksempel han bruker er dersom det er snakk om olje til et produkt, da kan det være siste gangen du leverer olje til den kunden, for nå vet han hvor du handler det.

> *«At vi prøver å holde de tingene som er viktig for oss selv. Og det kan vi jo miste enten ved å være slepphendte, ha datainnbrudd eller at vi utgir dokumentasjon uten at det egentlig er mening.» (Deltaker 6)*

COO er opptatt av hva en deler og hvem en gir tilganger til og sier at dette er noe han snakker om med de ansatte han har lederansvar for, dette for å bevisstgjøre. To ganger forteller COO i intervjuet om sin skepsis knyttet til bruken av Microsoft Teams og sier at dette er noe han har prøvd å utfordre IT-ansvarlig på. Bakgrunnen for skepsisen er knyttet til at Microsoft Teams ikke ligger inne i Citrix eller VPN, det vil si at det er nok å bare koble til et nettverk for å komme inn. Han viser til at en noen få ansatte har tilgang til mange områder på Microsoft Teams og sier at dersom noen skulle få tilgang til hans Microsoft Teams så er det en ganske åpen historikk der inne for alt som skjer i selskapet.

VP Project er den siste som tar opp dette med hva en deler. Det første han sa da han hørte digital sikkerhet var GDPR (General Data Protection Regulation) regulativet. Han sier det å bli frastjålet identiteten sin må være ultimate trusselen for deg som person. Ved å rette blikket mot

GDPR viser han til at en må være bevisst på hva en kan dele på vegne av andre og at dette er noe spesielt de på prosjektavdelingen må ta stilling til i hverdagen.

> *«Det er at du kan skade andre ved å utlevere pass og personlig personnummer og sånne ting som kan bli misbrukt fra andre. Du stoler på den du sender det til, men som gjerne kan misbruke det videre. Da er vi inne på GDPR regulativet» (Deltaker 1)*

Forståelsen for hva som ligger i digital sikkerhet er i gruppen generelt samstemt og HR oppsummerer det hele med å si:

> *«Vi er jo aldri tryggere enn det svakeste leddet.» (Deltaker 3)*

## 4.2 Selskapets organisasjon og teknologi

### 4.2.1 Selskapets struktur

Digital sikkerhet handler om samspillet mellom mennesket, teknologi og organisasjon, og en del av dette omhandler formell organisering. Innledningsvis COO forteller at selskapet har vært gjennom noen endringer i årenes løp. Da selskapet for en tid tilbake gikk ut av et annet konsern ble det bestemt at i stedet for å ha en egen avdeling til å jobbe med digital sikkerhet, så ble jobben satt bort til en IT-leverandør.

> *«Jobber som COO i selskapet […] så var jeg vel også IT sjef i tiden etter vi gikk ut ifra […]» (Deltaker 4)*

I overgangsfasen han viser til, satt han selv som IT-ansvarlig i selskapet. Dette gjorde han frem til selskapet ansatte dagens IT-ansvarlig for et par år siden. Dagens IT-ansvarlig er alene om å ha rollen som han beskriver på følgende måte:

> *«På folkemunne er jeg dataansvarlig. Det er det jeg liker best å kalle det, jeg er ikke så glad i fancy titler. Men har da total ansvaret for IT, utstyr og telefoner, abonnement, drift, oppfølging, sikkerhet, egentlig alt.» (Deltaker 5)*

Her toner han selv ned rollen sin ved å si at han på folkemunne er dataansvarlig og at det er det han selv også liker best å kalle seg. Han legger også til at det er nok han som har hovedansvaret, etter CEO i selskapet, at det er CEO som har det øverste ansvaret. Videre sier IT-ansvarlig at

han har ansvaret for at eventuelle verktøy, systemer og overvåkning er på plass, men at han mener alle har et ansvar når det kommer til digital sikkerhet.

> *«Og når jeg sier overvåkning av trafikk, da gjelder det ikke å lese hva folk sende, men mer det at vi fanger opp om det er en klient, en node, et eller annet som oppfører seg rart i forhold, ja, til trafikkmønster da.» (Deltaker 5)*

Det å overvåke gjør at en kan følge med på om det skjer unormal aktivitet på ansatte sin datamaskin. Det er programvarer som gjør denne overvåkningen, og som sender ut alarmer til IT-leverandør og/eller IT-ansvarlig dersom noe trigger alarmen. CFO viser til at han fikk telefon fra IT-leverandør om at de merket noe unormal aktivitet på hans datamaskin. Han legger lettet til at det ble undersøkt og at de ikke fant noe unormalt når de gikk inn og sjekket.

### 4.2.2 Standarder og sanksjoner

Standarder kan uttrykkes og håndheves gjennom prosedyrer eller teknologi. Her ser en på standarder i sammenheng med de prosedyrer, retningslinjer og anbefalinger som er i selskapet. VP Project tok opp GDPR regulativet med en gang digital sikkerhet ble nevnt. Han viser til at prosjektavdelingen må forholde seg til prosedyrer rundt GDPR på en jevnlig basis, da de har med prosjekter som er rundtomkring i hele verden, noe som medfører at de på prosjektavdelingen arbeider med utsending av dokumentasjon i forbindelse med selskapets prosjekter. Han forteller at selskapet har en portal, et kvalitet og ledelsessystem, TQM (Total Quality Management) som alle ansatte har tilgang til ved innlogging.

> *«Ja det er der det lagres, og det er der vi finner det. Alt skal lagres der. Så er det veien dit som kan vær litt, kanskje litt vanskelig av og til for å finne, for der er så mange valg.» (Deltaker 1)*

Portalen har flere formål, lagring av selskapets prosedyrer og avviksrapportering er to av bruksområdene. Når det kommer til hvilke prosedyrer relatert til digital sikkerhet som ligger på TQM er VP Project noe usikker.

> *«[…] Jeg er faktisk usikker på hvilke prosedyrer som ligger der for digital sikkerhet. Men det fokuset som har vært og det som er så vil jeg, så er jeg ganske sikker på at det er prosedyrer på det, men jeg må innrømme at jeg har ikke lest den godt nok. […] Så vi har sterkt fokus på det, men om vi har prosedyrer, det vil jeg tro, men jeg er usikker.» (Deltaker 1)*

En annen som viser til noe usikkerhet rundt prosedyrer for digital sikkerhet er COO, som henviser til at dette er noe IT-ansvarlige har kontroll på. COO mener det ikke er noen prosedyrer for «vanlige ansatte», men at det er retningslinjer som IT-ansvarlig prøver å innføre. Både IT-ansvarlig og COO sier at det er vanskelig å vite om alle har fått med seg de retningslinjene som er presentert. HR på sin side viser til at en har prosedyrer på digital sikkerhet, men som han ikke kjenner til i detalj og viser til at dette er noe som IT-ansvarlig sitter med.

> *«Vi har jo en ypperlig IT-ansvarlig som har det høyt på agendaen. Og som gjennomfører mange tester for oss og sender ut mye for å lære oss opp.» (Deltaker 3)*

Når en sjekker med IT-ansvarlig hvilke prosedyrer selskapet har på digital sikkerhet sier han at det ikke er noen definerte prosedyrer på det, men at de har anbefalinger og at de også driver opplæring.

> *«Vi har jo litt opplæring på de ansatte. Frivillig sånn sett. Det ligger der, det er tilgjengelig, de får varsel om det, men det er ikke alle som gjør det likevel.» (Deltaker 5)*

For at de ansatte skal lære om digital sikkerhet gjennomføres det noen kurs i selskapet. Det blir blant annet nevnt at nyansatte får en presentasjon av IT-ansvarlig når de starter i selskapet. Den opplæringen IT-ansvarlig viser i sitatet over, er den e-læringen som selskapet har introdusert. Han viser til at den sånn sett er frivillig, da den ligger tilgjengelig og at den vil sende ut påminnelser til de som ikke har fullført de delene av kurset som ligger tilgjengelig. CFO kommenterer også e-læringen, han mener derimot at det er krav til å ta kursene, men at en ikke er god nok på å følge opp hvem som har tatt dem og ikke:

> *«Kurset der er bra, det er jo krav om at alle skal ha de, men det er ikke slik at du ikke får lønn om du ikke har tatt det og det blir purre mailer og sånt. Vi burde kanskje vært litt tøffere på å passe på hvem som ikke har tatt det, tror jeg.» (Deltaker 2)*

Samtlige nevner også e-post simuleringer som IT-ansvarlig sender ut med jevne mellomrom, for å se hvor mange som ser at det er en farlig e-post eller ikke. Også Site Manager viser til disse testene som IT-ansvarlig sender ut og sier at disse simuleringene er med på å holde bevisstheten oppe.

Når en ser på at uønskede hendelser kan oppstå ved å trykke på farlig e-poster, så er det relevant å også se på hvilke sanksjoner selskapet har når det kommer til uønskede hendelser innenfor digital sikkerhet. Kun en av seks sier at det er sanksjoner for dette:

> *«Ja, altså visst vi oppdager at ansatte gjør noe som er hodeløst og vi ser det, så vil det jo være naturlig å reagere med å gi en advarsel.» (Deltaker 3)*

En kan likevel se, at selv om de fem andre har startet med å si «nei», så viser flere av de også til at vedkommende på en eller annen måte vil få, kall det en mild, form for sanksjon. Enten i form av ekstra opplæring, oppfriskning om risikoen eller en liten påpakning. Site Manager sa med et smil:

> *«Nei, du må nok jobbe litt overtid for å være med å reparere dette her, men ikke noe utover det» (Deltaker 6)*

Det som helt klart kommer frem av disse svarene er at, det er ikke nødvendigvis det at vedkommende gjorde noe som brøt med digital sikkerhet som er viktig, det viktige er å vite hvordan en kan unngå det i fremtiden. CFO sin kommentar om sanksjoner er ganske oppsummerende på dette:

> *«Det har vi egentlig ikke tenkt på. Det kan jo skje den beste det. Vi må liksom finne ut hvorfor og hvordan, så må man jo finne ut hvordan vi kan stoppe at noen andre gjør noe lignende.» (Deltaker 2)*

Dette viser at selskapet har fokus på å etablere gode praksiser fremfor det å ta enkelt personer. IT-ansvarlig forklarer også at det ikke er alltid en kan finne årsaken til at den uønskede hendelsen har oppstått heller, og da er det vanskelig å straffe noen for det. På den andre siden sier han at dersom det er en tydelig handling for å skade selskapet så er det en annen sak og det da går på ansattforholdet. I en slik situasjon ville han tatt det med HR, han sier at det ikke er en prosedyre, men at det er det som er fornuftig å gjøre. Han legger også til at det helt sikkert står noe i kontrakten til hver enkelt ansatt at en ikke skal gjøre noe som kan gjøre selskapet vondt.

Site Manager viser til at det ofte kommer falske e-poster fra leveranseselskap. I en hektisk hverdag sier han det kan være lett å la seg lure av slike e-poster om en venter på en forsendelse og det haster. Det blir diskutert om han tror at en prosedyre eller en sjekkliste ville ha hjulpet de ansatte i slike situasjoner. Han tror gjerne det hadde hjulpet, men er usikker på om det hadde vært praktisk å gjennomføre, uten at han utdyper det noe videre.

Etter å ha snakker om prosedyrer på digital sikkerhet nevner både CFO, HR og IT-ansvarlig at det er en beredskapsplan på digital sikkerhet under utarbeiding av IT-ansvarlig og CFO. IT-ansvarlig sier fra sin side at den i grunn er klar for å bli publisert, men grunnet det kommende bytte av IT-leverandør er det blitt valgt å utsette utrullingen av denne til ny IT-leverandør er på plass, dette fordi beredskapsplanen vil trenge en større oppdatering etter byttet. Som HR nevner, så er det ikke alle som tenker på hacking når det er snakk om beredskapsplan.

> *«Når det handler om beredskap, de fleste tenker jo at det er personulykker, men det kan jo like gjerne være noe som skjer i forhold til hacking.» (Deltaker 3)*

Det at de tar opp beredskapsplan under diskusjon om prosedyrer er ikke så rart. En vil normalt si at en prosedyre er mer spesifikk og detaljert for handlinger som skal utføres i en bestemt situasjon. En beredskapsplan vil normalt gi en overordnet retningslinje, den vil ikke være like konkret med steg for steg som en prosedyre, i de fleste tilfeller. Hva som vil være tilfelle for selskapet kommer ikke frem av intervjuene.

### 4.2.3 Teknologisk infrastruktur og brukervennlighet

Innenfor teknologisk infrastruktur ser en på utstyr og programvarer, men også selve infrastrukturen i selskapets lokaler. Sistnevnte ble ikke kommentert i intervjuene, annet enn i bisetninger. Det som kom frem av intervjuene er de tekniske løsningene selskapet har når det kommer til programvarer, sikring på internett, samt hvordan bruken av dette oppleves av deltakerne.

Da VP Project tok snakket om TQM kom det frem at bruken av portalen ikke er like godt etablert hos alle avdelingene i selskapet. Han viser til at selskapet har tre forskjellige lokasjoner som alle stammer fra ulike bakgrunner, noe som gjør at selskapene har ulike behov. Selv sier han at prosjektavdelingen var tidlig ute med å ta TQM i bruk.

> *«Det er mange som ser på dette som en ekstra plage i hverdagen, men der inne, i TQM systemet, der ligger alle prosedyrene. Så er det dette med å finne de i TQM systemet, det oppleves at det fort kan bli litt, hva skal jeg si, rotete, litt vanskelig å finne.» (Deltaker 1)*

Han viser til at det kan være noe vanskelig å finne frem på TQM, at det oppleves som litt rotete. Når han snakker om TQM viser han til at portalen ble møtt med veldig stor motstand i avdelingene da selskapet lanserte det. Tolker en det VP Project sier videre riktig skyltes

motstanden mer enn bruken i seg selv. Det ene var at TQM også brukes til å rapportere avvik, noe som generelt genererer en del e-post og i starten førte det til en del støy fordi brukerne ikke var vant med å bruke det nye systemet. Når en skulle venne seg til det nye systemet, ble det i starten gjort litt feil, noe som skapte enda flere e-poster.

> *«Da ble det mer en konflikt i stedet for en nytte. Og det var det ikke meningen at det skulle være» (Deltaker 1)*

Han forteller også at like i forkant TQM implementeringen så ble Microsoft Teams introdusert i selskapet, noe som også møtte stor motstand. Det at TQM ble lansert, parallelt med Microsoft Teams ble introdusert, gjorde at det ble mye motstand på begge delene.

Ser en videre på selskapets bruk av Microsoft Teams kommer det frem at dette er selskapets intranett, som VP Project viste til over så ble det ikke tatt godt imot i starten. Microsoft Teams er den kanalen der IT-ansvarlig hovedsakelig sender og legger ut informasjon om digital sikkerhet.

> *«Pr. i dag så har vi teams, som vi bruker som kommunikasjon og informasjon om alt egentlig. Derav også IT-sikkerhet og IT-rutiner.» (Deltaker 5)*

COO viser til sin skepsis om at Microsoft Teams er intranett i selskapet. Det er ikke behov for noen ekstra innlogging for å komme seg inn, hverken på kontoret eller på reise. Han viser til at han og noen til i selskapet har mange tilganger i programmet og synes det er faretruende å tenke på hva som kan skje dersom noen får tilgang i deres tilgang til Microsoft Teams. Dette er noe han har utfordret IT-ansvarlig på, men det kom ikke frem om det har blitt sett nærmere på. Han trekker også frem hvilke tilganger en gir ut:

> *«Da er det spesielt forholdet mellom, altså, det vi velger å dele utad og det vi velger å gi folk tilgang til da. Både inn mot teams og hvilke informasjon som ligger på teams til ulike folk. […] Å klart, det vi har liggende på vår teams, som er relativt enkel å komme seg inn på visst en først kommer seg inn på pc-en til noen, er et faremoment som jeg ser i vårt sitt selskap.» (Deltaker 4)*

Dette tolkes dit hen at det ikke bare er kunder og andre leverandører han sikter til, men også om hvordan det gjøres internt i selskapet, da med hvilke valg en tar når det kommer til hvem som har tilgang og til hva.

Alle datamaskinene kommer ferdig installert med Office-pakken, inkludert Microsoft Teams og Outlook. Site Manager tar opp at de har fått en funksjon i Outlook, Mail Risk, som gjør at han enkelt kan sjekke om en e-post er mistenkelig eller ikke. IT-ansvarlig foreller at selskapet har prøvd å gjøre hverdagen til de ansatte med å installere denne funksjonen, av Secure Practice, i Outlook. Dette slik at de ansatte enkelt kan sjekke om e-postene de mottar. Site Manager synes konseptet er veldig lurt, men savner at svaret er litt tydeligere.

> *«Så det er klart det at når vi fikk laget en sånn funksjon i Outlook, at sånn "mistenkelig mail" knapp så er det jo kjempelurt for selskapet. Da er det veldig lett å teste, selv om at svaret fra "Mistenkelig mail" er veldig likt. Så om du tester en mail da, jeg kunne tenkt meg klare ja eller nei svar. Jeg liker ikke slike svar som "kan inneholde skummelt materiale"» (Deltaker 6)*

CFO er en annen som viser til flittig bruk av Mail Risk knappen og sier han synes det er veldig enkelt. Det er som Site Manager forklarte, at en får opp hva den analyserer e-posten til, i tillegg forteller CFO, viser den hvem du svarer dersom du svarer på e-posten, det er tilfeller der spam e-post kommer fra en e-post konto, men om du svarer på e-posten så blir det sendt til noen andre. Det er ikke alltid du får helt klare svar, som Site Manager peker på. Da kan en, som CFO tilføyer, sende den videre til IT-leverandør eller til Secure Practice for å få den sjekket ut nærmere, det kommer opp et valg om det.

I tillegg til programmene som de ansatte bruker i hverdagen, forteller IT-ansvarlig at datamaskinen kommer ferdig kryptert, med antivirus installert, konfigurert og oppdatert, alt klart slik at brukeren ikke skal måtte tenke på dette. Han legger til at det i tillegg er det installert Cisco Umbrella, som skal sperre for en del farlige sider som er kjente.

> *«Og så vil vi selvfølgelig ha sikker oppdaterte servere og applikasjoner på servere. Vi ønsker å ha sikre applikasjoner både de vi har, eier selv, og de vi abonnerer på, altså sånn type skytjeneste. Sikre på at det er kryptert trafikk, at det er at vi følger lover og regler.» (Deltaker 5)*

Han viser også til at det er de ansatte selv som til en viss grad styrer når oppdateringer skal skje, da det pleier å være lite populært at maskinen tar en tvungen omstart. Han viser da til at en kan ha jobbet med et dokument i flere timer som en da mister, dersom en ikke har lagret og da blir ikke IT-ansvarlig populær.

CFO informerer også om hvilke tiltak og regler som ligger til grunn dersom en skal koble seg på nettverk som er utenfor arbeidsplassen:

> *«Så har vi jo sånn veldig klare regler for, vertfall IT sier i vertfall det rundt med å logge på hotell nettverk og andre […] så må du i vertfall på VPN, før du eventuelt vurderer om du skal gå på via 4G eller 5G på mobilen og bruke VPN da. Jeg vet at det er noe av opplæringen var om dette med hjemmenettverket ditt og hvor bra du kode du har på det.» (Deltaker 2)*

Alle deltakerne snakket om VPN, i tillegg nevnte blant annet COO og Site Manager at selskapet også benytter seg av flerfaktor autorisering. Disse ble tatt opp i forbindelse med hvordan en kobler seg på nett og system når en er på reise eller hjemmekontor.

Da selskapet består av flere lokasjoner, hvor noen av lokasjonene er relativt nær hverandre, så ligger andre et godt stykke unna. Site Manager forteller at mellom lokasjonene har det blitt lagt en egen fiber, der en av de to lokasjonene som ligger nært hverandre har sentralen. Det å ha en egen fiber gjør at data ikke går via utlandet og blir kryptert inn igjen til Norge, men at det nå går i egen fiber. Dette medfører at det er mindre sjanse for at data blir plukket opp.

> *«Det er vel noe av det lureste jeg har hørt at vi holder på med.» (Deltaker 6)*

På tidspunktet intervjuene ble gjennomført var selskapet i gang med å bytte IT-leverandør, skifte var planlagt noen måneder etter intervjuprosessen var ferdig. Fire av seks tok opp dette med IT-leverandør og viktigheten med å ha en IT-leverandør som kan levere den sikkerheten og tjenestene selskapet trenger.

> *«Det er klart det, vi er en IT-avdeling med en mann, det er vel mer at han må overvåke og våre leverandører til å levere et bra produkt da. Det er det da, det er vårt mål da. Vi er helt avhengig av at vi har en leverandør som har kompetanse og system som hjelper oss på dette.» (Deltaker 2)*

COO legger frem at den IT-leverandøren de har hatt frem til nå har vært bra, men at de har sett at det er muligheter for å få det bedre. Når en har sett på hvordan selskapet skal løse dette har de sett på muligheten for å kjøpe tilleggspakker for å øke sikkerheten med nåværende leverandør, som er relativt dyrt. Alternativet er bytte til ny IT-leverandør som generelt har mer inkludert i pakken sin. Angående det planlagte skifte av IT-leverandør og de valgene som har blitt tatt sier IT-ansvarlig at dette valget er tatt ut av blant annet et sikkerhetsperspektiv.

*«Vi har kommet opp i en relativt stor størrelse og vi trenger egentlig umiddelbar hjelp visst-om-at det skulle skje noe. De nye har kontor på alle lokasjoner og kan komme på plass visst det skulle være noe.» (Deltaker 5)*

## 4.3 Kommunikasjon, kunnskap og bevissthet

Det kommer frem ulike kommunikasjonsformer i intervjuene. Blant annet viser IT-ansvarlig til at det er Microsoft Teams som er plattformen informasjon om IT-arbeid legges ut. VP Project viser til at digital sikkerhet blir kommunisert ut til de ansatte via allmannamøter og avdelingsmøter. Han viser til at det et par måneder før intervjuet, så ble det arrangert et avdelingsmøte hvor IT-ansvarlig var til stede og fortalte om viktigheten rundt digital sikkerhet. Han forteller videre at dette er noe som IT-ansvarlige gjorde med alle avdelinger. I disse møtte IT-ansvarlig personlig opp for å få øyekontakt med alle når han forklarte om digital sikkerhet og hvilken risiko selskapet har. Opplevelsen VP Project sitter igjen med, var at når noen først åpner samtalen så er den i gang. Han forteller at hans opplevelse var at det ble gode diskusjoner i møtet og mente på at flere av de som var til stede på møtet fikk seg noen overraskelser. Han sier at dette med å få det presenter ansikt til ansikt skapte en diskusjon. Om disse avdelingsmøtene sier IT-ansvarlig selv at han prøver å gjøre noe ut av det for å fange oppmerksomheten deres, slik at det han gjør blir husket.

*«Det som hjelper litt, det er å gå litt bananas. Prate til folk når, altså face-to-face, altså ikke via teams. Se de inn i øynene, prøve å tenne et eller annet i de, rett og slett gå litt crazy. Rett og slett for at de skal huske det, gjerne fordi at jeg var crazy, men da gjerne litt av budskapet også.» (Deltaker 5)*

Han opplever at denne metoden funker, men legger til at det er uvisst hvor lenge. CFO som også har deltatt på en av de andre avdelingsmøtene, sitter også igjen med at det ble stilt spørsmål og at det var fokus. Han legger til:

*«Tror de fleste er ganske bevisste dette da, men det er på en måte de her siste 10% som er den farlige biten da» (Deltaker 2)*

COO viser til at han tror interessene til de ansatte har noe å si også. Han har merket seg at det ofte er de samme personene som sender inn det de anser som trusler eller om mulige sikkerhetsbrudd, og at disse personene gjerne er de som har interesse for data og gaming. Videre viser han til at han tar praten med de han har under seg om hva en velger å dele, da spesielt hva en velger å dele utad og hva en velger å gi folk tilgang til. COO kommenterer også at han

reagerer når han går forbi tomme kontor hvor datamaskinen ikke er låst. Dette er ting som plager han, men som han føler at gjerne ikke plager andre like mye. Han sier han prøve å bevisstgjøre de andre ved å kommentere på om det var så lurt å gå fra datamaskinen ulåst.

Om arbeidet med bevisstgjøring i selskapet sier blant annet HR at en ser hvordan store og seriøse selskap har blitt hacket og at en hører at det har kostet mange millioner å få det opp å gå igjen, og viser til at det er ganske ødeleggende for et selskap da det kan sette en langt tilbake.

> *«Jeg synes det er utrolig positivt. Og jeg er så utrolig glad at vi har IT-ansvarlig på plass, som har så høyt fokus på det. Fordi det er jo det at, det er jo en av de største truslene våre faktisk. […] Og det er jo en kjempe fordel i forhold til industrispionasje og annet også, at vi øker bevisstheten vår.» (Deltaker 3)*

Han legger også til at han tror at bevisstheten i selskapet blir lavere, dess lenger ut i organisasjonen en kommer. HR om bevissthetsarbeid i selskapet:

> *«Og de som ikke har PC til vanlig, som kanskje ikke leser alt som kommer på teams, tror kanskje de er mindre bevisste enn oss andre. Men da kan det jo være aktuelt å ha egne møte med de for eksempel, for å informere om faren.» (Deltaker 3)*

Simulerings e-poster som sendes ut i selskapet er også med på å øke bevisstheten til de ansatte. HR kommentere at de kan se nedgang i antall folk som åpner lenker og som velger å dele informasjon.

Det at disse intervjuene ble gjennomført viser Site Manager til som et eksempel på hvordan det øker bevisstheten. Han sier at det gjør at han dagen etter kommer til å ta det opp i morgen møte, gjerne dagen etter også, men som han selv sier, om to uker er det gjerne ikke tema på morgenmøte lenger. Han sier også at:

> *«Jeg er veldig opptatt av at vi skal bestå i fremtiden. Så vi må ha fokus på det. Fordi vi lever i en slik verden. Så jeg opplever det som positivt at vi blir utfordret på det. Og det må ligge fremme i pannen på alle» (Deltaker 6)*

## 4.4 Holdninger og kultur

Fokus på digital sikkerhet er det en samstemt formening om blant deltakerne. Det blir tatt opp at det styres fra toppen og nedover i rekkene, en av de som sier at det starter i toppen er COO.

Han viser til at det starter i ledergruppen og at det i anledning ansettelse av IT-ansvarlig ble gjort endringer strukturen til selskapet. Frem til da var det COO som hadde hatt ansvaret for digital sikkerhet, men når IT-ansvarlig ble ansatt ble det flyttet fra COO til CFO:

> *«Det er CFO som styrer datasikkerhet sammen med IT-ansvarlig da, og så rapporterer han det inn da til CEO […]» (Deltaker 4)*

En annen som viser til at det styres fra ledelsen og mener det må være slik er Site Manager. Han mener at dersom ansvaret blir tatt nedover i organisasjonene til Site Manager eller avdelingsledere, så vil de alltid prioritere oppgaver som bringer selskapet fremover. Han mener avdelingsledere ikke vil prioritere det han kaller «stille problem» når det er andre oppgaver som bringer selskapet fremover, eventuelt de som maser og truer mest.

> *«Det må være styrt i fra ledelsen at vi ønsker at det skal være noe bedriften skal være bestemt god på.» (Deltaker 6)*

Han sier også på et annet tidspunkt at det gjerne kunne vært litt lenger oppe på agendaen nedover i rekkene også. IT-ansvarlig sier også at fra toppen av er det godt fundamentert. Men han på sin side skulle ønske at den aktive deltakelsen, fra avdelingsledere spesielt, kunne vært større.

> *«Jeg savner kanskje mest den aktive deltagelsen fra avdelingsledere, kanskje spesielt da. Jeg tror ikke det handler om at de synes det er uviktig, men de har så mange ting å gjøre at det blir ikke prioritert.» (Deltaker 5)*

IT-ansvarlig viser her til at han ikke tror det blir prioritert fordi avdelingslederne har andre ting de må gjøre, som er det Site Manager også viste til. Site Manager viser også til at det til tider kan komme mye e-poster og at dersom en da er opptatt eller har mye som skjer, så er det lett for å trykke seg gjennom e-postene og ikke lese mer enn starten av dem, spesielt om det er slike informasjons e-poster. En idé han trekker frem er at når viktig informasjon om digital sikkerhet skulle ut, skulle det vært slik at det låste e-posten, slik at en måtte gå gjennom et kort skjema og huke av på noen spørsmål. Noe som ikke skulle tatt mer enn et minutt. Det ble da stilt et oppfølgingsspørsmål om det var noe han hadde gjort uten å la seg irritere over at e-posten var låst. Han sier han hadde gjort det, om han hadde blitt irritert svarte han ikke på, men han la til at det ville hjulpet å vite at dette var noe alle måtte gjennom.

Det kommer frem i intervjuet med IT-ansvarlig at han opplever at det som kommuniseres ut om digital sikkerhet ikke alltid blir lest. Han trekker frem eksempel ved at han kan ha sendt ut en informasjons e-post og ikke lenge etter ringer noen og spør om akkurat det e-posten fortalte. Av årsakene han trekker frem er det ikke at de ansatte ikke forstod budskapet, det er mer at de ikke har sett eller lest det som kom ut og syntes det var lettere å ringe enn å lete. Han forteller videre at han har laget en plan på hva de ansatte skal gjøre i ulike situasjoner, men at han ikke har distribuert denne planen.

> *«Og der har jeg skrevet, men ikke distribuert hva de ansatte er nødt til å ta hensyn til i de forskjellige situasjonene. For det er et 5 siders dokument som ikke vil bli lest og som vil bli glemt etterpå.» (Deltaker 5)*

Han viser til at grunnen for å ikke ha distribuert dokumentet er grunnet forventningen om at det ikke vil nå frem til de som skal ta til seg budskapet.

Videre viser IT-ansvarlig til at han skulle ønske at flere av de ansatte stilte seg selv noen kritiske spørsmål når de for eksempel mottar en e-post med lenke i.

> *«[…] de ser kanskje ikke at de er en brikke, de ser ikke at de er et mål, de ser ikke at de er en vei inn og de stiller alt for lite kritiske spørsmål til, ja, til ting som kommer inn. Altså skal det klikkes på, er det et vedlegg, burde det være et vedlegg, hvem som har sendt den, hvorfor sendte de den, hvorfor fikk jeg den e-posten, og sånne ting, forventer jeg det. Masse slike kontrollspørsmål som egentlig bare de ansatte kan stille seg.» (Deltaker 5)*

Videre tar han opp utfordringen han opplever med å nå frem til de som ikke stiller seg disse kritiske spørsmålene, at det gjerne er de som vegrer seg for både endringer og annet.

> *«Men det er jo vanskelig å komme inn i hode på de som ikke gjør det da. For de er gjerne litt sånn reserverte, gjerne ikke blant de yngre og vegrer seg litt på både endring og annet.» (Deltaker 5)*

IT-ansvarlig mener det ikke er blant de yngre han møte mest utfordring. Han legger også til at han håper at noen generasjonsskifter så vil det bli bedre. En annen som tar opp alder er COO, han mener at en må lære de eldre at de er en brikke som hackerne ønsker å utnytte for å komme inn i selskapets systemer.

> *«[…] Og så er det vel ikke til å legge skjul på at akkurat med slike ting som dette der, så er det kanskje den eldre generasjonen som er litt mer naive enn den yngre da. Etter hvert som du får yngre folk inn så, ja, er ikke sannsynligheten like stor for at det er de som går inn. Da er det mer å lære de eldre at her er det faktisk noen som prøver å lure de.» (Deltaker 3)*

Det er ikke bare å si at i dette selskapet skal vi ha god sikkerhetskultur, sier IT-ansvarlig. Han viser til at en må jobbe med å øke de ansattes fokus. Han viser til at han i møter med de ulike avdelingene har oppfordret til å snakke om det ved kaffemaskinen, dersom en har fått en mistenkelig e-post så snakker en om det med andre, ta opp ting som gjør en usikker. Han ønsker at de ansatte skal ha en dialog på det og med dette få opp bevisstheten om at dette er noe vi må tenke på.

> *«Jeg kan jo ikke fortelle at her skal vi ha en sikkerhetskultur – YES. Det er opp til alle ansatte.» (Deltaker 5)*

I diskusjonen som var med Site Manager blir det tatt opp at en kan kjøpe de beste systemene på markedet, men at det gjerne blir som en falsk trygghet dersom de ansattes holdninger eller sikkerhetskultur ikke er på plass.

Et annet aspekt med bevisstgjøring er hva det gjør med en å høre om andre selskaper som har vært utsatt for alvorlige hendelser knyttet til digital sikkerhet. Ut fra intervjuene virker det til å ha være en sunn påminnelse om hvor lett ting kan skje og hvor alvorlig det er for selskapet. CFO viser selskap som har hatt datainnbrudd og som hadde systemene nede i lang tid og hvor kostbart det var for selskapet. Det at andre selskap har vært åpen om at de har hatt datainnbrudd sier han ikke endrer synet han har til dem, ei troverdighet. Han viser til at han kjenner til hvordan der er å jobbe mot digital sikkerhet og at det nesten er umulig å være 100% sikret mot at noe slikt skal skje. Han sier at når han hører om selskap som har hatt datainnbrudd er tanken heller «håper ikke det skjer oss». Om hva han tror selskapet hadde gjort i samme situasjon sier han at han ikke egentlig har tenkt over, men han tror at de ville valgt å være åpen om det. Og viser til at med et par hundre ansatte skal det noe til å holde det hemmelig uansett.

Også VP Project sier han i grunn synes det er bra at en deler. Han viser til at å innrømme at en har trykket på en lenke som viste seg å være farlig ikke er noe han ser poeng i å hemmeligholde. Det er fint å kunne lære av andre sine feil legger han til. Han sier likevel at det kan hende det

er situasjoner som gjør at det kan føre til at det ikke bør deles, men han har ikke noe eksempel på hva det skulle være.

Det å være et selskap som har vokst en del, så sier COO at det å profilere seg i media også gjør at en blir mer utsatt, og når en ser hvor sårbart det er for selskap dersom noen virkelig går inn for å skade, det viser bare hvor viktig det er å jobbe med og ha fokus på digital sikkerhet.

Flere bemerker seg verdensbilde som er, der HR tar opp at det er ikke mange år siden en bekymret seg over hva som skjer dersom strømmen skulle forsvinne. Nå sier han at dersom noen skulle klare å ta ned internett så vil det påvirke samfunnet på et helt annet nivå, og viser til at samfunnet vårt i dag er sårbart på en helt annen måte enn før.

# 5 DRØFTING

Den stadige økningen innen digitalisering kommer med både muligheter og utfordringer. I dag utvikles informasjonsteknologi i stadig større hastighet, og evnen til å beskytte sine sensitive data og ressurser er avgjørende for at selskap skal kunne bestå i fremtiden. Det merkes også at hackerne ikke lenger er «*unge gutter som sitter på rommet sitt*» *(Deltaker 4)*, som det blir sagt i et av intervjuene etterfulgt av *«det er profesjonelle aktører med høy utdanning.» (Deltaker 4)*

I forrige kapittel ble de mest sentrale funnene fra intervjuene presentert, nå begynner jobben med å trekke linjer mellom funnene og teorien. Før så en gjerne på digital sikkerhet som en teknologisk utfordring, men det som kommer frem i funnene er at det ikke bare er teknologien som spiller inn. Dette gjenspeiles i teorien, hvor Schiefloe (2021) i sin diskusjon viser til Orlikowski (2009) om den tredje tilnærmingen til teknologi i organisasjonsforskning, der poenget er det å forstå bruken av teknologien og teknologiens betydning som resultat av et komplekst samspill mellom atferd, narrative og institusjonelle kontekster.

I en organisasjonsanalyse er både mennesket, teknologi og organisasjon i sentrum. Schiefloe (2021) presenterer i sin bok «Organisasjonsanalyse» et nyttig hjelpemiddel for analysering av store mengder data, pentagonmodellen. Pentagonmodellen er, som tidligere nevnt, et hjelpemiddel for å trekke linjer mellom de ulike kategoriene ved drøfting av funnene opp mot relevant teori. En vil med dette kunne se hvordan det formelle påvirkes av det uformelle, hvordan det uformelle påvirker det formelle, og hvordan påvirkningene innad i disse to hovedkategoriene også oppstår. Illustrert i Figur 3Figur 6 ser en hvordan de ulike kategoriene påvirker hverandre. Organisasjonsanalysen er delt opp i kapitler basert på utvalgte spørsmål som er relevante for problemstillingen. Innledningsvis vil det bli sett på hva som legges i digital sikkerhet fra ledelsens sin side, da med fokus på forståelse, trusler og sanksjoner. Videre undersøkes selskapets strukturelle oppbygging, etterfulgt av en gjennomgang av de standarder og teknologier som blir vektlagt i intervjuene. Deretter undersøkes tilnærmingen ledelsen har til bevissthet omkring digital sikkerhet, og avslutningsvis en vurdering av hvordan sikkerhetskulturen oppleves.

## 5.1 Hva legges i digital sikkerhet, sett fra ledelsens perspektiv?

Innledningsvis i empirien ble det undersøkt hva deltakerne la i digital sikkerhet. Som Jøsang (2021) tar opp har tiden en lever i noe å si hvilke begrep en velger om digital sikkerhet og at det var først i 2019 begrepet digital sikkerhet ble tatt i bruk i Norge. Siden det er et relativt nytt utrykk er det naturlig å tenke at begrep som IT-sikkerhet og datasikkerhet fremdeles er uttrykk en møter i dagligtalen. Ut fra intervjuene oppleves det slik at det gjerne ikke er terminologien digital sikkerhet deltakerne selv bruker mest, dette da de i intervjuet i tillegg viste til IT-sikkerhet og datasikkerhet, men ut fra den informasjonen som kommer frem ved bruk av begrepet digital sikkerhet tolkes det til at begrepet ikke var noen utfordring å forstå.

Rettes blikket mot hvilke trusler og bekymringer deltakerne ser er hacking et moment som trekkes frem. Det å bli hacket er en form for uønsket hendelse, der noen har et ønske om å påvirke selskapet i en negativ forstand (Bergsjø & Windvik, 2018). På eksempler om hvordan de er bekymret for hacking viser deltakerne til det å få e-poster med farlige lenker eller vedlegg. Dette er også det Bergsjø og Windvik (2020) viser til som en av de viktigste kanalene hackerne anvender for å plante ondsinnet kode på en datamaskin i norske selskap. Bergsjø og Windvik (2020) poengterer viktigheten av at de ansatte må ha en mulighet til å forstå en risiko, det vil med andre ord si at det kreves at de ansatte har kunnskap om digital sikkerhet.

> *«Naiviteten til veldig mange er vel min største frykt med tanke på digital sikkerhet. Det er veldig mange som er alt for naive og som ikke tenker seg om før de trykker på noe. Og da er risikoen for at noen kommer seg inn i systemet vårt relativt stor dersom vi ikke har fokus på det da» (Deltaker 4)*

Her trekker HR blant annet frem at naiviteten hos enkelte ansatte som hans største frykt. Han viser til da ansatte ikke tenker seg om før de trykker på lenker i e-poster. En annen som trekker frem naivitet er COO, som viser til at den eldre generasjonen gjerne er mer naiv enn den yngre generasjonen. Aldersrelaterte utfordringer blir også påpekt av IT-ansvarlig, som tror at situasjonen vil være annerledes etter noen generasjonsskifter. Noe IT-ansvarlig viser til er at mange ansatte ikke stiller seg de kritiske spørsmålene før de handler, som om det er en e-post de forventer, om det er forventet at det skal være et vedlegg og den slags. Bergsjø og Windvik (2020) spesifiserer at det ikke er nok at de ansatte bare vet at dette er noe som kan skje, men at de i tillegg blant annet må kjenne til hyppigheten av slike forekomster. For at de skal vurdere e-postene som kommer inn trenger de også å vite hva som kjennetegner en utrygg e-post for å kunne gjøre en slik vurdering. IT-ansvarlig legger til at kanskje de ansatte ikke forstår hvilken

brikke de har, at de ikke har fått med seg at de selv faktisk er et mål for hackere som for eksempel har til hensikt å skade selskapet.

> *«Jeg tror du skal lete lenge etter en sikkerhetsansvarlig, eller hva som helst, som sier det at: mennesket er ikke de viktigste komponentene. Fordi, alt annet har vi kontroll på, altså har vi så god kontroll på som vi kan ha.» (Deltaker 5)*

Ser en til forskning, viser den til at i de fleste granskninger av ulykker trekkes menneskelig svikt frem, men at det sjeldent blir stående som eneste årsak og at en gjerne retter blikket mot organisasjonen for å se på konteksten (Schiefloe, 2017). IT-ansvarlig viser over til at han mener mennesket er den viktigste komponenten, og at selskapet kan investere i de beste systemer og ha de beste leverandørene, men når en situasjon oppstår så er en avhengig av hvordan den ansatte reagerer. Hvordan en ansatt reagerer er avhengig av den ansattes forståelse for situasjonen og kunnskap, noe som er avgjørende for om situasjonen kan avverges eller ikke. Det er nødvendig, som nevnt over, at de ansatte har fått det de trenger for å kunne forstå risikoen og derav handle ut fra det risikobildet de ser. Et eksempel fra intervjuet med IT-ansvarlig er at ikke alle ansatte har en egen datamaskin, det at en ikke jobber med den slags teknologi i hverdagen vil nok kunne medvirke til at vedkommende vil ha et annet risikobilde enn en som sitter fremfor datamaskinen hele dagen. Selv om en har god forståelse for risikobildet kan en likevel gjøre feil, Bergsjø og Windvik (2020) viser til at noen kan overvurdere sin egen evne til å kontrollere risiko. Schiefloe (2017) viser til at det er flere typer menneskelig svikt: feilvurdering, feilhandling, utelatelser eller koordineringsfeil. Når en ser på forholdet mellom de ansatte og de miljøene de jobber i ser en på menneskelig faktor. De ansatte påvirkes av hvilke utstyr de har til å gjennomføre oppgavene sine (Schiefloe, 2021).

CFO viser til at han gjerne mottar e-poster som utgir seg for å være fra CEO om en betaling som må gjennomføres. Bergsjø og Windvik (2020) viser til det som kalles direktørsvindel som et eksempel når de sier at svindlerne blir frekkere og frekkere. Direktørsvindel startet på den måten som CFO her forklarer, en enkel e-post til økonomiansvarlig om en regning som må betales eller en hasteoverføring. Som det kommer frem i teorien, kom disse e-postene tidligere formulert på dårlig norsk, noe som gjorde det lettere å gjennomskue, men i de siste årene viser Bergsjø og Windvik (2020) til at det er blitt flere nordmenn, eller folk som er gode i norsk, som står bak direktørsvindel. I tillegg så ble det gjerne oppgitt utenlandske kontoer tidligere, mens det nå går til norske kontorer som tilhører et «firma» eller en person. Svindlerne tar ikke selv

risikoen lenger og har gjerne fått inn noen som trenger raske penger, eller som er naive, til å gjøre overføringen fra disse norske kontoene til utenlandske kontoer.

E-poster er det som kommer tydeligst frem når en ser på hvilke trusler som bekymrer deltakerne. Site Manager viste til hvordan de som arbeider med leveranse og mottak ofte blir utsatt for falske e-poster fra leverandørselskap og viser til at når en venter på en forsinket leveranse og en e-post med sporing dukker opp er det lett for å klikke på sporingslenken om en er stresset. Site Manager viste også til at tidligere var minnepenn en større trussel, da med eksempelet at en finner en minnepenn på parkeringsplassen, kobler den i datamaskinen og med det har åpnet opp for hackerne. Han ser det ikke som trolig at dette er noe ansatte gjør i dag. Når en over lenger tid har fått opplæring om bruken av minnepenner, er det naturlig å tolke det til at det nå er blitt en sosial norm innenfor selskapet sin sikkerhetskultur og blir da som en form for retningslinje (Bergsjø & Windvik, 2020). IT-ansvarlig legger også til at han har gått ut med at minnepenner skal ikke brukes på selskapets datamaskiner med mindre en har kjøpt en ny minnepenn og har full kontroll på hva som er på den.

Blant deltakerne presiserte både HR og VP Project at en må huske at den digitale sikkerheten ikke bare er for selskapet, men også for de ansatte personlig. En trussel som også løftes frem som påvirker den ansatte personlig, er det å bli frastjålet identiteten sin. Det at ens identitet er på avveie kan føre til at andre personer utgir seg for noen de ikke er, hvor en vanlig form for dette er ved å søke etter kredittkort, lån eller andre økonomiske måter (Bergsjø & Windvik, 2020). VP Project legger spesielt vekt på at en som selskap må tenke nøye over GDPR, da med tanke på hvilken informasjon en gir ut om andre.

Truslene som her omtales kan føre til uønskede hendelser, og som Bergsjø og Windvik (2020), samt Schiefloe (2017) påpeker, er det ofte mennesker, her de ansatte, som er involvert i slike uønskede hendelser. I lys av slike uønskede hendelser, er det også naturlig å se på hvilke sanksjoner selskapet har. Selv om fem av seks deltakere svarte at det ikke var noen sanksjoner, la de likevel til at det gjerne ville bli noe ekstra opplæring eller oppfølging i etterkant for de det gjaldt. HR på sin side var ganske tydelig på at det er naturlig å reagere med en advarsel dersom ansatte gjør noe alvorlig som fører til en uønsket hendelse.

> *«Ja, altså visst vi oppdager at ansatte gjør noe som er hodeløst og vi ser det, så vil det jo være naturlig å reagere med å gi en advarsel.» (Deltaker 3)*

Også IT-ansvarlig viser til at dersom det er ansatte som bevisst handler slik at en uønsket hendelse oppstår så tas det videre til HR, da dette går på ansettelsesforholdet til den ansatte. Det både IT-ansvarlig og CFO legger vekt på, fremfor sanksjoner, er å forstå hva der er som har skjedd og hvordan en kan unngå en slik uønsket hendelse i fremtiden.

Det kommer frem av intervjuene at fokuset til selskapet er å etablere barrierer og gode praksiser når det kommer til digital sikkerhet, fremfor å straffe de som da har vært involvert i en uønsket hendelse. Selv om IT-ansvarlig og CFO var tydelig på at det å forstå situasjonen var viktig, indikerer kommentarer om advarsel, opplæring og oppfølging et ønske om å påvirke forholdene slik at lignende hendelser ikke gjentar seg. Dette er en del av sikkerhetshjulet (Figur 3) som Bergsjø og Windvik (2020) viser til når de snakker om syklusen sikkerhetsarbeid går i. At for å øke kompetansen må det være en hendelse en har undersøkt, for å ha en hendelse å undersøke må en ha sikkerhetsovervåkning. For å ha rett sikkerhetsovervåkning er en avhengig av god og riktig deteksjonsteknologi som igjen bygger på hvilken kunnskap en sitter med når en bestemmer deteksjonsteknologien en skal bruke.

> *«Det er fremst av intervjuene at fokuset til selskapet er å etablere barrierer og gode praksiser når det kommer til digital sikkerhet, fremfor å straffe de som da har vært involvert i en uønsket hendelse. Selv om IT-ansvarlig og CFO var tydelig på at det å forstå situasjonen var viktig, indikerer kommentarer om advarsel, opplæring og oppfølging et ønske om å påvirke forholdene slik at lignende hendelser ikke gjentar seg. Dette er en del av sikkerhetshjulet (Figur 3) som Bergsjø og Windvik (2020) viser til når de snakker om syklusen sikkerhetsarbeid går i. At for å øke kompetansen må det være en hendelse en har undersøkt, for å ha en hendelse å undersøke må en ha sikkerhetsovervåkning. For å ha rett sikkerhetsovervåkning er en avhengig av god og riktig deteksjonsteknologi som igjen bygger på hvilken kunnskap en sitter med når en bestemmer deteksjonsteknologien en skal bruke.»*

NSM sin risikorapport for 2023 viser til at økonomi er en faktor som spiller inn på sikkerheten i norske selskaper. Økonomiske utfordringer kan gjøre at noen selskap, gjerne de mindre, velger å spare inn penger når det kommer til digital sikkerhet. Om dette sier NSM:

> *«Sikkerheten vår blir ikke bedre enn det svakeste leddet i leverandørkjeden»*
> *(Nasjonal sikkerhetsmyndighet, 2023, s. 9)*

Mens NSM viser til leverandørkjeden i sin diskusjon rundt de økonomiske utfordringene, viser også HR til at han mener at det svakeste leddet påvirker sikkerheten, på en mer generell basis:

> *«Vi er jo aldri tryggere enn det svakeste leddet.» (Deltaker 3)*

## 5.2 Hvordan er den formelle strukturen til selskapet?

Deltakerne som har vært med i intervjuene sitter enten med en form for lederrolle eller spesiell kunnskap om digital sikkerhet og ikke alle sitter på samme lokasjon, da selskapet er delt over flere lokasjoner. Om hvem som har ansvar for digital sikkerhet, tolkes det slik at de fem lederne har en felles formening om at ansvaret for digital sikkerhet ligger hos IT-ansvarlig. Bergsjø og

Windvik (2018) viser til at innenfor ledelse for datasikkerhet er det ikke lenger tilstrekkelig med å kun ha egne sikkerhetsavdelinger som jobber med det. Allerede i 2012 tok Bjørnsen (2012) opp at den nye epoken en er inne i krever mer deltakelse og tilstedeværelse fra ledelse og eventuelle styrer. Videre viser Bergsjø og Windvik (2020) til at det er viktig at de som jobber med de ansatte i det daglige får et større ansvar for å følge opp; det er de som ser de ansatte i det daglige og kan følge med på hvordan digital sikkerhet i praksis fungerer. Den aktive deltagelsen nedover i organisasjonen, da spesielt fra avdelingsledere, er noe IT-ansvarlig trekker frem som noe han savner i selskapet. Han presiserer at han ikke tror det handler om hva som er viktig og uviktig, men at det er prioriteringene som blir gjort når det er mye å gjøre, som fører til at digital sikkerhet ikke havner øverst på prioriteringslisten. Site Manager viser til dette med prioritering, at en avdelingsleder, også andre, prioriterer de oppgavene som bringer selskapet fremover, og at arbeid med digital sikkerhet da blir sett på som et «stille problem» som havner lenger ned i bunken. Dette med å prioritere oppgavene som bringer en fremover ser en på som en av effektene av sosial kapital på et høyt nivå, at en setter de oppgavene som bringer selskapet fremover over sine egne personlige mål (Schiefloe, 2021). Samtlige av deltakerne mener at fokuset på digital sikkerhet står høyt hos selskapet. Selv om selskapet har høyt fokus på digital sikkerhet, tolkes det basert på kommentarene Site Manager og IT-ansvarlig legger frem, dit hen at arbeid med digital sikkerhet ikke blir kategorisert som «det som bringer selskapet fremover», på lik linje med de arbeidsoppgavene Site Manager viser til.

En annen ting Site Manager viser til er arbeidet med sporfjerning, både analogt og digitalt, dette viser han til er noe han er god på. Med sporfjerning henviser Site Manager til det han kaller «analogt arbeid», det å for eksempel fjerne en etikett på en pappkasse før du bruker pappkassen på nytt til en ny forsendelse. En kan også se på sporfjerning digitalt, noen ganger kan kunder sine spørsmål svares på raskere om en videresender en pakkseddel, ulempen er at en pakkseddel gjerne inneholder informasjon en ikke ønsker kunden skal ha. Her er to moment som er essensielt å se videre på. Det første er at de som best kan følge opp at sporfjerning blir gjort, enten analogt eller digitalt, er de som er nærmest de ansatte, altså avdelingslederne. I tillegg kommer det frem at det kun er en IT-ansatt i selskapet og at selskapet har flere lokasjoner, det er da tydelig at IT-ansvarlig ikke kan være på alle lokasjonene til enhver tid. Bergsjø og Windvik (2018) understreker at avdelingsledere, eller mellomledere, er de som befinner seg nærmest de ansatte, og at de derfor ha digital sikkerhet på agendaen. Det andre poenget som kommer frem med sporfjerning er at det er en måte å opprettholde konfidensialitet, at informasjonen ikke blir tilgjengelig til uautoriserte individer (Bergsjø & Windvik, 2018).

IT-ansvarlig presiserer at det ikke er han som sitter alene med ansvar når det kommer til digital sikkerhet, selv mener han at litt ansvar ligger hos alle de ansatte, men at hans ansvar ligger i å tilrettelegge for at de systemer, oppsett og verktøy er på plass. All organisering bygger på arbeidsdeling og koordinering (Shiefloe, 2021), en kunne gjerne her inkludert de ansatte inn i ansvaret med å koordinere kjente oppgaver ved å ha prosedyrer og regelverk på digital sikkerhet. IT-ansvarlig viser til at etter CEO så er det nok han selv som sitter med hovedansvaret, men at det totale ansvaret ligger hos CEO.

Det kommer også frem at selskapet har vært gjennom noen endringer i årenes løp, der blant annet roller har blitt byttet. Det kommer også frem at selskapet, etter en omfattende endringsprosess for noen år siden, besluttet at arbeidet med digital sikkerhet skulle overføres til en ekstern IT-leverandør istedenfor å etablere en intern avdeling for oppgaven. Under intervjuene kommer det frem at selskapet er i en prosess med å bytte IT-leverandør, og at det byttet ville skje i løpet av de neste månedene. Av vurderingen fra bytte ble det nevnt at økonomi og hva de kunne tilby i sin pakke var faktorer som var avgjørende i beslutningen. Også det faktum at ny IT-leverandør har kontor i nærheten av alle lokasjonene til selskapet og kan møte opp fysisk om det skulle være behov for dette. Fra selskapets side er det IT-ansvarlig som følger opp IT-leverandøren og koordinerer den delen.

## 5.3 Hvordan arbeides det med standarder og teknologi fra ledelsen sin side?

Om arbeid med prosedyrer for digital sikkerhet i selskapet var det noe usikkerhet om hva som fantes av prosedyrer, hvem de gjaldt og hvor en kunne finne disse. VP Project tok opp at han var usikker på hvilke prosedyrer som var, sa han trodde selskapet hadde dette, men at han kunne innrømme at han da ikke hadde lest de godt nok. HR tar opp at det er prosedyrer, men annet enn det som står i personalhåndboken kjenner han ikke til. Han henviser til at dette er noe IT-ansvarlig har kontroll på. Samme gjør COO og legger til at det ikke er noen prosedyrer for «vanlige» ansatte som han vet om, men at det er noen retningslinjer som IT-ansvarlig har prøvd formidle ut i selskapet. Ser en til Barley (2020) ser en at samspillet mellom posisjon, rolle og rolleforhold, en kan stille spørsmål ved hvordan samhandlingen mellom lederne og IT-ansvarlig er om de ikke vet om det er prosedyrer knyttet til digital sikkerhet når det flere ganger blir poengtert at digital sikkerhet er noe selskapet har høyt fokus på. Selv om flere var inne på at det trolig var prosedyrer på digital sikkerhet sier IT-ansvarlig at det ikke er noen definerte prosedyrer.

> *«[…] ikke definerte prosedyrer nei. Men vi har anbefalinger og er det et problem så skal en ringe IT-leverandør». (Deltaker 5)*

IT-ansvarlig viser til at det er anbefalinger, som også COO tok opp, men ikke noen definerte prosedyrer. Anbefalinger er veiledning og råd, mens prosedyrer er klare steg-for-steg for hva en skal gjøre i en gitt situasjon. Slik en tolker IT-ansvarlig har han forberedt et dokument på fem sider om hva de ansatte skal gjøre i ulike situasjoner, men legger til at det ikke er distribuert ut enda da det må settes opp på en måte som gjør at det blir lest.

I Outlook har de ansatte en funksjon som kalles Mail Risk. Secure Practice er selskapet som leverer e-læringen selskapet benytter som en del av sin opplæring og som også leverer Mail Risk funksjonen i Outlook. Denne funksjonen er for at de ansatte skal ha mulighet til å analysere e-post som kommer inn. Dersom en ansatt bruker Mail Risk vil den gjøre en analyse av e-posten og gi en tilbakemelding på om e-posten fremstår som mistenkelig eller ikke. Bergsjø og Windvik (2020) viser til sikkerhetshjulet, med overvåkning og teknologi som brukes for å gjøre overvåkning. De e-posten som ansatte sjekker med Mail-Risk er e-post som har kommet gjennom de vanlige sikkerhetsbarrierene som overvåker mai for å luke ut e-poster som ser mistenkelig ut. Dette er ny teknologi som de ansatte har tatt i bruk og som modifiserer arbeidspraksis, som Barley (2020) viser til, Mail Risk endrer hvordan de ansatte håndterer en mistenkelig e-post og hvordan de handler når de mottar en. Med å se på eksempelet med Mail Risk, ser en at blant retningslinjer og anbefalinger finner en også programvarer som de ansatte bruker i hverdagen. Slik en tolker Bowker og Star (1999), med å si at noen programvarer er fryste politiske diskurser, så vil det si at noen av de programvarene som selskapet bruker, er med på å styre hvordan den ansatte jobber og på den måten er det en form for prosedyre. Andre teknologiske barrierer som deltakerne tar opp og viser til at brukes er VPN og flerfaktor autorisering, og viser til at det er anbefalinger fra IT-ansvarlig som viser til at en skal bruke VPN når en er på reise. Site Manager tar også opp at selskapet bruker fiber mellom lokasjonene for å unngå at informasjon må til utlandet, noe som også viser til en av selskapets tiltak med sikkerhetsbarrierer.

IT-ansvarlig viser til at rollen hans blant annet innebærer å kontrollere at overvåkning er på plass. Han presiserer at med overvåkning menes det ikke å lese hva de ansatte skriver i e-post, men å overvåke trafikkmønsteret på maskinen for å se etter normal aktivitet eller om det er noe som skiller seg ut. Bergsjø og Windvik (2020) viser til at det er flere utfordringer knyttet til sikkerhetsovervåking. Når en alarm går er det kun en indikasjon på at det er et datainnbrudd.

Det sier ikke noe om hvilken type innbrudd det er og i noen tilfeller er informasjonen som er knyttet til alarmen mangelfull eller ukorrekt. En årsak til at alarmen går av kan være at det er driftsproblemer eller en eller annen form for konfigurasjonsfeil. Ved alarm må en klassifisere den og agere på den. CFO forteller om at han selv har blitt kontaktet av IT-leverandør en gang da de mente det var noe trafikk på hans datamaskin som virket unormalt. Da er det en alarm som har utløst dette hos IT-leverandør som gjør at de sjekker det opp. I dette tilfelle, som CFO sa, så fant de ingenting galt.

## 5.4 Hvordan arbeides det med bevissthet av digital sikkerhet fra ledelsens side?

Bergsjø & Windvik (2020) tar opp at forståelsen til de ansatte er en viktig brikke i hvor vidt de ansatte kan vurdere de truslene de møter. De må kjenne til hvilke trusler som er der, hvor ofte disse truslene kan oppstå og hvordan kjenne de igjen. Samtlige av deltakerne viser til opplæring av de ansatte, både med introduksjon til nyansatte når de starter i selskapet, men også via e-læring og simulering av falske e-poster. Det er IT-ansvarlig som sender ut simuleringene og blant annet HR og Site Manager viser til at han sender de ut med jevne mellomrom. COO tar opp sin bekymring over at mange lar seg lure av slike e-poster.

> *«[…] det er fryktelig mange som lar seg lure av falske e-poster eller det som er[…] trykke på lenker og det som hører til.» (Deltaker 4)*

Det at de ansatte får trene på å kjenne igjen farlig e-post er med på å øke den ansattes evne til å vurdere de e-poster som kommer inn, se om vedlegg, lenker og avsendere ser troverdig ut eller ikke. Bergsjø og Windvik (2020) tar opp nettopp dette. For at de ansatte skal kunne behandle en risiko på rett måte, må de vite hva de ser etter og ha kunnskap relatert til risikoen, mer enn at de vet at slike e-poster kan komme.  Selv om en ser av kommentaren til COO over, viser han også til at han ser at resultatet av de grepene som er gjort med blant annet opplæring og simulering har gjort at hva folk åpner og hva de deler har gått drastisk ned. En kan tolke de dit hen at kompetansen til de ansatte på hva som er farlig og ikke i en e-post er blitt styrket etter denne opplæringen startet og at det gjenspeiles på resultatene.

IT-ansvarlig viser til at distribusjon av informasjon relatert til digital sikkerhet hovedsakelig skjer via selskapets intranett, Microsoft Teams. Han legger til at noe av informasjonen også sendes ut på e-post. Ved å distribuere informasjon via slike kanaler ser en på Schiefloe (2021) sin lineære kommunikasjonsmodell, der budskapet som sendes fra IT-ansvarlig blir delt enten på Microsoft Teams eller e-post. IT-ansvarlig vil da ikke selv se mottakerne og vil heller ikke

vite om det når frem eller hvordan det når frem til de ansatte, noe han også selv poengterer med at det ikke er noen garanti for at det som blir sendt ut, eller publisert, blir lest av alle. Det er mye «støy», som illustrert i Figur 7, som kan gjøre at budskapet ikke når frem til de ansatte. Han viser til episoder det han har sendt ut informasjon, hvor det kort tid etter kommer telefon med spørsmål om akkurat det som kom frem av informasjonen han sendte ut. Slik en tolker IT-ansvarlig skyldes ikke telefonsamtalen at innholdet ikke var forstått, men at de ikke har sett at informasjonen var kommet ut og at det derfor er «enklere» å bare ringe. Han tar videre opp at han har laget et dokument, der det står hva de ansatte skal gjøre i ulike situasjoner, men at dokumentet ikke er distribuert. Bakgrunnen for at det ikke er distribuert ut til de ansatte er fordi det er et dokument på fem sider som han mener ikke vil bli lest, og at han derfor først må komme på en annen måte å presentere det på. COO er en annen som viser til at IT-ansvarlig prøver å distribuere ut informasjon og retningslinjer, som også viser til utfordringen med å få de ansatte til å ta til seg informasjonen.

Et annet sted hvor digital sikkerhet blir kommunisert er i møter, og det vises til blant annet morgenmøter, avdelingsmøter og allmannamøter. De som trekker frem allmannamøtene er blant annet CFO og VP Project, som viser til at digital sikkerhet er tema på møtene og at det vises til simuleringene som blir gjort i selskapet. Hvor ofte disse møtene holdes, og hvem det er som presenterer informasjonen kommer ikke frem i intervjuene. Det en kan trekke frem fra allmannamøter er at den kan sees på som en enveiskommunikasjon, der ledelsen presenterer informasjon til de ansatte. Av Figur 7 (Shiefloe, 2021) er da ledelsen «sender» og de ansatte «mottaker». Det viser at selv om ledelsen viser til at det på allmannamøter bli informert om digital sikkerhet, er det flere momenter som gjør at det ikke er sikker at budskapet kommer frem til de ansatte slik som tenkt. Momenter som anses å påvirke kommunikasjonen er 1) hvordan ledelsen velger å formulere budskapet 2) støy som forstyrrer den sender ut 3) støy som forstyrrer for den som skal tolke budskapet 4) tolkningen til den som mottar budskapet. I tillegg er det ingen garanti for at alle de ansatte tolker budskapet likt, uavhengig av støy som påvirker underveis i kommunikasjonen. De ansatte setter informasjonen de mottar inn i mentale modeller, en slags ramme. Disse rammene fremstår som oftest som ubevisste og intuitive, noe som vil si at det lite sannsynlig at alle de ansatte vil tolke budskapet til ledelsen likt. Noe av det som påvirker rammene de ansatte har er kunnskap og erfaringer (Schiefloe, 2021).

Avdelingsmøtene som vises til i intervjuene, er de hvor IT-ansvarlig hadde fysisk oppmøte i avdelingsmøtene for å få frem viktigheten av å ha god kommunikasjon rundt digital sikkerhet. I intervjuene sier både IT-ansvarlig, VP Project og CFO at de opplever at det har vært aktiv

deltagelse fra de ansatte i avdelingsmøtene hvor IT-ansvarlig har vært og presentert. Et interessant perspektiv er hvordan møtene starter med at IT-ansvarlig kommuniserer med en lineær overføringskanal til de ansatte som deltar i møtet, som lytter og observerer, men at det blir en slags overgang til interaktiv overføringskanal når det kommer frem at det som ble presentert i møtene gikk over i gode diskusjoner mellom de ansatte og IT-ansvarlig. Den interaktive kommunikasjonsmodellen som Schiefloe (2021) viser til, viser kommunikasjonen som hovedsakelig mellom to personer og at en med interaktiv overføring av budskapet gir rom for at begge parter kan kommunisere. Det gjør at det er rom for å stille spørsmål om noe er uklart og IT-ansvarlig kan omformulere seg dersom han opplever at det budskapet han ønsker å dele ikke kommer frem slik som ønsket, en ser ut fra dette at deltakerne samarbeider om å skape en mening som Askehave (2006) tar opp.

Site Manager viser til hvordan bevisstgjøring er med på å sette digital sikkerhet på dagsorden, da han viser til at i tiden etter intervjuene så er det trolig at digital sikkerhet vil bli tatt opp på morgenmøtene. Han viser også derimot til at han tror det kanskje vil virke noen dager og at en om en to ukers tid gjerne vil ha glemme å ta det opp, dersom en ikke blir gjort oppmerksom på viktigheten av det. Det kommer ikke frem av intervjuet hvor store grupper det er på morgenmøtene, men antas at det i disse møtene vil være rom for diskusjon og at en kan se disse møtene under interaktiv kommunikasjonsmodell (Shiefloe, 2021).

En måte CFO bidrar i arbeidet med bevisstgjøring av digital sikkerhet er å stille det som han kaller «dumme spørsmål» til IT-ansvarlig, at han på den måten kan tenke litt utenfor boksen og på denne måten gi innspill til IT-ansvarlig ved å legge til et perspektiv fra en med annen kompetanse.

> *«Jeg har jo sagt til IT-ansvarlig også at det er ikke min kompetanse, men jeg kan bidra med å stille litt dumme spørsmål og tenke gjerne litt annerledes enn en IT-person, så det er mitt bidrag […].» (Deltaker 2)*

Interesser former ens holdninger, samtidig som den er med på å utvikle ferdigheter og kunnskap, dette gjør at en også får en økt bevissthet og nysgjerrighet rundt interessene sine (Bergsjø & Windvik, 2020). COO tok opp den ansatte sin interesse og viser til en gruppe ansatte som har skilt seg ut når det kommer til bevissthet rundt mulige sikkerhetsbrudd og trusler. Han viser til at dette er ansatte som har interesse for data og gaming. Bergsjø og Windvik (2020) sier det er fristende å slå fast at de med interesse innenfor teknologi og IT har en fordel fremfor de som ikke har det, sett i lys av at en lever i et samfunn med stadig mer digitalisering. De viser

også til at det ikke alltid er positivt at en har interesse innenfor fagområdet. Det kan også føre til at de ansatte med mye kompetanse kan ha en tendens til å overvurdere sine egne evner når det kommer til å håndtere trusler og at de på den måten kan ende opp med å ta større risiko.

Flere av deltakerne var inne på at de har sett hva hacking har gjort med andre store selskap og at dette har vært med på å øke deres bevissthet på hvor utsatt en er som selskap og hvor store konsekvenser det kan få dersom noe skulle skje dem. Bergsjø og Windvik (2020) viser til at risikooppfattelse ikke bare er å kalkulere fakta, men at det i tillegg er subjektive faktorer som virker inn. Som eksempel på dette viser de til hvordan den enkelte kan sine opplevelser og væremåter kan være med på å styrke dette. Eksempler de viser til er om ansatte har vært ute for noe lignende situasjon tidligere så vil det gjerne gjøre at en er mer forsiktig i dag. Nå viser ikke deltakerne til at de selv har opplevd dette, men viser til selskap, og personer de kjenner i disse selskapene, og hvordan det har påvirket deres væremåte. De sier at deres syn på selskapene som har vært ute for noe sånt ikke er blitt påvirket og at de tror det er en god ting at selskap går ut med informasjon om dette, nettopp slik at det kan øke bevisstheten til andre og på den måten unngå at det skal skje med flere.

I en undersøkelse Norstat gjorde for fagforeningsorganisasjonen NITO i 2022 kommer det frem at det er de yngre som er dårligst på IKT-sikkerhet. Den viser først og fremst at omtrent halvparten av Norges befolkning ikke følger rådene til ekspertene, men at i aldersgruppen 15-29år var det hele 62% som ifølge undersøkelsen ikke følger rådene til ekspertene (digi, 2023). I intervjuene viser både IT-ansvarlig og COO til at de mener det er den eldre generasjonen som er den gruppen som ikke tar til seg de råd som gis. Bergsjø og Windvik (2020) sier at alder er en faktor som spiller inn, men det kom ikke frem hvordan de så på alderen. COO trakk frem at den eldre generasjonen gjerne er mer naiv enn den yngre og HR viser til at naiviteten til de ansatte er en risiko. Det å arbeide med bevisstgjøring er noe en gjør, men IT-ansvarlig viste også til at det er litt vanskeligere å nå inn til de som er litt reserverte, gjerne ikke i den yngre generasjonen og som generelt er skeptisk til endringer.

## 5.5 Hvordan oppleves sikkerhetskulturen av ledelsen?

Kultur er noe som vokser frem i en organisasjon, men den kan til en viss grad påvirkes av bevisste lederatferder. Bergsjø og Windvik (2020) viser til at en må ha i bakhode at det er mennesket som skaper kultur og det er også de som skal påvirkes av kulturen. Med bakgrunn i dette viser de til at sikkerheten selskapet legger opp til må være mulig å forstå for de ansatte. Det kommer tydelig frem at IT-ansvarlig vet at kulturen kommer fra de ansatte og for å fortsette

arbeidet med sikkerhetskulturen er det de ansatte han må arbeide sammen med. På denne måten kan han være med påvirke sikkerhetskulturen gjennom dem.

> *«Jeg kan jo ikke fortelle at her skal vi ha en sikkerhetskultur – YES. Det er opp til alle ansatte.» (Deltaker 5)*

Som det kom frem under kommunikasjon av digital sikkerhet, har IT-ansvarlig deltatt på flere av selskapets avdelingsmøter. I disse møtene presenterer han viktigheten rundt digital sikkerhet og hvordan den ansatte sin rolle spiller inn. Om en stopper opp her og ser på dette med roller, så er rolle og rolleforhold i kjernen av teknologisk endring og påvirker derfor organisasjonens struktur og kultur (Bergsjø & Windvik, 2020). Det er ikke bare nødvendig at de ansatte ser hvilken brikke de har i digitalt sikkerhetsbilde, det er også viktig at de vet hvordan de er med på å påvirke sikkerhetskulturen i selskapet. I avdelingsmøtene det vises til, har IT-ansvarlig deltatt fysisk. Han begrunner at dette er noe han gjør for å få opp bevisstheten til de ansatte og at han gjør dette på flere måter. Det første IT-ansvarlig trekker frem er det å ha øyekontakt med de ansatte som i møte, på hvordan de hører og observerer han når han formidler budskapet. I intervjuet bruker han metaforen *«gå litt bananas»* når han viser til hvordan han ønsker å fange oppmerksomheten til de ansatte. Han forteller at han håper det vil være med på å gjøre at de husker det som ble sagt litt lenger enn om han ikke hadde gjort det. Han presiserer at om det er innholdet som gjør at de husker det lenger, eller det at han oppførte seg på en måte som gjorde inntrykk, ikke er så relevant, så lenge budskapet blir værende i minnet hos de ansatte. Han sier også at han så langt opplever at denne måten å presentere informasjon på fungerer, men legger også til at han ikke kjenner til hvor lenge det vil vare. Han beskriver ikke måten han presenterer på mer enn med metaforen *«gå litt bananas»* så om dette er en metafor han kun bruker i intervjuet eller også trekker frem i avdelingsmøtene er uvisst. Det å bruke metaforer styrer hva, hvilke og hvordan informasjon som blir presenter blir oppfattet (Shiefloe, 2021). Å bruke metaforer vil altså være med på å påvirke hvordan de ansatte oppfatter budskapet, men utfordringen er at en må passe på at ikke er andre viktige elementer faller bort mens man gjør det.

Eriksen & Sajjad (2015) viser til at for å forstå hvorfor de ansatte gjør som de gjør, så er det ikke nok å «kjenne til en kultur», da kultur er som en matrise for handlinger. Formålet med hvorfor IT-ansvarlig deltok i de avdelingsmøtene var for å øke bevisstheten deres til hvordan de selv kan bidra til å skape en god sikkerhetskultur. Schiefloe (2021) viser til at infrastrukturen på arbeidsplassen er med på å skape møteplasser for uformell kontakt. En ser på infrastrukturen

som en faktor som påvirker relasjonsbygging innad i det kollegiale. IT-ansvarlig sier han i møtene oppfordrer de ansatte til å snakke sammen. Dersom en ansatt har mottatt en mistenkelig e-post så er det ønskelig at vedkommende skal snakke med noen om det, skape en diskusjon rundt det. Det å snakke sammen, skape diskusjoner er ikke bare med på å øke bevisstheten, det er også med på å dele kunnskap og å utvikle sikkerhetskulturen til selskapet. Det å formidle dette budskapet ut til de ansatte er et stort fokusområde for IT-ansvarlig. COO tar også frem at han arbeider med bevisstgjøring, blant annet i eksempelet der han viser til at han reagerer på at de ansatte går fra kontoret sitt uten å låse datamaskinen. Han viser til at i de tilfellene kommenterer han det gjerne til den det gjelder, om det er så lurt å gå fra datamaskinen ulåst.

Et tema som er relevant når en ser på sikkerhetskulturen til selskapet, er holdninger, både hos de ansatte og hos lederne. En episode IT-ansvarlig snakker om er hvordan ansatte ringer til han i stedet for å lese informasjonen som er sendt ut. I denne situasjonen viste IT-ansvarlig til at det ikke var innholdet som gjorde at den ansatte ringte, men det at den ansatte ikke hadde fått med seg informasjonen som var sendt ut og syntes det var lettere å ringe IT-ansvarlig enn å undersøke selv. IT-ansvarlig sier ikke om dette er noe typisk atferdsmønster fra de ansatte generelt, men det sier noe om hvordan holdningen til noen av de ansatte er. De ulike elementene innenfor kultur påvirker hverandre som en ser i Figur 10, og slike holdninger og atferdsmønstre som IT-ansvarlig vil påvirke hans holdninger og atferdsmønstre også. Det at IT-ansvarlig ikke har distribuert dokumentet om hvordan de ansatte skal håndtere ulike situasjoner innenfor digital sikkerhet kan være påvirket av det holdningene han har møtt hos ansatte tidligere, og at det er grunnen til at han ikke vil distribuere det som et fem siders dokument. Han poengterte selv at det ikke ville bli lest dersom han sendte det slik som det er nå, det kan tyder på at han tolket de ansattes holdninger og atferdsmønster fra tidligere.

# 6 AVSLUTNING

## 6.1 Oppsummering

I denne masteroppgaven var formålet å se nærmere på hvordan det jobbes fra ledelsens side når det kommer til prosedyrer og bevisstgjøring av digital sikkerhet. Til dette har en sett på relevant teori som omhandler digital sikkerhet innenfor ledelse og organisasjonsanalyse. Funnene er hentet fra kvalitativ forskning, gjennom dybdeintervju med seks ledere i et selskap fra den maritime næringen.

Det kommer frem at det er noe usikkerhet blant fem av lederne når det kommet til hvilke prosedyrer selskapet har for digital sikkerhet. Det kommer frem at de tror det er prosedyrer på digital sikkerhet, men hvor de er, hva de inneholder og hvem de er for, er noe usikkert. Det blir vist til at selskapet har anbefalinger og retningslinjer, noe som bekreftes av IT-ansvarlig samtidig som han viser til at det ikke er noen definerte prosedyrer på digitalsikkerhet. Dette viser at det ikke er prosedyrer som danner rammene for digital sikkerhet i selskapet. Noen av programvarene selskapet har er med på å styre hvordan de ansatte jobber og på den måten sees på som en form for prosedyre.

Det kommer frem at som selskap har de fokus på digital sikkerhet, at det er godt etablert hos ledelsen, men nedover i organisasjonen kommer det frem at arbeidsoppgaver som oppleves å bringe selskapet fremover prioriteres fremfor arbeid med digital sikkerhet. Teorien viser til viktigheten av at de som jobber nært de ansatte tar del i arbeidet med digital sikkerhet, da det er de som kan observere de ansatte og fange opp eventuelle risikoer.

I arbeidet med å bevisstgjøre de ansatte om hvilken rolle de har i arbeidet med digital sikkerhet, er det flere metoder som brukes fra ledelsen. Det vises til at informasjon om digital sikkerhet deles via ulike kanaler, både gjennom møter, e-poster og Microsoft Teams. Ut fra intervjuene ser en at det er møtene der IT-ansvarlig deltar fysisk som virker til å gi best virkning for å spisse de ansattes kompetanse på digital sikkerhet. Av drøftingen ser en at et møte normalt starter som en lineær kommunikasjon, mens når en i avdelingsmøtene klarte å skape dialog med de ansatte skapte de sammen forståelse for det som ble presentert, når en gikk fra den lineære kommunikasjonen til den interaktive kommunikasjonen. I møtene det vises til oppfordres de ansatte til å snakke om digital sikkerhet sammen, gjerne ved kaffemaskinen, dette for å bygge

oppunder sikkerhetskulturen i selskapet. Det at sikkerhetskulturen som vokser frem i selskapet er styrt av de ansatte er noe ledelsen har forståelse for og noe de arbeider med å bevisstgjøre for de ansatte.

Det vises også til at selskapet har opplæring for de ansatte, i form av simuleringer og kurs. Teorien viser til at for å kunne håndtere en risiko på en god måte er en avhengig av at de ansatte har den kunnskapen som trengs for å tolke de risikoene de møter i hverdagen. En form for trening som selskapet gjør for de ansatte, er å sende ut simuleringer av mistenkelig e-post. Etter flere runder med slik simulering, gikk suksessraten for rapportering av mistenkelig epost opp. Det vises også til at det fremdeles er en vei å gå. En er aldri sterkere enn det svakeste ledd, og som selskap må en arbeide med å kontinuerlig øke bevisstheten til de ansatte.

## 6.2 Tanker om masteroppgaven og videre forskning

Bergsjø og Windvik (2020) viser til at interessen for digital sikkerhet er med på å påvirke hvem en omgås med, hva en legger merke til og hvordan en vurderer en risiko. De sier at interessen kan skyldes flere ting, det blir tatt opp at gamere gjerne har en økt interesse for digital sikkerhet. I denne husstanden bor det to stykker og begge med stor interesse for teknologi. Samboeren kan en gjerne referere til som gameren, opptatt av ny teknologi, spesielt innenfor kunstig intelligens. Han har mye kunnskap og er nok litt den «det skjer ikke meg»-typen. Så er det undertegnede, som har interesse for tematikken digital sikkerhet, som følger med i media på hvordan digital sikkerhet påvirker samfunnet, både lokalt, i Norge og i verden generelt. Kan nok også beskrives som den forsiktige typen, som er naturlig skeptisk og er mer en «det skjer nok med meg»-type.

I denne masteroppgaven har en fått sett på hvordan det jobbes med digital sikkerhet fra et ledelsesperspektiv. I retrospekt ser en at interessen for å se på hvordan de ansatte opplever dette er økende, og er derfor et tema en ville gått videre med i en videre forskning. Noen spørsmål som har dukket opp underveis er:

- Hva legger de ansatte i sikkerhetskultur?
- Hvordan opplever de ansatte at det er å jobbe med digital sikkerhet?

Ideelt sett, og som i utgangspunktet planlagt, skulle en helst ha gjort både en kvalitativ og en kvantitativ analyse for å få frem både hva som jobbes med fra ledelsens side og fra de ansattes side. Da en jobbet med utforming av intervjuguide det et håp om å få til å gjøre nettopp det, ha

en liten spørreundersøkelse i ettertid med fokus på de ansatte i selskapet. Av ulike grunner ble ikke det mulig å gjennomføre denne kvantitative undersøkelsen.

Noe annet en ser i etterkant, er når en jobber med intervjuene og kommer på et eller flere oppfølgingsspørsmål en gjerne skulle ha stilt hadde. Det er en liten trøst å vite at dette er noe erfarne forskere også opplever.

# 7 REFERANSER


Andersen, F. S. (2001). *Den meningsskapte organisasjon.* Oslo: Universitetsforlaget AS.

Askehave, I. (2006). Communication: Transmitting messages or fusing horizons. I B. Norlyk, & I. Askhave (Red.), *Meanings and Meetings: - intercultural business communication* (ss. 33-60). Århus, Danmark: Academica.

Askehave, I. (2006). Communication: Transmitting messages or fusing horizons. I B. Norlyk, & I. Askhave (Red.), *Meanings and Meetings: - intercultural business communication* (ss. 33-60). Århus, Danmark: Academica.

Barley, S. R. (2020). *Work and Technological Change.* New York: Oxford University Press.

Bergsjø, H., & Windvik, R. (2018). *Datasikkerhet for ledere.* Oslo: Universitetsforlaget AS.

Bergsjø, H., & Windvik, R. (2020). *Digital sikkerhet - en innføring.* (L. Øverlier, Red.) Oslo: Universitetsforlaget AS.

Bjørnsen, J. T. (2012). *Slik får du IT-styring og -kontroll.* Oslo: Universitetsforlaget AS.

Bowker, G. C., & Star, S. L. (1999). *Sorting things out : Classification and its consequences.* Cambridge: The MIT Press.

Dahl, Ø., & Baker, C. N. (2020, okt 24). *NDLA*. Hentet fra Kommunikasjonsmodeller: https://ndla.no/nb/subject:1:1f1865fc-e4cc-48a0-918f-3530485ec424/topic:1:ae0e6304-d30e-4d3f-8e94-306d1a884e10/topic:1:b4a83480-e593-4b51-ae4c-9dee708c1616/resource:4a8c58f3-9bd6-4c19-92c6-c7f970cc7c07

*digi*. (2023, februar 3). Hentet fra Unge er dårligst på IKT-sikkerhet: https://www.digi.no/artikler/nito-unge-er-darligst-pa-ikt-sikkerhet/525766

Eriksen, T. H., & Sajjad, T. A. (2015). *Kulturforskjeller i praksis.* Oslo: Gyldendal.

Helseinnovasjonssenteret. (2023, des 3). *Helseinnovasjonssenteret*. Hentet fra Samhandling - Bare sammen kan vi utvikle fremtidens helsetjeneste: https://www.helseinnovasjonssenteret.no/satsingsomrader/samhandling

Holliday, A. (2009). Interrogating the concept of stereotypes in intervultural communication. I D. Oakley, & S. Hunston, *Introducing Applied Linguistics: concept and skills* (ss. 134-141). London: Routledge. Hentet desember 08, 2021 fra https://adrianholliday.com/wp-content/uploads/2020/01/stereotypes-2009.pdf

Hårberg, T. M. (2020, mar 4). *NDLA*. Hentet fra Hva betyr kommunikasjon?: https://ndla.no/nb/subject:1:777ae87e-ca79-4866-920a-115cfeb7bbe1/topic:2:183732/topic:2:184512/resource:1:4052

Jøsang, A. (2021). *Informasjonssikkerhet.* Oslo: Universitetforlaget AS.

Kvale, S., & Brinkmann, S. (2015). *Det kvalitative forskningsintervju* (3. utg.). Oslo: Gyldendal Norsk Forlag AS.

Larsen, A. K. (2017). *En enklere metode* (2. utg.). Bergen: Fagbokforlaget.

Nasjonal Sikkerhetsmyndighet. (2020, aug 31). *NSM*. Hentet fra Grunnprinsipper for sikkerhetstyring: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/introduksjon/

Nasjonal sikkerhetsmyndighet. (2023). *Risiko 2023.* 13: feb. Hentet fra https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2023

NITO. (2022, oktober 18). *NITO*. Hentet fra Unge er dårligst på IKT-sikkerhet: https://www.nito.no/aktuelt/2022/10/nasjonal-sikkerhetsmaned/

Orlikowski, W. J. (2009, aug). The sociomateriality of organisational life: considering technology in management research. *Cambridge Journal of Economics*, ss. 125-141.

Schiefloe, P. M. (2017). Pentagonanalyse: En helhetlig modell for sikkerhet i organisasjoner. I S. Antonsen, F. Heldal, & S. A. Kvalheim (Red.), *Sikkerhet og ledelse* (ss. 281-301). Gyldendal Akademisk.

Schiefloe, P. M. (2021). *Organisasjonsanalyse* (1, 2021. utg.). Bergen: Vigmostad & Bjørke AS.

Shiefloe, P. M. (2021). *Organisasjonsanalyse* (1, 2021. utg.). Bergen: Vigmostad & Bjørke AS.

Standard Norge. (2018, feb). International Standard. *Information technology - Security Tevchniques - Information security management systems - Overview and vocabulary*. (ISO/IEC 27000). Hentet fra https://lese.standard.no/product/2475033/nb

Store norske leksikon. (2023, oktober 21). *Store norske leksikon*. Hentet fra Sikkerhet: https://snl.no/sikkerhet

# 8 VEDLEGG

## 8.1 Vedlegg 1

## INTERVJUGUIDE – SEMISTRUKTURERT

Digital sikkerhetskultur - DET FORMELLE VS. DET UFORMELLE

**TEMATISERING:** Digital Sikkerhet, Organisasjons analyse – pentagonmodellen, Kultur – Organisasjonskultur

**FORMÅLET MED UNDERSØKELSEN:** Undersøkelsen blir gjort som en del av min masteroppgave innen «Krevende maritim ledelse» hvor jeg har ønsker å ta utgangspunkt i et selskap, se på ledelse og ansatte om hvordan de jobber med prosedyrer, praksiser og holdninger når det kommer til digital sikkerhet i selskapet.

**UTVALG:** Oppgaven vil ta utgangspunkt i et selskap innen den maritime næringen. I dette selskapet er det for intervjuet foretatt et strategisk utvalg: 5 ledere av ulik rang + en spesialist innenfor fagfeltet oppgaven berører.

**ETISKE UTFORDRINGER:** Personopplysninger som kontaktinformasjon er ikke nødvendig. Det vil bli spurt om bakgrunn og rolle, men kjønn og alder kan bli holdt utenfor i intervjuet. I intervjuet vil alder og kjønn bli aktuelt, men ikke på et nivå som kan identifiseres. Etter transkribering vil opptaket av intervjuet slettes.

**GUIDE:**

1. Kan du si litt om hvem du er, og hva du jobber med?
2. Hva tenker du når jeg sier digital sikkerhet?
   2.1. Hva tenker du er de største truslene?
3. Er digital sikkerhet et tema som er aktuelt i ditt arbeid?
   3.1. Hvordan?
4. Kan du si litt om hvordan dere i selskapet jobber med det?
   4.1. Utforming av prosedyrer
   4.2. Hvordan jobber dere med
      4.2.1. Utforming
      4.2.2. Formidling av
      4.2.3. Trening på?
      4.2.4. Intensiv/sanksjonering
      4.2.5. Virkningen av?
   4.3. Valg av teknologi/implementering av teknologiske barrierer
      4.3.1. Valg av teknologi
      4.3.2. Implementering av prosedyrer
      4.3.3. Brukervennlighet/informasjon
   4.4. Kommunikasjon (forum, strategi og medvirkning)
5. Hvordan opplever du det er å jobbe med å øke bevisstheten rundt digital sikkerhet?
6. Avslutningsvis: er det noe mer du ønsker å tilføye som vi enten ikke har vært innom eller du ønsker å utdype mer?

## 8.2 Vedlegg 2

**Vil du delta i forskingsprosjektet «Digital sikkerhet – det formelle vs. det uformelle?» Ref.nr. 496671**

Dette er eit spørsmål til deg om å delta i eit forskingsprosjekt der føremålet er å sjå på korleis leiarar og ansatte jobbar med prosedyrar og praksisar, samt kva haldningar ein har til digital tryggleik i selskapet. Forskingsprosjektet er ein del av mi masteroppgåve innan Leiing i krevjande maritime operasjonar. I dette skrivet gjev eg deg informasjon om måla for prosjektet og om kva deltaking vil innebere for deg.

**Føremål**

Prosjektet eg ber deg om å delta på er eit forskningsprosjekt for mi masteroppgave som er planlagt ferdigstilt i andre kvartal 2023. Formålet med masteroppgava er få forståelse for korleis ledelse og ansatte jobbar med prosedyrar, praksisar, samt holdninger når det kjem til digital tryggleik.

**Kven er ansvarleg for forskingsprosjektet?**

Ingvild Kvamme (student) er ansvarleg for prosjektet.

Marte Fanneløb Giskeødegård (rettleiar)

**Kvifor får du spørsmål om å delta?**

Eg spør deg om å delta i prosjektet i kraft av di rolle i selskapet, samt basert på lokasjon du jobbar frå. Prosjektet har som formål å få betre kunnskap om korleis det vert jobba med digital tryggleik i selskapet.

**Kva inneber det for deg å delta?**

Dersom du vel å delta i undersøkinga, et metoden som blir brukt intervju. Det blir satt av 60 minutt til intervjuet, men lengda vil variere. Den er derfor satt som eit referansepunkt.

Grunna ulike lokasjonar er teams ein moglegheit framfør fysisk møte. Dersom intervju blir tatt over teams vil teams samtalen bli tatt opp. Dersom vi vel å ta intervjuet på teams er det ynskjeleg at kamera er på, dette for å ha det så likt som eit fysisk intervju.

**Det er frivillig å delta**

Det er frivillig å delta i prosjektet. Dersom du vel å delta, kan du når som helst trekkje samtykket tilbake utan å gje nokon grunn. Alle personopplysingane dine vil då bli sletta. Det vil ikkje føre til nokon negative konsekvensar for deg dersom du ikkje vil delta eller seinare vel å trekkje deg.

**Ditt personvern – korleis vi oppbevarer og bruker opplysingane dine**

Opplysningane om deg vil berre bli brukt til det føremålet som kjem fram av dette skrivet. Opplysningar vil bli behandla konfidensielt og i samsvar med personvernregelverket.

Intervjuet vil bli tatt opp (lyd/video), denne fila vil bli lagra med et filnamn som ikkje skal kunne identifisere deg. I etterkant blir intervjuet transkribert og lyd/video-fila vil bli sletta. Transkriberinga vil også vere lagra med eit filnamn som ikkje kan knytast til deg.

For prosjektet er det ingen behov for kontaktinformasjon. Selskapet er også anonymt, så i transkriberinga vil ein nytte «selskapet» framfor namnet til selskapet dersom det skulle dukke

opp.  Til informasjon vil masteroppgåva også vere konfidensiell. Transkriberinga vil berre vere tilgjengeleg for masterstudenten og hennar rettleiar.

**Kva skjer med opplysingane dine når vi avsluttar forskingsprosjektet?**

Opplysingane blir anonymiserte når prosjektet er avslutta. Som nemnt tidlegare i skrivet så vil lyd/video-fil bli sletta når transkriberinga er gjort. Transkriberinga blir lagra med eit filnamn som ikkje kan knytast til deltakar eller selskap. Når oppgåva er ferdig og sensur er levert vil transkriberingane også bli sletta. Det kan førekomma grunnlag for å utsette innlevering av masteroppgåva. Dersom dette skulle skje vil avsluttinga av forskingsprosjektet bli noko forskyvd. Dette til informasjon.

**Kva gjev oss rett til å behandle personopplysingar om deg?**

Vi behandlar opplysingar om deg basert på samtykket ditt.

På oppdrag frå NTNU har personverntenestane ved Sikt – Kunnskapssektorens tenesteleverandør vurdert at behandlinga av personopplysingar i dette prosjektet er i samsvar med personvernregelverket.

**Dine rettar**

Så lenge du kan identifiserast i datamaterialet, har du rett til:

- innsyn i kva opplysingar vi behandlar om deg, og å få utlevert ein kopi av opplysingane,
- å få retta opplysingar om deg som er feil eller misvisande,
- å få sletta personopplysingar om deg,
- å sende klage til Datatilsynet om behandlinga av personopplysingane dine.

Dersom du har spørsmål til studien, eller om du ønskjer å vite meir eller utøve rettane dine, ta kontakt med:

- Masterstudent: Ingvild Kvamme – ingvildkvamme@gmail.com – mob.: 906 45 476
- Rettleiar ved NTNU: Marte Fanneløb Giskeødegård - marte.giskeodegard@ntnu.no

Dersom du har spørsmål knytt til vurderinga av prosjektet frå Sikts personverntenester kan du ta kontakt via:

- e-post (personverntjenester@sikt.no) eller telefon: 73 98 40 40.

Venleg helsing

| | |
|---|---|
| Marte Fanneløb Giskeødegård | Ingvild Kvamme |
| (Forskar/rettleiar) | Mastergradstudent |

---

**Samtykkeerklæring**

Eg har motteke og forstått informasjon om prosjektet «Digital sikkerhet – det formelle vs. det uformelle» og har fått høve til å stille spørsmål. Eg samtykker til:

- å delta i intervju

Eg samtykker til at opplysingane mine kan behandlast fram til prosjektet er avslutta.

---

(Signert av prosjektdeltakar, dato)

## 8.3 Vedlegg 3

# Vurdering av behandling av personopplysninger

**Referansenummer**
496671

**Vurderingstype**
Automatisk

**Dato**
21.02.2023

**Tittel**
Digital sikkerhet - det formelle vs det uformelle

**Behandlingsansvarlig institusjon**
Norges teknisk-naturvitenskapelige universitet / Fakultet for ingeniørvitenskap / Institutt for havromsoperasjoner og byggteknikk

**Prosjektansvarlig**
Marte Fanneløb Giskeødegård

**Student**
Ingvild Kvamme

**Prosjektperiode**
01.01.2023 - 15.06.2023

**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 15.09.2023.

Meldeskjema

**Grunnlag for automatisk vurdering**

Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
    - Rasemessig eller etnisk opprinnelse
    - Politisk, religiøs eller filosofisk overbevisning
    - Fagforeningsmedlemskap
    - Genetiske data
    - Biometriske data for å entydig identifisere et individ
    - Helseopplysninger
    - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

**Informasjon til de registrerte (utvalgene) om behandlingen må inneholde**

- Den behandlingsansvarliges identitet og kontaktopplysninger
- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)
- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)
- Hvor lenge personopplysningene vil bli behandlet
- Retten til å trekke samtykket tilbake og øvrige rettigheter

Vi anbefaler å bruke vår mal til informasjonsskriv.

**Informasjonssikkerhet**

Du må behandle personopplysningene i tråd med retningslinjene for informasjonssikkerhet og lagringsguider ved behandlingsansvarlig institusjon. Institusjonen er ansvarlig for at vilkårene for personvernforordningen artikkel 5.1. d) riktighet, 5. 1. f) integritet og konfidensialitet, og 32 sikkerhet er oppfylt.

## 8.4 Vedlegg 4

# Vurdering av behandling av personopplysninger

**Referansenummer**
496671

**Vurderingstype**
Automatisk

**Dato**
16.09.2023

**Tittel**
Digital sikkerhet - det formelle vs det uformelle

**Behandlingsansvarlig institusjon**
Norges teknisk-naturvitenskapelige universitet / Fakultet for ingeniørvitenskap / Institutt for havromsoperasjoner og byggteknikk

**Prosjektansvarlig**
Marte Fanneløb Giskeødegård

**Student**
Ingvild Kvamme

**Prosjektperiode**
01.01.2023 - 22.12.2023

**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 15.03.2024.

Meldeskjema

**Grunnlag for automatisk vurdering**

Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
    - Rasemessig eller etnisk opprinnelse
    - Politisk, religiøs eller filosofisk overbevisning
    - Fagforeningsmedlemskap
    - Genetiske data
    - Biometriske data for å entydig identifisere et individ
    - Helseopplysninger
    - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

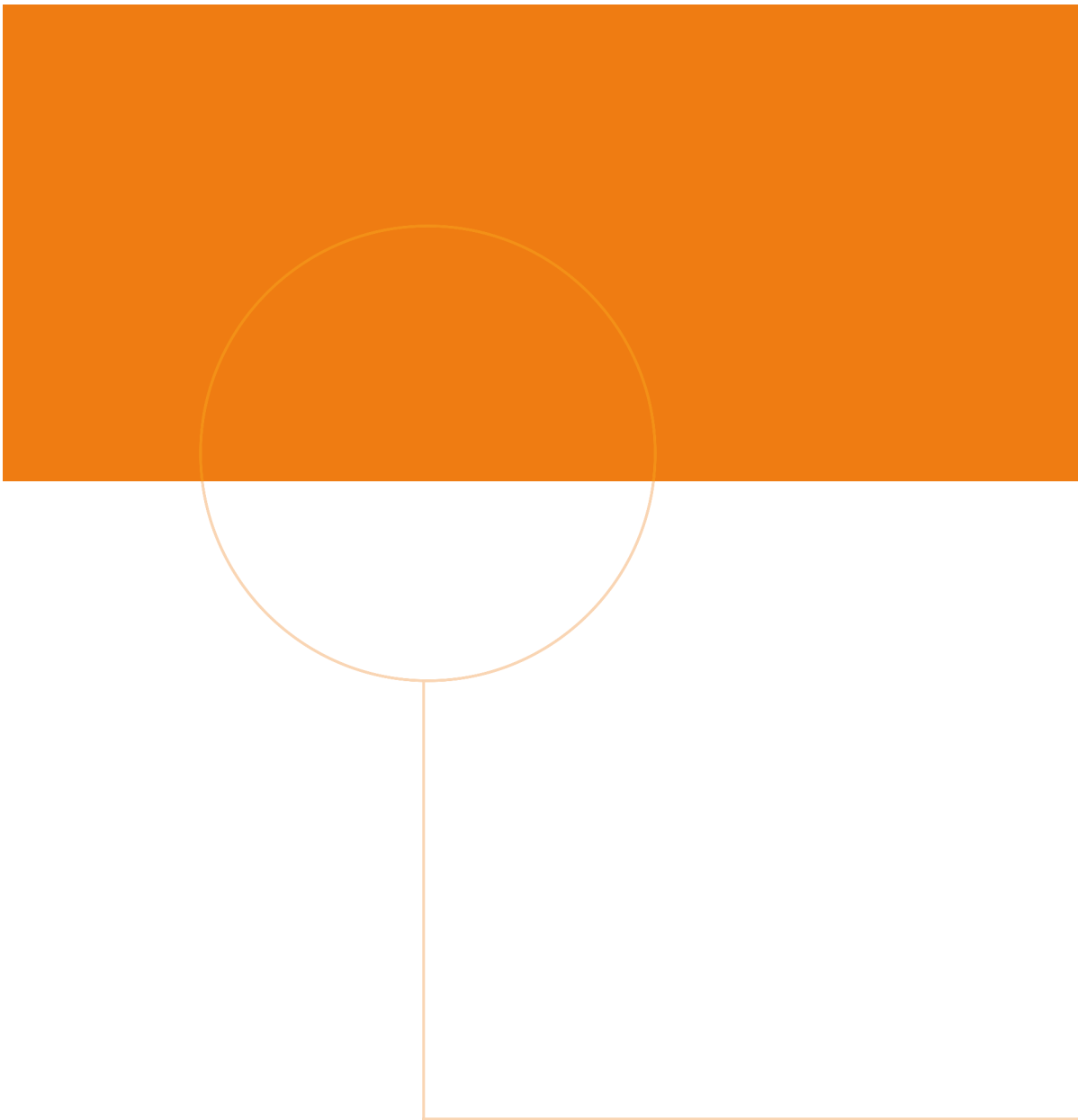
**Informasjon til de registrerte (utvalgene) om behandlingen må inneholde**

- Den behandlingsansvarliges identitet og kontaktopplysninger
- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)
- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)
- Hvor lenge personopplysningene vil bli behandlet
- Retten til å trekke samtykket tilbake og øvrige rettigheter

Vi anbefaler å bruke vår mal til informasjonsskriv.

**Informasjonssikkerhet**

Du må behandle personopplysningene i tråd med retningslinjene for informasjonssikkerhet og lagringsguider ved behandlingsansvarlig institusjon. Institusjonen er ansvarlig for at vilkårene for personvernforordningen artikkel 5.1. d) riktighet, 5. 1. f) integritet og konfidensialitet, og 32 sikkerhet er oppfylt.



NTNU

Kunnskap for en bedre verden