Digital sikkerhetskultur i en hybrid hverdag

En studie av digital sikkerhetskultur ved hybride kontorløsninger

Tore Molde

Masteroppgave 2021

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER: Vår/Høst 2021

FORFATTER: Tore Molde

VEILEDER: Ole Andreas Engen

TITTEL PÅ MASTEROPPGAVE:

Digital sikkerhetskultur i en hybrid arbeidshverdag

EMNEORD/STIKKORD:

Hjemmekontor, hybridkontor, sikkerhetskultur, digital sikkerhetskultur, adferd, kompetanse, holdninger, informasjonssikkerhet og digital sikkerhet

SIDETALL: 90

STAVANGER ……10.12.2021…….

DATO/ÅR

Forord

Med denne masteroppgaven avsluttes et lengre utdanningsløp for meg. Det har vært en lang reise, med mange utfordringer, lange dager og kvelder. Samtidig har det åpnet for utallige diskusjoner med ulike perspektiv i en lærerik og givende prosess.

Jeg vil spesielt takke veileder Ole Andreas Engen for gode diskusjoner og veiledning gjennom master-jungelen. Din kunnskap, nøyaktighet og til tider tydelige forventninger har vært en god los å ha for å vise vei.

Dette studieløpet og masteroppgaven hadde ikke vært mulig uten mine nærmeste. Spesielt vil jeg takke familien min, som har vært der i tykt og tynt. Dere har alle sammen vært en uvurderlig bistand gjennom årenes løp, dette har ikke vært mulig uten dere. Uendelig mange takk.

Når jeg ser tilbake på all tiden som er gått med til utarbeidelsen av denne oppgaven, så er en ting tydelig: Bruk tiden du har godt, vi er bare tildelt en avmålt mengde tid. Så med de udødelige ordene til Pink Floyd og fra deres sang «Time»:

"And you run, and you run to catch up with the sun but it's sinking.
Racing around to come up behind you again
The sun is the same in a relative way but you're older
Shorter of breath and one day closer to death."

Med vennlig hilsen,

Tore.

Sammendrag

I mars 2020 ble tusenvis av arbeidstagere sendt på hjemmekontor over natten. Virksomheter så seg nødt til å digitalisere og implementerte ny teknologi i rekordfart. Mange ansatte opplevde å ikke få veiledning om hvordan de skulle arbeide sikkert hjemmefra. Dette i sammenheng med utviklingen med den økte digitaliseringen av samfunnet, så har vi sett en fremvekst av digitale trusler. Koronapandemien var med på å skjerpe det nasjonale risikobildet. Dette var med på å forme problemstillingen til denne oppgaven: *Hvilke elementer ved digital sikkerhetskultur bør virksomheter prioritere ved hybride kontorløsninger?*

Metodikken for denne oppgaven har vært en kvalitativ, eksplorativ fremgangsmåte. Det er gjennomført flere dybdeintervjuer av informanter med relevant kompetanse i relevante stillinger, som ble vurdert til å representere virksomheter som ble påvirket av *den nye normalen*. Denne nye normalen representeres i denne oppgaven som hybridkontoret.

Det er brukt blant annet litteraturstudier, analyser av spørreundersøkelser gjennomført av blant annet NSM og deres rapport *Nordmenn og digital sikkerhetskultur,* samt andre spørreundersøkelser og studier med hjemmekontor, for å kunne besvare problemstillingen. Funn gjort i intervjuene og i analyse av spørreundersøkelser m.m, har blitt vurdert og drøftet opp mot det teoretiske grunnlaget som oppgaven lener seg på. Det er for øvrig verd å merke seg at selv om det finnes utbredt forskning på hjemmekontor og dens effekt på mennesker er det dog færre studier av utfordringene knyttet til digital sikkerhetskultur, hybridkontoret og den nye normalen.

Denne nye normale medfører både muligheter og utfordringer. For eksempel kan ansatte endre sin adferd, væremåte og holdninger når at de ikke lengre er til stede på kontoret, og ikke deltar i gruppedynamikken og organisasjonskulturen. Videre kan hybride kontorløsning medføre endringer for hvordan en må prioritere for å ivareta og arbeide med en den digital sikkerhetskultur.

Tidligere var flertallet av ansatte «under samme tak», men med hybridkontor vil spredningen av de ansatte kunne føre til at det ikke bare må benyttes andre metodikker for samhandling og kommunikasjon, men også andre vesentlige endringer for hvordan ansatte ledes. Studier viser også at forlenget hjemme eller hybridkontor påvirker den ansattes adferd og holdninger, og

på sikt vil kunne medføre at en får en større sannsynlighet for at det oppstår uønskede hendelser med tap av informasjon, kompromittering av konfidensialitet og integritet.

Løsningen på problemstillingene som oppstår kan finnes i at virksomhetsledere i større grad må jobbe ut ifra tillit og en situasjonsbestemt tilnærming med tettere grad av oppfølging. Videre er det indikasjoner på at ledere i større grad må involvere de ansatte, og kommunisere bredere. Like viktig kan det også være at ledere går foran og er gode eksempler for de ansatte – litt enkelt sagt må de «være gode bjellesauer», samt at man må skape forståelse for hvorfor det er viktig å gjennomføre tiltakene eller følge de forskjellige prosessene, heller enn å fortelle at det må gjøres på den ene eller andre måten.

Innholdsfortegnelse

Oversikt over figurer og tabeller

1. Innledning

Datoen viser 25. september 2021, og de nasjonale tiltakene mot korona er avsluttet. Selv om nordmenn da i stor grad hadde vendt tilbake til en normal hverdag, var ikke dette den samme hverdagen vi kjente til før korona. Ett av tiltakene som ble med videre i den nye normalen er hjemmekontoret.

Hjemmekontor blir av Norsk akademisk ordbok definert som *«det å arbeide hjemme(fra) i en stilling som normalt krever at man er til stede på kontoret hos arbeidsgiveren* (Norsk akademis ordbok, 2021) . Hjemmekontoret har tidligere blitt brukt som et alternativ til å kunne utføre kontorarbeid i en organisasjons kontorlokaler. Bruken av hjemmekontor har da vært et begrenset alternativ i tilfeller der man har tatt imot håndverkere i hjemmet eller for å jobbe noe begrenset samtidig som man har hatt syke barn. Nedstengingen av samfunnet i mars 2020 aktualiserte hjemmekontoret på en helt ny måte som fikk betydning for store deler av norsk arbeidsliv.

Etter lang tid på hjemmekontor, eller med delvis hjemmekontor, gir imidlertid flere uttrykk for ønske om et arbeidsliv som er fleksibelt som gir frihet til å velge hvor, når og hvordan arbeidsoppgaver gjennomføres. Flere gir for eksempel uttrykk for at hjemmekontor passer bedre for konsentrasjonsarbeid enn det åpne kontorlandskapet, og de ønsker seg frihet til å kunne tilpasse omgivelsene til oppgavenes karakter (Akademikerne, 2021).

En slik fleksibel og dynamisk måte å arbeide på, blir av flere definert som en hybrid kontorløsning, eller hybridkontor. En ansatt på hybridkontor vil gjerne ha noen arbeidsdager på kontoret og noen dager utenfor kontoret, det være seg hjemme, på hytta eller på andre lokasjoner. Nøkkelen til hybridkontoret er å tilby en fleksibilitet og la arbeidstakerne velge arbeidssted ut ifra oppgavene som skal løses. Selv om mange arbeidsgivere og arbeidstakere er positive til denne nye måten å organisere arbeidshverdagen på, så medfører hybride kontorløsninger også flere utfordringer på aspekter som det per dags dato finnes lite eller mangelfull forskning på. Disse er blant annet relatert til arbeidsmiljø, sikkerhet, psykososiale tilpasninger og ikke minst det som denne oppgaven vil se nærmere på – hvordan den digitale sikkerhetskultur til virksomheten kan bli påvirket av den ansatte adferd, holdninger og kompetanse på hybridkontoret.

Nedstengningen som startet i mars 2020 medførte også andre nødvendige endringer i arbeidslivet. Arbeidsgivere så det nødvendig å gjennomføre flere endringer i hvordan digitale

tjenester ble gjort tilgjengelig for bruk av sine ansatte eller eksterne kunder/brukere. Med dette fulgte også spørsmålet om hvordan og ikke minst fra hvilke lokasjoner disse tjenestene skulle være tilgjengelige. Mange virksomheter implementerte ny teknologi eller endret eksisterende tjenester nærmest over natten. Denne typen prosjekter ville vanligvis tatt flere måneder eller år å fullføre. Og hva skjedde da med arbeidsprosesser, kultur, kompetanse o.l? Ble disse blitt oppdatert sammen med de nye prosessene som er blitt introdusert for å imøtekomme utfordringene knyttet til denne nye, hybride kontorhverdagen? Eksempelvis påpeker NorSIS i en spørreundersøkelse fra 2021, at så mange som 47 prosent av respondentene, ikke har fått informasjon fra sin arbeidsgiver for regler og/eller rutiner om hva som er gjeldende for digital sikkerhet på hjemmekontoret (Norsk senter for informasjonssikring, 2021a).

1.1. Problemstilling

I denne oppgaven har jeg valgt å se nærmere på ulike typer sikkerhetsutfordringer som kan oppstå som følge av økt bruk av hybride kontorløsninger. Nyere forskningsrapporter og artikler viser til interessante funn og utfordringer knyttet til bruken av hybride kontorløsninger:

Psykososial problematikk: I en artikkel publisert av Norsk forening for arbeidsmedisin(Norsk forening for arbeidsmedisin, 2021) skriver Morten Birkeland Nielsen v/ STAMI(Statens Arbeidsmiljøinstitutt) om enkelte psykososiale aspekter som skaper bekymring vedrørende bruken av hjemme- og hybridkontor. Han peker på økt grad av usikkerhet og stress knyttet til både hvordan oppgaver skal løses og bruk av bruk av verktøy for å løse dem. Manglende balanse mellom krav i jobben og liten kontroll kan gi helseplager på sikt. Det andre aspektet forfatteren trekker frem er at skillet mellom jobb og privatliv hviskes ut når man arbeider hjemmefra. Denne rollekonflikten kan være krevende å stå i over tid og ifølge Birkeland Nilsen mer belastende for helsen og arbeidsevnen enn for eksempel økt arbeidsmengde eller tempo.

Digital trusler: Både NorSIS, NSM, NSR og en rekke andre aktører påpeker hvordan hybridkontor potensielt kan bidra til en vekst i digitale trusler. Bakgrunnen for dette er at:

- Holdninger til sikkerhet kan bli mer avslappet hjemme. (Norsk senter for informasjonssikring, 2020, 2021b; Næringslivets sikkerhetsråd, 2020)

- Mangelfull teknisk sikring og/eller kvalitet av utstyr benyttet på hjemme/hybridkontoret (Norsk senter for informasjonssikring, 2020, 2021b; Næringslivets sikkerhetsråd, 2020).
- En ser en generell økning i mengde og forsterkning av eksisterende cybertrusler (Norsk senter for informasjonssikring, 2021b).
- En potensielt manglende og avvikende kompetanse om digital sikkerhet. (Norsk senter for informasjonssikring, 2021b; Næringslivets sikkerhetsråd, 2020).
- NSM presiserer i helhetlig digitalt risikobilde for 2021 (2021a) at de er bekymret for manglende digital risikoforståelse blant norske bedrifter og virksomheter.

Formålet med denne oppgaven, dens problemstilling og tilhørende forskningsspørsmål er å studere om det er konkrete elementer ved digital sikkerhetskultur en virksomhet bør prioritere ved hybride kontorløsninger. Hypotesen og forstudiet som ligger til grunn, gir indikasjoner på at den ansattes holdninger, adferd og kompetanse spiller en større rolle enn tidligere antatt. Denne oppgaven har som målsetning å se nærmere på er:

Hvilke elementer ved digital sikkerhetskultur bør virksomheter prioritere ved hybride kontorløsninger?

For å kunne besvare dette, er det valgt følgende forskningsspørsmål:

1. *Hvilke digitale sikkerhetsutfordringer opplever/opplevde virksomheter som en følge av nedstengningen grunnet koronatiltakene og hybride kontorløsninger?*

2. *Hvordan kan den ansattes kunnskap, adferd og holdninger påvirke digital sikkerhetskultur i en hybrid kontorsituasjon?*

Oppgaven baserer seg på semistrukturerte intervjuer av informanter som arbeider innen sikkerhet, sikkerhetskultur, digitalisering, HR tjenester og digital sikkerhet. Det vil også bli studert og vurdert større spørreundersøkelser som er komparative og representative for oppgaven, og som er utført av ledende aktører og arbeidsgivere. For å få et best mulig utvalg av informanter, så representerer informantene er bredt spekter av virksomheter innen forskjellige sektorer, og både små, mellomstore og nasjonale aktører er representert.

På samme måte som det er et bredt spekter med virksomheter, representerer også informantene forskjellige fagfelt og kompetanseområder. Informantene innehar stillinger som CISO, Sikkerhetssjefer, Direktører innen digitalisering og informasjonssikkerhet samt

avdelingsleder og senior rådgivere innen HR og digitalisering. Informantene og prosessen rundt intervjuene er nærmere beskrevet i kapitel 4.3.

1.2. Bakgrunn og motivasjon

Informasjonsteknologi og digital samhandling, har skapt og endret mange strukturer innad i virksomheters forståelse for når, hvor, hvordan og av hvem arbeid kan og skal utføres. I henhold til Schein (2009) har kulturer en tendens til å vokse frem som en følge av interaksjoner mellom samlokaliserte medarbeidere/kollegaer. Schein (2009) stiller spørsmål til hvilke type kulturer og subkulturer som kan og vil vokse frem innen nettverk av kollegaer som er elektronisk forbundet og som aldri vil møte hver andre: Det er av forfatterens oppfattelse og mening at det er nødvendig å se nærmere på hvordan en kan legge til rette og etablere gode rammer både for en god sikkerhetskultur og en trygg digital tilstedeværelse i hybride kontorløsninger.

På feltet hybride kontorløsninger, så finnes det per i dag ikke store mengder forskning tilgjengelig. Hjemmekontor er her et mer definert begrep som det tilsvarende finnes mer forskning på. STAMI (Statens arbeidsmiljøinstitutt) og deres rapport «Arbeid hjemmefra, helse og arbeidsmiljø – En systematisk kunnskap oppsummering» (Statens arbeidsmiljøinstitutt, 2021) har imidlertid sett nærmere på problematikken rundt hjemmekontoret. I denne rapporten har de systematisk vurdert forskning og publikasjoner rundt temaet tilhørende hjemmekontor, hvor Pål Molander, direktør uttaler*: «Hovedkonklusjonen er at kunnskapsgrunnlaget er svakt og at norske virksomheter risikerer å fatte endringsbeslutninger på spinkelt kunnskapsgrunnlag»* (Statens arbeidsmiljøinstitutt, 2021). Tilsvarende har NITO på sin side gjennomført en medlemsundersøkelse, hvor flere stiller seg negativ til hjemmekontor og har hatt eller har psykisk eller fysiske negative plager forbundet til å jobbe fra hjemmekontoret.

Rapporten «Hjemmekontor: utbredelse og sentrale kjennetegn våren 2021» er blitt utarbeidet av Arbeidsforskningsinstituttet AFI ved OsloMet på oppdrag av Arbeids- og sosialdepartementet. I denne rapporten kommer det frem (av 2578 besvarelser) at 14% ønsker hjemmekontor 3-4 dager i uken, mens 30% ønsker 2 dager i uken på hjemmekontor. Tar vi med de som ønsker 1 dag (21%) i uken på hjemmekontoret, så kommer det frem at 65% ønsker hjemmekontor i en eller annen grad etter at Koronapandemien er over. Tilsvarende

resultater kan en finne iblant arbeidslivsundersøkelser gjennomført av Telenor(referanse) og NHOs medlemsundersøkelse fra mars 2021.

NSM/PST har i sine årlig trussel rapporter (Nasjonal sikkerhetsmyndighet, 2020, 2021b) påpekt en tydelig økning det siste året i både forsøk på svindel, phising, direktørsvindel m.fl. Det finnes eksempler på hvordan direktørsvindel tidligere har blitt avslørt med bakgrunn i tilfeldig og direkte sosial interaksjon. Men hvordan skal arbeidsgivere klare å opprettholde kunnskapen og årvåkenheten til sine ansatte, hvis de nå i større grad skal jobbe hjemmefra? Og hvordan kan arbeidsgivere minimere de sikkerhetsutfordringene man står ovenfor i overgangen til hybride kontorløsninger?

1.3. Avgrensinger

For at omfang på oppgaven skulle være overkommelig både i tid og størrelse, var det nødvendig å gjøre konkrete avgrensinger. Nødvendigheten for en avgrensning ble tydelig som en del av forstudiet. Fokuset for denne oppgaven vil være å se om det er områder eller elementer av en digital sikkerhetskultur som utpreger seg som mer utsatt enn andre som følge av hybride kontorløsninger – de områdene som vil bli spesielt vektlagt og vurdert er adferd, kompetanse og holdninger. Det er av forfatteren oppfattelse at digital sikkerhetskultur vil være avgjørende fremover i den *«nye normale»* og hvordan vi jobber hjemmefra eller kontoret. Videre forskning på dette området vil være viktig, da det er uavklart og usikkert hvordan dette potensielt kan ha innvirkning på organisasjons-, sikkerhets og den digitale sikkerhetskulturen.

2. Begrepsavklaring

Denne oppgaven bygger på en rekke teori og perspektiver som det er viktig å ha en grunnleggende forståelse for. Dette kapitelet tar høyde for å avklarere noen av de viktigste begrepene som er i bruk i denne oppgaven.

2.1. Risiko

Den tradisjonelle beskrivelsen var lenge at risiko var noe som kom til uttrykk ved å multiplisere sannsynlighet for, og konsekvensen av en uønsket hendelse.

Risiko er nødvendigvis ikke en negativ effekt og/eller resultat. Dette påpekes av Aven og Renn som også påpeker at risiko kan være av positiv faktor (Aven & Renn, 2010). En slik tilnærming kommer også frem i ISO 31000:2018 *«Retningslinjer for Risikostyring»* (Standard Norge, 2018) og 31004:2013 *«Risikostyring - Veiledning til implementering av NS-ISO 31000»* (Norsk Standard, 2013):

«Risiko – virkningen av usikkerhet knyttet til et mål. Begrepsmerknad 1: En virkning er et avvik fra det forventede. Den kan være positiv, negativ eller begge deler og kan ta for seg, skape eller resultater i muligheter og trusler»

ISO 31004:2013(Norsk Standard, 2013, s. 7): «*En risiko oppstår eller endres når beslutninger tas. Siden det nesten alltid er noe usikkerhet assosiert med beslutninger eller når beslutninger tas, så vil det nesten alltid være risikoer tilstedte. De som er ansvarlig for å oppnå resultater må forstå og sette pris på at risiko er en uunngåelig del av en organisasjons aktiviteter når beslutninger tas. Risikoer assosiert med beslutninger bør være forstått på det tidspunktet en beslutning tas, og at tilhørende risikoer tas med vilje og informert.»*

2.2. Digitalisering

Mye at det teoretiske grunnlaget innen det digitale området som danner utgangspunktet for denne oppgaven, har sitt utspring fra blant annet veiledere utgitt av nasjonale aktører i Norge. Dette er aktørene som Nasjonal sikkerhetsmyndighet (NSM), NorSIS, Digdir m.fl.

Som definisjon/beskrivelse av digitalisering i denne oppgavens kontekst, brukes ordlyden slik det står beskrevet i «Samfunnssikkerhet i en usikker verden st.meld 2020-2021»:

«Digitalisering er en betegnelse på hvordan samfunnet i økende grad tar i bruk og gjør seg avhengig av informasjons- og kommunikasjonsteknologi. Stadig flere produkter og tjenester er avhengig av IKT-infrastruktur og nettilkobling. Det er en vedvarende og svært kraftig vekst av data som lagres. Gjennom utvikling av mobilnettene (5G), bruk av sensorteknologi og kunstig intelligens vil vi få nye digitale tjenester som vil fornye og forbedre måten vi lever og arbeider på. Vår hverdag er digital, primært til det gode for privatpersoner, virksomheter og forvaltningen. Samtidig endrer digitaliseringen risikobildet.» (Justis og beredskapsdepartementet, 2020, s. 27)

Graden av fokus på digitalisering har vært svært varierende i norske virksomheter. For de som ikke har hatt dette fokuset, har den pågående korona pandemien på mange måter vært en katalysator for økt digitalisering. KS (Kommunsektorens organisasjon, 2021) viser til at pandemien har satt fart på digitaliseringen i kommune-Norge. 9 av 10 kommunedirektører har innført nye digitale løsninger under pandemien. Kommunene er også blitt mer positive til digital samhandling og de opplever at digitale løsninger nå gir dem bedre kapasitet , tilgjengelighet og høyere kvalitet (Kommunsektorens organisasjon, 2021). Dell Technologies (Dell Technologies, 2020a) har gjennomført en tilsvarende undersøkelse (Digital transformation Index (DT Index)(Dell Technologies, 2020b) , denne viser at blant 4200 forretningsleder i mellomstore og store virksomheter har pandemien medført at 75% har fremskyndet sine digitaliseringsprosjekter. Digitalisering handler ikke bare om å ta i bruk nye digitale tjenester, men også hvordan en endrer arbeidsprosesser og hvordan mange virksomheter fungerer i sin helhet (EenerWE Partner, 2017; Store Norske leksikon, 2019).

2.3. Digitale trusler og sårbarheter

NSM (2021b) skriver i sin årlig risiko rapport: «*Rask digitalisering endrer og skaper nye samfunnsverdier. De lange, digitale verdikjedene som dannes for å understøtte tjenester og funksjoner i samfunnet, medfører samtidig nye sårbarheter og avhengigheter trusselaktører kan utnytte. Dette resulterer i et skjerpet digitalt risikobilde».* NSM (2021b) fremhever også at det har oppstått nye personellmessige utfordringer og sårbarheter relatert til informasjon teknologi som en følge av endrede arbeidsmønstre og raskere digitalisering. De påpeker også et meget komplekst risikobilde, som vil i økende grad være gjeldende i tiden fremover, basert på de endrende økonomiske ringvirkninger og dynamikk som koronapandemien har medført. økonomiske ringvirkninger og dynamikk som korona pandemien har medført.

2.4. Informasjon- og cybersikkerhet

Informasjon og cybersikkerhet er begreper som brukes om hver andre i dagligtale. For mange kan det utfordrende å skille disse fra hverandre. *Informasjonssikkerhet* handler i denne oppgaven som om at informasjonen ikke bli kjent for uvedkommende (**Konfidensialitet)**, at informasjonen ikke blir endret utilsiktet eller av uvedkommende (**Integritet)** og at informasjonen er tilgjengelig for autoriserte brukere ved behov (**Tilgjengelighet).** Dette er omtalt som KIT (CIA) prinsippet innen informasjonssikkerhet (Bergsjø, Windvik & Øverlier, 2020; Digitaliseringsdirektoratet, 2021a):

2.5. Digital sikkerhet

Begrepet *cybersikkerhet* vil i denne oppgaven være koblet mot digital sikkerhet. Dette er et begrep som *«… Handler om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjon- og kommunikasjonsteknologi. Brukes synonymt med begrepene IKT-sikkerhet og cybersikkerhet»* (Justis og beredskapsdepartementet, 2020, s. 79).

2.6. Robusthet og resilience

Et annet viktig begrep som brukes i sammenhengen med digital sikkerhet, er *robusthet.* Dette kan ses på som evnen til å gjenopprette en normaltilstand etter at en uønsket hendelse eller avvik har funnet sted (Datatilsynet, 2021). Robusthet omtales også som resilience. Resilience defineres av Engen et al. (Engen, Kruke, Lindøe, Olsen, Olsen & Pettersen, 2016) *«som den kapasitet et sosialt system har til å motstå og tilpasse seg forventede og uventede forstyrrelser, og til å gjenopprette funksjonaliteten etter alvorlige påkjenninger fra slike forstyrrelser»*.

3. Teori

Det vil i dette kapittelet diskuteres teori om sikkerhetskultur og se den opp mot et teoretisk perspektiv rundt digital sikkerhetskultur. Det vil bety å vise hvordan organisasjonskultur, subkultur og sikkerhetskulturer henger sammen.

Sett i lys av at store deler av arbeidet ved hybridkontor gjennomføres på lokasjoner utenfor kontorlokalene, kan det oppstå nye og andre problemstillinger knyttet til sikkerhetskulturen. Her vil en god digital sikkerhetskultur kunne spille en avgjørende rolle for å unngå uønskede hendelser innen den digitale sfæren.

Det teoretiske grunnlaget i denne oppgaven vil:

- Vise hvordan organisasjonskultur, subkultur, sikkerhetskultur henger sammen og hvordan en ut ifra disse prinsippene kan forstå digital sikkerhetskultur. Dette er viktig, da sikkerhetskultur er direkte avledet fra organisasjonskultur, og inneholder viktige ledelseskomponenter for sikkerhetsstyring.
- Vise teorier rundt ledelse, sikkerhetsstyring og som sammenfaller med og understøtter utfordringene rundt ledelse av blant annet arbeidstakere som jobber, eller ønsker å jobbe fra en hybrid kontorsituasjon.
- Gi en forståelse for uønskede hendelser, og hvordan disse kan oppstå i virksomheter.

3.1. Hybride kontorløsninger

Hybride kontorløsninger eller hybridkontor er et forholdvis nytt begrep, og brukes vekselsvis sammen med uttrykket hjemmekontor. Om uttrykket h*ybrid*, så kan en si at det er noe som forekommer, når det er en krysning eller når flere sammensetninger oppstår av flere elementer(Norsk akademisk ordbok, 2021; Store Norske leksikon, 2021a). Hybridkontor har sitt utgangspunkt i hjemmekontor, eller internasjonalt *Remote work, teleworking* (RWT) eller *Work from home* (WFH). Arbeidsforskningsinstituttet (AFI) ved OsloMET har i sin rapport «Hjemmekontor: Utbredelse og sentrale kjennetegn våren 2021» (Holm Ingelsrud & Hoff Bernstrøm, 2021) definert hjemmekontor som *«… å jobbe hjemmefra eller et annet sted som man selv velger, om man skulle ønske det*». AFI bygger sin definisjon på International labour organization (ILO) og deres guide Teleworking during the corona-19 pandemic and beyond (ILO, 2020). En viktig presisering som ILO gjør, er at *teleworking* ikke benyttes for å definere dem som alltid jobber utenfor et fast arbeidsted, type freelancene o.l (ILO, 2020).

Hjemmekontor har i utgangspunktet tidligere vært noe som var sporadisk, midlertidig og ikke på fast basis. Hybridkontor blir å anse som noe fast, hvor arbeidstakere jobber fast fra andre lokasjoner enn etablert eller definert arbeidssted/kontor på faste angitt tidspunkt eller dager. Sporadisk hjemmekontor har tidligere ikke vært problematisk fra et lovmessig ståsted. Men med etablering av en fast ordning som hybridkontor, oppstår det uklarheter i f.eks. arbeidsmiljølovgivningen, eksempelvis forskrift 5. juli 2002 nr. 715 om arbeid som utføres i arbeidstakers hjem. §1 i denne forskriften (Forskrift om arbeid som utføres i arbeidstakers hjem, 2002) står det «Denne forskriften gjelder for arbeid som utføres i arbeidstakers eget hjem. Forskriften gjelder ikke kortvarig eller tilfeldig arbeid.»

Forskriftsmessig og lovmessige elementer vil ikke bli videre gjennomgått, men det illustrerer hvor ny og foreløpig noe udefinerbar den hybride kontorløsninger er. Det er nærliggende å forvente at det vil komme endringer innen dette området i nærmeste fremtid.

I denne oppgaven vil begrepet hjemmekontor bli brukt når man på enkelte tidspunkt velger å gjennomføre arbeidsoppgaver hjemmefra basert på midlertidig behov. Hybrid kontorløsning vil beskrive situasjonen der en på fast basis fordeler arbeidstiden mellom arbeidsplassen og sted valgt selv av arbeidstakeren.

3.2. Organisasjons- og subkulturer

Alle virksomheter har en kultur, og på en eller annen måte har de fleste virksomheter søkelys på, og arbeider med, sikkerhetskultur og adferd. Kultur som begrep kan defineres på ulike måter, og innen den relevante forskningen finnes det flere definisjoner. Definisjonene varierer ut ifra hvilket perspektiv en betrakter begrepet, for eksempel fra et sosialpsykologisk eller organisatorisk perspektiv (Bang, 2020).

En klassisk antropologisk definisjon av *kultur* tilskrives E.B Taylor, som i 1871 beskriver kultur slik; *«Kultur er den sammensatte helhet, som omfatter viten, tro, kunst, rett, moral, skikker og alle andre ferdigheter og vaner som mennesket erverver som medlem av samfunnet»* (E.B Taylor sitert i Schiefloe, 1999, s. 2).

Deal og Kennedy (1982, s.4 - gjengitt fra Bolman, Thorbjørnsen og Deal (2014), s.298) har en generell kultur definisjon. Den sier at kultur er *«måten vi gjør ting på her hos oss».* Dette er et begrenset begrep, men viser en etablert og utbredt forståelse for hva mange legger i begrepet kultur i en organisatorisk kontekst iht. Bolman et al. (2014).

Begrepet kultur er også beskrevet av Edgar Schein. Iht. Schein (Schein, 2009, s. 27): *«Kultur er et mønster av grunnleggende antakelser utviklet av en gitt gruppe etter hvert som den lærer å mestre sine problemer med ekstern tilpasning og intern integrasjon – som har fungert tilstrekkelig bra til at det blir betraktet som sant, og som derfor læres bort til nye medlemmer som den riktige måten å oppfatte på, tenke på og føle på i forhold til disse problemene»* (Norsk oversettelse gjengitt Jacobsen & Thorsvik, 2016, s. 130)

Schein deler kultur inn i fire typer. ***Makrokultur*** er typiske kultur fenomener vi finner på nasjonalt eller et mer globalt nivå. Disse kan gjerne videre være basert på etniske, religiøse eller andre yrkesgruppe typer. En kan bruke legeyrket som et eksempel. Det finnes en global kultur for hvordan legeyrket er, men den vil bli påvirket av makrokulturen for hvordan legeyrket utøves på grunn av påvirkning av kulturen i det aktuelle landet (Schein & Schein, 2017)

Organisasjonskulturer (Schein & Schein, 2017)er noe en finner i alle typer virksomheter. Det skilles ikke mellom om organisasjonen er privat, offentlig eller veldedig. Verdensomspennende virksomheter som Microsoft eller IBM har en organisasjonskultur som dekker et globalt aspekt. ***Subkulturer*** *(Schein & Schein, 2017)* finner en internt i en organisasjon i dens avdelinger, divisjoner og andre typer gruppering som oppstår. Subkulturer i en organisatorisk sammenheng oppstår ofte i sammenheng med yrkesgrupper. Til slutt har vi ***mikrokulturer*** *(Schein & Schein, 2017)*; dette er et kulturelt aspekt som oppstår i mindre grupperinger i eller utenfor en organisasjon. Mikrokulturer er ikke nødvendigvis basert på yrkeskategorier, men mer i retning av mindre gruppering som jobber tett sammen i et prosjekt, av nødvendighet eller lignende. Det finnes lite kjent forskning på dette området sett fra ett hjemme- hybridkontor perspektiv, men fra et teoretisk perspektiv vil vi kunne se en fremvekst av mikrokulturer som en følge av hjemmekontorbruken i løpet av pandemien. Det kan argumenteres for at, som en følge av pandemien og utstrakt bruk av hjemmekontor, vil en nå kunne se at en mengde nye mikrokulturer har oppstått og har fått etablert seg i flere virksomheter.

Schein (2017) påpeker at kulturbegrepet er komplekst da det inneholder flere typer og nivåer. Videre uttrykker Schein (2017) at en organisasjonskultur har tre forskjellige nivåer:

- Artefakter (artifacts)
- Tiltalte verdier (Espoused values)
- Grunnleggende antagelser (Basic assumptions /Underlying assumptions)

Figur 1 (til høyre): Visualisering av Scheins kultur nivåer (Vidya Hattangadi, 2017)

Artefakter er det nivået som er mest synlig og bevisst ved en organisasjonskultur. Dette er den delen av kulturen du kan se, høre og føle. En må være seg bevist på hvordan en oppfatter og tolker disse artefaktene for de kan være vanskelige å tolke og å avdekke hvordan de er utformet og er med på å utforme organisasjonskulturen (Schein, 2009). Et eksempel som Schein (2009) bruker er pyramider. Dette ble bygget av blant annet Maya indianere og Egyptere i oldtiden. De er tydelige artefakter på en kultur, men de representerer veldig forskjellig kulturer. Andre eksempler på artefakter kan være ID-kort, utforming av kontorlandskap, bekledning, og andre ritualer på en arbeidsplass. De er lette å observere, men kan være vanskelig å tolke.

Verdier *(Espoused values)* representeres med en organisasjons verdier, målsetning, visjon m.fl. og er kort fortalt tuftet på verdigrunnlaget til organisasjonen. Dette blir ofte synlig gjennom oppførselen til ansatte som representerer organisasjonen, og har ofte sitt utspring fra ledelsen i en organisasjon.

Grunnleggende antagelser *(underlying /basic assumptions)* er de tingene man gjerne tar for gitt. Dette foregår gjerne på et ubevisst nivå, og man kan si at dette nivået handler om ting som er immaterielle, med andre ord, elementer en ikke kan ta og føle på. Det farges gjerne av hva medarbeidere mener er riktig, hva de mener bidrar til utvikling, hva mestring betyr, de historiene som fortelles til nyansatte. Som Schein (2017) påpeker tar dette nivået ofte utgangspunkt i tidligere erfaringer og hvordan problemer har blitt løst tidligere.

Når en vurderer forskjellige definisjoner av begrepet kultur eller organisasjonskultur, så er det viktig at de vurderes ut ifra den kontekst den skal beskrive. (Bang, 2020). Dette påpekes også av Jacobsen og Thorsvik med at organisasjonskultur skiller seg fra generell kultur og andre kulturelle prosesser nemlig med at organisasjonskultur oppstår innenfor en

organisasjonsmessig sammenheng (Jacobsen & Thorsvik, 2016). Dette er med på å danne grunnlaget og utgangspunktet for hvordan organisasjonskultur og dens oppbygging kan forstås. Digital sikkerhetskultur har sitt utspring i, og er en intrikat del av den helhetlige organisasjonskulturen, og defineres derfor som en sub- eller mikrokultur.

Som tidligere nevnt, og med Schein's utgangspunkt for kulturtyper, så vil en organisasjon som utvikler seg og vokser over tid også utvikle nye grupperinger med tilhørende delkulturer. Dette kalles en subkultur. Bang (2020) forklarer en subkultur som en undergruppe, som består av organisasjonens eller virksomhetens medlemmer og hvordan disse samhandler over tid med hverandre. Fellesskapet danner grunnlag for at de identifiserer seg med hverandre. Ett slikt fellesskap eller subkultur, deler et sett av felles normer, verdier, og det oppstår en delt virkelighetsoppfattelse (Bang, 2020).

Figur 2: Organisasjonskultur og subkulturer (Gjengitt etter Kaufmann & Kaufmann, 2015, s. 370)

I figur 2 ovenfor finner vi eksempler på slike undergrupper eller subkulturer. Disse kan være avdelinger eller konkrete profesjonskulturer som igjen ofte har egne kjerneverdier. Kaufmann (Kaufmann & Kaufmann, 2015) illustrerer en slik inndeling med f.eks. ingeniørgrupperinger eller sykepleiere på ett sykehus.

3.3. Kulturelle konsekvenser av hjemmekontor

Schein (Schein & Schein, 2016) påpeker at subkulturer kan utvikle seg på en slik måte at de avviker eller kommer i direkte «konflikt» med den overordnede organisasjonskulturen. En slik konflikt kan for eksempel være at subkulturen, f.eks. med de som «jobber på gulvet», ikke har samme interne verdi/subkulturgrunnlag som ledelsen, som på sin side representerer en annen og gjerne mer overordnet del av organisasjonskulturen (Schein, 2017). Schein (2017) mener at en leders forståelse av subkulturer er viktigere enn noen gang tidligere, blant annet fordi subkulturer kan være like sterke, eller sterkere enn den overordnede

organisatoriske kulturen. Det er viktig å være oppmerksom på at *digital sikkerhetskultur* kan representerer både en sammensatte sub- eller en mikrokulturer. En av hensiktene med å arbeide med en digital sikkerhetskultur er å skape en helhetlig og omforent måte å jobbe trygt, sikkert og effektivt på i det digitale rommet. Med opprettelse av hybride kontorløsninger vil en organisasjon i større grad kunne bli mer fragmentert og medarbeiderne vil i større grad kunne jobbe fra et økende antall lokasjoner (Holm Ingelsrud & Hoff Bernstrøm, 2021). Man ser at medarbeidere gjennom pandemien i større grad jobbet tettere med sine kollegaer og mindre tett på ledelsen (Holm Ingelsrud & Hoff Bernstrøm, 2021), og det er nærliggende å anta at flere nye subkulturer og mikrokulturer har oppstått som en følge av dette. Hybride kontorløsninger vil kunne bidra til å forsterke dette ytterligere. Utfordringen for ledere kan oppstå da disse sub- og mikrokulturene blir vanskeligere å oppdage, og at de kan oppstå uten at ledelsen er bevisst på utviklingen.

3.4. Sikkerhetskultur

En av dem som har forsket på det organisatoriske perspektivet av ulykker er James Reason. Reason (1997) påpeker at en god sikkerhetskultur er motoren som driver systemet mot målsetningen om maksimal sikkerhetshelse, uavhengig av ledelsens personlighet eller nåværende kommersielle bekymringer. Selv om *maksimal sikkerhetshelse* er et ideal som kan være vanskelig å oppnå i den virkelige verden, påpeker Reason (1997) at det er en målsetning det er verd å jobbe mot. Det er med andre ord en kontinuerlig prosess mot en ideell tilstand.

Reason (1997) har i sin forsknings satt søkelys på organisatorisk ulykker/uønskede hendelser. Det er spesielt hendelser innen kompleks, moderne teknologi hans fokus dreier seg rundt. Selv om hans fokus i all hovedsak var mot teknologier som atomkraftverk, flyindustrien, transport, banker m.m, så kan man trekke korrelasjoner fra hans teoretiske perspektiv inn mot komplekse systemer/prosesser som vi finner i dagens teknologiske og digitale samfunn. Med digitalisering kan man ende opp i en situasjon hvor risikobildet forverres, ikke bare fra organisasjonens ståsted, men også med øket risiko for nasjonale funksjoner. En slik kompleksitet bekymret også regjeringen; som påpekte i *Nasjonal strategi for digital sikkerhet* (Justis og beredskapdepartemenet, 2019). hvordan økende grad av digitalisering av kritiske nasjonale funksjoner vil kunne skape ett forverret risiko og trusselbildet. Denne bekymringen ble også en realitet da, NSM i sin rapport Risiko 2021 og helhetlig digital risikobilde (Nasjonal sikkerhetsmyndighet, 2021a, 2021b) påpekte at den økte digitaliseringen gjennom 2020 og 2021 har bidratt til å forsterke det digitale trusselbildet.

Reason (1997 s. 194) påpeker at en *god* sikkerhetskultur kan formes ved at en prosess der en danner prosesser og betingelser som er med på å bearbeide verdier og oppfatninger i en bestemt og ønsket retning. En slik sikkerhetskultur er av hva Reason definerer som en informert kultur. I følge James Reason(1997) består en slik sikkerhetskultur av følgende elementer, rapporterende, rettferdig, fleksibel og lærende. Dette skaper sammen den informerte kulturen som Reason påpeker er nødvendig.

En **informert** sikkerhetskultur forutsetter at det er etablert et organisatorisk organ som fanger opp, analyserer og formidler informasjon til alle i organisasjonen om uønskede hendelser og nesten-uhell, så vel som proaktivt arbeid fra revisjoner og andre sikkerhetsanalyser. Når en organisasjon er velinformert vil den være i stand til å oppnå en «god» sikkerhetskultur ifølge Reason (1997, s. 195).

I en **rapporterende** kultur må det skapes en opplevelse av likevekt mellom ansattes rapportering, og at ledelsen tar tydelig ansvar for å motivere og gi støtte til å behandle og utveksle informasjon.

I en **rettferdig** sikkerhetskultur, påpeker Reason viktigheten av å ha gjensidig tillit til systemet. Det er viktig å forsøke å etablere en «no-blame» kultur. En organisasjonskultur som gir amnesti og ikke fordeler skyld, er ikke ønskelig ei heller gjennomførbart. Det er viktig å beholde kredibiliteten til justisen internt i en organisasjon, hvis ikke vil dette potensielt kunne medføre annen uønsket adferd. Den rapporterende kulturen må være rettferdig (Reason, 1997, s. 195).

I den rettferdige delen av en god sikkerhetskultur er tillit sentralt. Den ansatte oppfordres strekt til å rapportere feil, mangler eller andre uønskede hendelser. Dette gjøres med den forutsetning at hendelsen ikke er gjort med overlegg og dermed ikke vil føre til straff, med mindre tydelig uansvarlig oppførsel kan bevises.

En **fleksibel** kultur må ta høyde for å kunne tilpasses mange forskjellige former. I mange tilfeller dreier det seg om å kunne endre seg fra en hierarkisk til en flat organisasjonsstruktur, men også sett fra den ansattes ståsted. Det vil kunne være situasjoner hvor kontrollen flyttes til personell på stedet, for så å gå tilbake til en mer byråkratisk struktur, når situasjonen er over. Reason (1997) er tydelig på at en slik type tilpasningsevne er et essensielt element hos en organisasjon som har planlagt og tatt høyde for mulige uønskede hendelser. Det som må vektlegges tungt, er organisasjonen tillit og respekt for kunnskapen og evnene til sine ansatte.

Ifølge Reason (1997) kreves det investering i kompetansehevning og kursing for å oppnå en kultur for **læring**. Dette er nødvendig for at en organisasjon skal kunne lære av sine feil og utvikle seg ved å iverksette nødvendige tiltak og endringer basert på erfaringer.

Informasjonsflyt som utgangspunkt for sikkerhetskultur

Westrum og Adamski (2009) koblet sikkerhetskultur til informasjonsflyt. Ifølge Westrum (2014) er overlevelsen til en organisasjon koblet til informasjonsflyten. En organisasjon vil ifølge Westrum (2014) slutte å fungere hvis informasjonsflyten ikke er funksjonell, da informasjon er nødvendig for å ta beslutninger. Informasjonsflyt kan kobles opp mot hvordan sikkerhetskulturen er i en virksomhet. Westrum og Adamski (2009) skiller mellom tre former for sikkerhetskultur; patologisk, byråkratisk og generativ. Disse kulturene har forskjellige perspektiver og er beskrevet på bakgrunn av organisasjonens evne til å behandle og reagere på sikkerhetsinformasjon. Fokus for denne oppgaven ligger på det generative perspektivet, da dette kan settes i sammenhengen med en god sikkerhetskultur og hvordan en god *digital* sikkerhetskultur bør vurderes.

Den **patologiske** kulturen kjennetegnes av tilstand der en undertrykker eller pakker inn problemet. Den **byråkratiske** kulturen preges av fokus rundt strukturer der en har en reaktiv holdning til uønskede hendelser. **Generative** kultur legger vekt på utvikling og nyskapning gjennom proaktivt arbeid, der ansvar deles og belønninger gis. Den generative kulturen kan omfatte alle aktiviteter som har betydning for beslutninger og valg som foretas i en organisasjon.

Det er den generative kulturen anses som den gode sikkerhetskulturen (Westrum & Adamski, 2009). Dette er en kultur hvor:

- En aktivt søker etter informasjon
- En lærer opp og belønner budbringere
- Det er delt ansvar
- Avdekkede feil fører til endring
- Nye ideer ønskes velkommen.

Et element som vi finner hos flere forfattere er viktigheten av god opplæring og ikke minst god informasjonsflyt. Westrum sier *"When there is a lack of dialogue, unpleasant thing can happen"* Westrum og Adamski (2009, s. 5-8).

Perspektivene til Reason og Westrum kan brukes til å beskrive problemstillinger som kan oppstå i virksomheter som tilbyr hybride kontorløsninger til sine ansatte. Det er flere kjerneelementer som det er viktig å kontinuerlig sette søkelys på, som proaktivitet, tillit og åpenhet og mange av de elementene som trekkes frem av Reason og Westrum har direkte relevans for digital sikkerhetskultur.

3.5. Digital sikkerhetskultur

Digital sikkerhetskultur som begrep har ingen helhetlig og definert definisjon (Pedersen & Ottestad, 2019). Begrepet *digital sikkerhetskultur* først nevnt i rapporten Nordmenn og digital sikkerhetskultur av NorSIS i 2016 (Norsk senter for informasjonssikring, 2016) og er videre utviklet over tid (Pedersen & Ottestad, 2019).

Digital sikkerhetskultur er våre felles verdier, holdninger, normer, kunnskaper og handlinger som bidrar til at vi unngår å bli rammet av digitale trusler (Norsk senter for informasjonssikring, 2020, s. 11).

Det store spriket og antall variasjoner av begrepet digital sikkerhetskultur, kan gjøre det utfordrende å falle ned på en definisjon som alle kan være enig i. Men gitt oppgavens problemstilling og med utgangspunkt i et organisatorisk perspektiv, og ikke samfunnsmessig i sin helhet, er definisjon til Digitaliseringsdirektoratet valgt:

«Sikkerhetskulturen er en del av organisasjonskulturen, og handler derfor om hvilke verdier som ligger til grunn for den enkeltes valg for håndtering av informasjon og systemer. Sikkerhetskultur er dermed den felles oppfattelsen virksomheten har som har positive eller negative konsekvenser for informasjonssikkerheten.» (Digitaliseringsdirektoratet, 2021c; Nettvett, 2021).

Definisjonene kan kobles opp mot Reason (1997) på flere områder, men også Westrum (Westrum, 2014; Westrum & Adamski, 2009). Den plukker spesielt frem viktigheten av kompetanse, holdninger, verdier, normer mfl. som igjen er tett relatert til kultur og hvordan organisasjonskulturer oppstår. Definisjonen til Digitaliseringsdirektoratet bygger på det teoretiske grunnlaget utarbeidet av NorSIS vedr. Digital sikkerhetskultur (Digitaliseringsdirektoratet, 2021b, 2021c).

NorSIS har utarbeidet åtte dimensjoner for hva utgjør en digital sikkerhetskultur. Disse er sammenfallende med både Reason (1997) og Westrum (Westrum, 2014; Westrum &

Adamski, 2009), uten at det kan konkluderes på noen måte at disse ligger til grunn for NorSIS sin rapport.

Disse punktene er som følger (Bergsjø et al., 2020; Digitaliseringsdirektoratet, 2021b, 2021c; Nettvett, 2021);

1. Fellesskap
2. Styring og kontroll
3. Tillit
4. Risikooppfattelse
5. Optimisme for teknologi og digitalisering
6. Kompetanse
7. Interesse for teknologi og IT
8. Adferdsmønstre

Disse åtte dimensjonene anses som nøkkelen til å beskrive digital sikkerhetskultur helhetlig. De gir ikke en detaljert oppskrift for hvordan en skal oppnå en god kultur, men gir anbefalinger for arbeid og fokus områder.

Fellesskap er et begrep som er viktig i kultursammenheng. Det påpekes av flere (Bang, 2020; Jacobsen & Thorsvik, 2016; Schein & Schein, 2017) at kultur er en effekt som oppstår ved en samling av mennesker, av deres holdninger, normer, verdier m.m. På samme måte som en kultur er med på å forme et individ, er også et individ med på å forme en kultur. Ved en samling av mennesker, har vi ikke bare et kulturaspekt, men det oppstår også ofte et fellesskap. Et hvert individ utvise lojalitet og solidaritet mot fellesskapet for at et felleskap skal vedvare og bestå (Jacobsen & Thorsvik, 2016). Noen kulturer bærer preg av å være mer individualistiske, der individets egne behov settes i fokus. Andre kulturer, som for eksempel en virksomhets overordnede kultur vil kunne være mer orientert mot fellesskapets behov. Et eksempel på en kultur som ivaretar fellesskapets behov vil kunne være en kultur der individer står frem når de har vært årsaken til at det har oppstått en uønsket hendelse. Og på denne måten bidrar individer til at fellesskapet og organisasjonen kan lære av hendelser, og forhåpentlig bidra til at man unngår at lignende hendelser oppstår i fremtiden. Slik kan man belyse nødvendigheten med et godt fellesskap innen en digital sikkerhetskultur (Bergsjø et al., 2020).

I en organisatorisk sammenheng vil det være nødvendig å kontrollere, regulere og styre et fellesskap. ***Styring og kontroll***; på samme måte som ledelsen har ansvar for risikoene og

annet sikkerhetsarbeid i en organisasjon, har den ansvar for styring og kontroll av digital sikkerhet. Det at vi lever i et samfunn som er veldig opptatt av personvern, frihet og åpenhet, gjøre at styring og kontroll kan oppfattes som noe negativt og belastende for mange. For hvor mye skal en overvåke og hvor mye skal en kontrollere? Hvor går grensen for det som er akseptabelt? Dette kan være ett sensitivt område, men ledelsen må legge føringer for hva som er akseptabelt i virksomheten. Dette kan gjøres ved å etablere prosesser, regler, retningslinjer som er forståelige og mulige for menneskene i organisasjonen å følge (Bergsjø et al., 2020; Digitaliseringsdirektoratet, 2021c).

Som en kontrast til styring og kontroll må man ta ***tillit*s** aspekt inn i vurderingen. Ved styring og kontroll er spørsmålet ofte hvor mye kontroll, hvor mye styring, og hvor detaljert man skal være. Premissene for tillit er sårbare, da det krever mye arbeid å bygge opp tillit, men den kan raskt brytes ned. På samme måte som tillit er en hjørnesten i ett fungerende demokrati, er det en tilsvarende hjørnesten i mange virksomheter og ledere.

Hjemme- og hybridkontor vil potensielt kreve mye av en leder. Det vil være nødvendig med en høyere grad av tillit fra ledere da de må forvente, stole på og ha tillit til at medarbeidere utfører sine arbeidsoppgaver. Dette er noe som belyses nærmere i delen om ledelsesteorien senere i dette kapitlet med tillitsbasert ledelse. Bergsjø et. al (2020) påpeker at tillit i sammenheng med digital sikkerhetskultur også må kobles mot digitalisering. De ansatte må ha tillit til at systemene og tjenestene de bruker har høy grad av sikkerhet, og ikke brukes til unødvendig kontroll og styring.

Neste moment er ***Risiko***. Risiko er i kapittel 2 knyttet til beslutninger, men en beslutning trenger ikke være relatert til avgjørelser tatt av ledelsen. En beslutning være en avgjørelse en ansatt tar om å utføre en handling i den digital sfære, eksempelvis å klikke på en lenke, eller installere programvare som ikke er godkjent. Alle disse handlingene kan være medføre risiko. Det oppstår med andre ord en sammenheng mellom den ansattes handlinger ut ifra deres kompetanse og evne til å forstå risiko. Skal man være i stand til å identifisere risiko, så må man besitte den nødvendige kunnskapen og kompetansen til å gjenkjenne risiko. En studie gjennomført av Kreuter og Strecher (1995) fant at mennesker som mener de besitter mye kompetanse og ferdigheter utviser større risikoadferd enn de som vurderer sin kompetanse som . Man ser med andre ord en tendens til at mennesker med egen oppfattelse av å inneha høy kompetanse innen digital sikkerhet, i dette tilfelle, står i fare for å overvurdere sine egne

evner og dermed være tilbøyelig for å ta mer eller flere unødvendige risikoer (Bergsjø et al., 2020).

En annen faktor som er knyttet til risikooppfattelse fremheves som et punkt i en undersøkelse gjennomført av Parsons et al. (Parsons, McCormac, Butavicius & Ferguson, 2010), hvor det ble avdekket at enkelte individer har urealistiske, og er overkant optimistiske, i møte med risikoer, da de oppfatter at de har bedre kontroll enn hva de i realiteten har. Det kommer også frem i denne studien (Parsons et al., 2010) at flere mener de har mer og bedre kontroll over egen datamaskin, da denne er deres egen besittelse og dermed oppleves som under kontroll, og at det med dette oppstår situasjoner hvor digitale trusler kan oppleves som mindre truende enn hva de i realiteten er. Ifølge Bergsjø et. al (2020) kan dette medføre at enkelte individer utvikler en digital adferd som kan utgjøre en større risiko ifm. fordi de overvurderer egne evner og kompetanse. Vi kan se for oss at personer som anser at de har god kompetanse og gode ferdigheter vil ta høyere risiko på hjemmekontoret enn andre. Dette kan bli aktuelt med tanke at høykompetansebedrifter med høyt utdannede, kompetente mennesker derfor har en iboende større digital risiko enn dem med mellom-kompetente mennesker. Sjöberg & Drottz-Sjöberg (2008) så i sin studie «risk perception by politicians and the public» at oppfattelsen av risiko blir en personlig ting og vil variere fra individ til individ. Individer lytter til sin egen overbevisning, avhengig av deres utgangspunkt, grunnlag eller kompetanse og ikke nødvendigvis utfra hva eksperter eller myndighetsrepresentanter mener. Mest sannsynlig vil de i større grad lytte til venner og familie, ifølge forfatterne.

NorSIS (Norsk senter for informasjonssikring, 2020) har valgt å se på digitalisering i et lengre perspektiv enn bare digitaliseringen utfra et samfunnsmessig perspektiv. Iht. NorSIS er det viktig at individer har en ***optimisme for teknologi og digitalisering*** for å kunne lykkes både med digitalisering, men også for å skape god digital sikkerhetskultur. Bergsjø et al. (Bergsjø et al., 2020, s. 40) påpeker «*... Din holdning til digitalisering påvirker måten du forholder deg til teknologi på, fordi en trygg digital innbygger presumptivt er en forutsetning den nasjonale digitaliseringen».* De beskriver en situasjon hvor det enkelte individet eller samfunnet som helhet er villige til å la digitaliseringen fortsette, og de blir dermed en faktor som har innflytelse potensielt både i negativ eller positiv favør (Bergsjø et al., 2020).

Optimisme for teknologi og digitalisering er tett knyttet til individets ***kompetanse*** på det digitale området. Det paradoksale er at selv med den hastigheten digitaliseringen gjennomføres, så gis det ikke nødvendigvis opplæring i dette (Bergsjø et al., 2020). Den

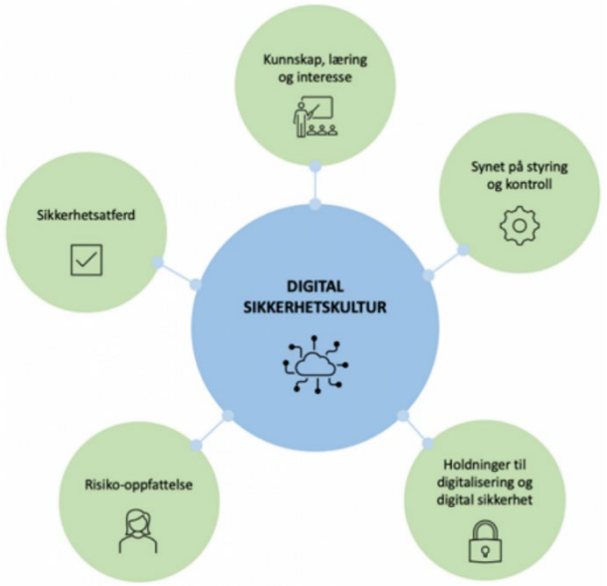
enkelte må selv ta ansvar med å søke opp informasjonen og sette seg inn i anbefalinger for hvordan bruke tjenester på en trygg og sikker måte. De fleste arbeidsgivere gir til en viss grad opplæring i digitale systemer, men oftest er det en forutsetning at ansatte behersker og allerede har et visst nivå på sin digitale kompetanse. Virksomheter som ønsker å jobbe målrettet med digital sikkerhetskultur bør investere både i kartlegging av nivået på kompetansen internt, men også planlegging av videre oppfølging for å gi medarbeidere den kompetansen som er nødvendig for å jobbe sikkert. Kun med den nødvendige kompetansen kan individet gjøres i stand til å identifisere mulige risikoer og ta gode beslutninger i det digitale rommet.

Interesse for teknologi og IT henger veldig tett opp mot flere av de forrige punktene, spesielt kompetanse, optimisme for teknologi og digitalisering. NorSIS (2020) er tydelig på at dette er en av nøkkelfaktorene for digital sikkerhetskultur, da dette er med på å underbygge ønsket og interessen for å kunne delta trygt i et digital samfunn. Som Bergsjø et al. (2020) også påpeker, så er interesse en hjørnestein i læring. Med interesse kommer også bevissthet, nysgjerrighet og villigheten til å bruke tid på å lære og tid på å ta riktige beslutninger. For en virksomhet er dette en viktig faktor å få innsikt i da dette kan være avgjørende for valg av metodikken man legger til grunn for å motivere og lære opp sine ansatte.

Til slutt i nevnes ***adferdsmønstre***. I mange virksomheter finnes det konkrete adferdsmønstre man ønsker å se i sammenheng med en digital sikkerhetskultur. Dette kan for eksempel være at de ansatte har en adferd hvor de alltid låser sin PC når de forlater den, og hvis det ikke gjøres, så finnes det en kultur for at medarbeidere gir tilbakemelding om at dette er noe en måte gjøre. Dette er eksempel på en type adferd som er ønsket. Problemstillingen er at adferdsmønstre og hva som er en *beste praksis* i en slik sammenheng kan endre seg over tid. Det som var best i går, er gjerne ikke best i morgen. Et godt eksempel på dette er anbefalinger om komplekse passord. Tidligere var anbefalingen av passordene skulle inneholde små og store bokstaver, spesial tegn og minst tre tall, samt at passordet skulle byttes minst hver 90 dager. Dette er en anbefaling som en nå har valgt å gå bort fra. Nasjonal sikkerhetsmyndighet (2019) anbefaler nå i stedet at en bruker passordfraser. Dette vil si en lengre setning, gjerne på dialekt, med mellomrom og med skrivefeil. De anbefaler også at en går bort fra å bytte passord ofte, da det viser seg at dette på sikt vil forringe sikkerheten. En har sett at ansatte adoptere ett adferdsmønstre som er med på forrige sikkerheten, fordi de når de må bytte passord ofte, lager for lette passord. Bergsjø et al. (2020) og NorSIS (2019) anbefaler at en studerer adferdsmønstre som en del av digital sikkerhetskultur, slik at en kan lære mer om

hvordan bestemte grupper og individer faktisk handler i gitte og ulike situasjoner. På den måten kan bruke den informasjonen til å bedre legge til rette for virksomme regler, prosesser og råd.

Digitaliseringsdirektoratet (2021c) har visualisert sammenhengen mellom disse åtte punktene, slik at en bedre kan se hvordan de henger sammen. En bør ikke se på disse punktene alene, en må se på helheten for at en kan oppnå best mulig langsiktig resultat.



Figur 3: Sammenhengen Digital sikkerhetskultur. (Digitaliseringsdirektoratet, 2021c)

Som det kommer frem fra figuren, så er flere av punktene konsolidert og satt sammen til ett eller flere punkter. Bergsjø et al. (2020) er tydelig på at disse åtte punktene er avgjørende, og gir en avsluttende oppsummering og påfølgende anbefalinger for arbeid med digital sikkerhetskultur (Bergsjø et al., 2020, s. 45):

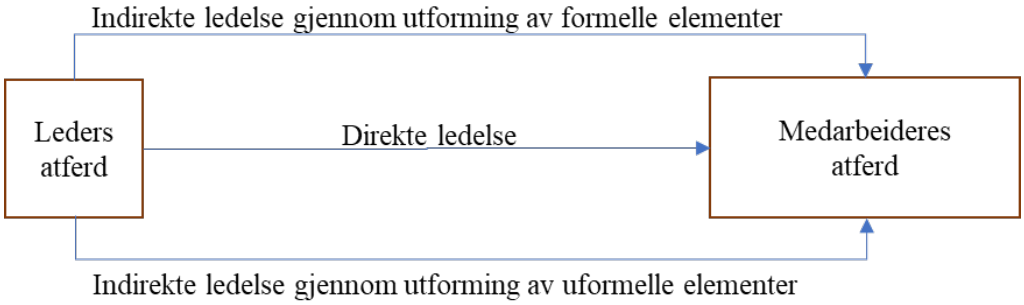
- *Sørg for at ledelsen har et tydelig mål for digital sikkerhet, og at dette er kommunisert til alle ansatte.*
- *Å utvikle eller påvirke kulturen i virksomheten er en kontinuerlig prosess som krever en helhetlig tankegang og innsats på mange områder samtidig. Ledere bør vurdere om virksomheten har en digital sikkerhetskultur som faktisk bidrar til at virksomheten når sine mål på en sikker måte.*
- *Sørg for at alle ansatte har kompetanse til å gjøre det ledelsen forventer av dem innen digital sikkerhet. De ansatte må gis nødvendig kunnskap, og denne må holdes ved like. Opplæring og bevisstgjøring setter de ansatte i stand til å ta sikre valg på arbeidsplassen.*

- *Tenk på at det er mennesker som skal skape kulturen og bli påvirket av den, og at sikkerhet derfor må være menneskelig mulig å gjennomføre.*

Disse anbefalingene, samt de overordene åtte punktene til NorSIS, sammenfaller tett med både Reason (1997) og Westrum (Westrum, 2014; Westrum & Adamski, 2009) og en kan tydelig se viktigheten av å se disse perspektivene i en større organisatorisk kontekst og sammenheng i arbeidet med digital sikkerhetskultur.

3.6. Ledelse

Ledelse kan utøves *indirekte* og *direkte* for å påvirke den ansattes organisasjonsadferd. Det er dette adferdsmønsteret som er viktig å jobbe mot og som går igjen i punkt åtte i digital sikkerhetskultur.



Figur 4: Direkte ledelse og to former for indirekte ledelse (Reprodusert fra Jacobsen & Thorsvik, 2016, s. 417).

Direkte ledelse omhandler alle former for samhandling og kommunikasjon mellom ledere og underordnede. Typiske eksempler på dette vil kunne være møter, beskjeder eller andre former for direkte handlinger. *Indirekte ledelse* er når lederen forsøker å påvirke/lede medarbeideres atferd uten å ha direkte samhandling med dem. Indirekte ledelse har også aspekter av formelle og uformelle elementer (som illustrert i figur 4). Disse aspektene indikerer rammene for hvordan indirekte ledelse gjennomføres. Formelle elementer kan være mål og strategier, formelle programmer for rekruttering, opplæring og sosialisering. Uformelle elementer på sin side retter seg mot å påvirke utvikling av kultur, ved for eksempel å styrke verdier og normer blant de ansatte. (Jacobsen & Thorsvik, 2016). Ledelsesteorier og metodikker spiller en stor rolle innen utforming og styring av digital sikkerhetskultur og er ytterst nødvendig for å kunne lykkes med arbeid relatert til dette (Bergsjø et al., 2020).

Ledelse på hjemmekontor

Hybride kontorløsninger kan komme til å sette ledelsesteorier og -perspektiver under press, og introdusere nye elementer for hvordan ledelse kan og bør gjennomføres. En studie

gjennomført av NBER (National Bureau of Economic Reshearch) i USA viser at det er stor spredning i hvordan medarbeidere ønsker dette skal skje. Som eksempel sier 13,7% prosent av total 25002 intervjuede er sterkt bekymret og sier de kommer til å fortsette med sosial distansering. Av disse sier 84% at deres bekymring er knyttet til manglende villighet til å ta vaksiner eller dens effektivitet (NBER, 2021). Ser vi til Norge, er det gjennomført studier (Holm Ingelsrud & Hoff Bernstrøm, 2021) som viser tilsvarende trender. Ett stort antall norske medarbeidere ønsker i ulike grad å fortsette med hjemmekontor på fast basis, altså en form for hybridkontor.

Hvilke elementer vil en leder måtte beherske for å best kunne lede sine ansatte i fremtiden? På samme måte som digital sikkerhetskultur angir tillit som en avgjørende faktor, påpeker både Reason (1997) og Westrum (2009) mye av det samme ved at kontroll og styring i stor grad må gjøres basert på tillit. Dette er overførbart til ledelse i en hybrid kontekst.

3.6.1. Tillit og tillitsbasert ledelse

Kuvaas (2017a, 2017b) argumenterer for en tillitsbasert ledelse. Han deler menneskers motivasjon inn i to hovedkategorier. Det er ytre og indre motivasjon. Når flere og flere velger å jobbe utenfor kontoret vil den indre motivasjonen bli enda viktigere enn tidligere, altså de ansattes egen følelse av tilfredshet, interesse, mening og glede knyttet til oppgavene de løser. I følge Kuvaas (2017a, 2017b) er det hensiktsmessig å ta i bruk en lederstil som skaper strukturer som gir insentiver og aktiverer ansattes indre motivasjon. Med andre ord, gi folk tillit og spill på de indre drivkrefter hos folk, enten det nå er å opptre sikkert, være produktive, eller å kunne utvikle egen kompetanse. Gjensidig tillit mellom leder og medarbeider er helt nødvendig for å kunne utøve tillitsbasert ledelse.

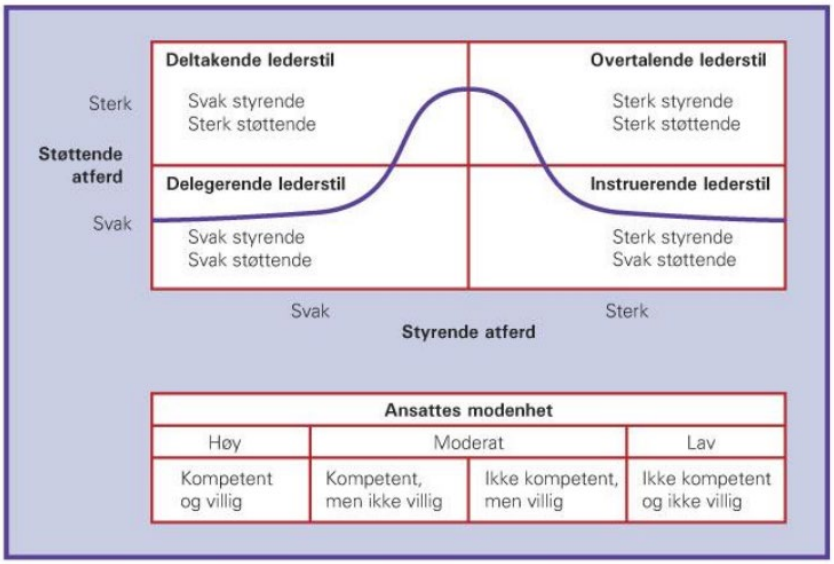
Som en følge av pandemien og innføring av hjemmekontor for mange yrkesgrupper, har Direktoratet for forvaltning og økonomistyring (DFØ) utarbeidet en veileder med anbefalinger for hvordan man kan lede medarbeidere som sitter på hjemmekontor. Disse punktene er direkte overførbare til en hybridkontorkontekst og denne oppgavens problemstilling. DFØ påpeker fem punkter en leder må være spesielt bevisst på. To av disse er basert på Kuvaas modell for tillitsbasert ledelse; å utøve kontroll ved å vise tillit, og å sette medarbeidere i stand til å lede seg selv. Både Kuvaas og DFØ (Direktoratet for forvaltning og økonomistrying, 2021; Kuvaas, 2017a, 2017b) er tydelige på at medarbeidere som opplever å få tillit ønsker å yte mer tilbake.

3.6.2. Situasjonsbasert ledelse

Situasjonsbasert ledelse ble utarbeidet av Blanchard og Hersey på 60- og 70-tallet. Denne teorien bygger på at ledelse gjennomføres i ulikes situasjoner med ulike utgangspunkt basert på både oppgavens art, men også medarbeidernes egenskaper/kompetanse og relasjon til lederen. Den grunnleggende antagelsen i denne teorien er at ulike situasjon krever forskjellige lederstiler for at resultatet skal bli som ønsket. (Jacobsen & Thorsvik, 2016; Kaufmann & Kaufmann, 2015; Store Norske leksikon, 2021b). Lederstilen til lederen og kompetansen til den ansatte er sentrale elementer her.

Ifølge Hersey og Blanchard (Jacobsen & Thorsvik, 2016; Kaufmann & Kaufmann, 2015) så kan en medarbeideres kompetanse deles inn i fire forskjellige kategorier fra lav til høy. Det er gradert ut ifra hvilken kompetanse vedkommende har, men tar også med deres villighet til å løse arbeidsoppgavene.

Hersey og blanchard påpeker at medarbeiderens kompetanse må være med på å bestemme hvilken form for ledelse som er mest hensiktsmessig i den enkelte situasjonen. I hovedsak deles lederstilene man kan velge mellom i støttende og styrende. Hersey og Blanchards teori kan illustreres som vist i figur 6 under:



Figur 5: Situasjonsbestemt ledelse iht. Hersey og Blanchard – figur kilde (Jacobsen & Thorsvik, 2016, s. 438)

Som det påpekes av Kaufmann & Kaufmann (2015) så ligger utfordringen i denne lederstilen i evnen til å kunne tilpasse sin lederstil til de betingelsene som gjelder under de til enhver tid rådende forholdene. Pandemien, hjemmekontor og hybridkontor er forskjellige betingelser ledelse da må tilpasses til. Et annet eksempel som viser kravene til lederens

tilpasningsdyktighet og situasjonsforståelse er at en leder må kunne ta i bruk like mange lederstilen som han har ansatte fordi de ansatte besitter forskjellig motivasjon, kompetanse og behov.

Vi vet at mye endret seg da arbeidstagere over natten ble sendt på hjemmekontor på grunn av pandemien. Også mange aspekter som innvirker på digital sikkerhetskultur må håndteres annerledes når ansatte «jobber fra kjøkkenbenken». Vi har blant annet sett på ulike aspekter ved kompetanse og hvordan de som f.eks. tror de innehar den nødvendige kompetansen muligens utgjør den største sikkerhetstrusselen. Videre ser vi at indre motivasjon blir viktigere når sjefen ikke har like mye kontroll over hvordan ansatte utfører arbeidet. Vi har drøftet tillitsbasert ledelse, og vi har også drøftet ulike lederstiler.

4. Metode

Denne oppgaven ble skrevet mens det var fremdeles korona tiltak i Norge. Denne situasjonen var med på å definere hypotesen til oppgaven, men påvirket også valgene av metode som ligger til grunn for hvordan oppgaven til slutt ble utarbeidet.

4.1. Forskningsdesign

I utarbeidelsen av denne oppgaven, ligger det flere valg til grunn for hvordan den ble utviklet. Dette refereres til som valg av *forskningsdesign* eller også gjerne som det blir beskrevet av Grenness (2020) et *undersøkelsesopplegg*. Dette kan skape en enklere forståelse av hva dette innebærer, eller rette og slett hva som ligger til grunn for hvordan en undersøkelse er gjennomført. Gjerne beskrive det som «*opplegget en har valgt for å gjennomføre undersøkelsen.* For som Grenness (2020) skriver, *«det å gjennomføre en empirisk undersøkelse har noen ganger blitt sammenliknet med å vandre nedover en vei hvor du stadig kommer til nye veikryss der du må velge hvor du skal videre»*. Dette er en god beskrivelse for hvordan det opplevdes å skrive en oppgave rundt den valgte hypotesen.

Innen forskningsdesign sier Blaikie (Blaikie & Priest, 2019, s. 36) at det er viktig å presisere nærmere hvordan et prosjekt og problemstillingen vil bli studert. Her er det spesielt fire grunnleggende momenter som må vurderes og besvares:

- Hvilken forskningsstrategi vil bli brukt?
- Hvor kommer data fra?
- Hvordan vil data bli samlet inn og analysert?
- Når vil de ulike stegen bli gjennomført?

Om en klarer å finne en god besvarelse på forskningsspørsmålene på en tilfredsstillende måte, dannes det et betydelig grunnlag, slik at det skapes en mulighet for faglig evaluering av forskningsdesign uten at mulighetene for å nå et vellykket resultat svekkes (Blaikie, 2010, s. 16).

Metoden som er valgt for gjennomføring av denne oppgaven er av kvalitativ karakter og et eksplorativt design. En kvantitativ metodikk ville ikke vært tilstrekke og dermed er heller ikke oppgaven av eksplorative utgangspunkt. Siden oppgaven ikke tar for seg ett område uten at det finnes forkunnskaper eller tidligere forskning. Thagaard (2018, s. 15) henviser til Denzin og Lincoln (2018) og fremhever at begrepet kvalitativt innebærer å fremheve

prosesser og mening som ikke kan måles i kvantitet eller frekvens. Ser en til problemstillingen i oppgaven, er dette med å understøtte at en kvalitativ metodikk er den mest hensiktsmessige for å kunne få besvart oppgaven. Thagaard (2018, s. 15) skaper en videre validitet for dette, med å henvis til Repstad (2007) som hevder at *«ordet kvalitativ viser til kvalitetene, det vil si til egenspaene eller karaktertrekkene ved de sosiale fenomener vi studerer».*

Selv om en kvalitativ metodikk ble valgt for denne oppgaven, er det en kjensgjerning at det finnes alternative metodikker tilgjengelig og som kunne vært relevante for oppgaven. Men gitt oppgavens størrelse, omfavn og struktur falt valget på en kvalitativ tilnærming.

Denne oppgaven har som målsetning å se nærmere på om det er elementer ved digital sikkerhetskultur som utpreger seg som viktig å prioritere, sett utfra en situasjon hvor en har ansatte som skal ledes og gis muligheten til å jobbe fra et hybridkontor perspektiv.

4.2. Datakilder og datainnsamling

Denne oppgaven benytter seg av informasjon hentet fra ett større antall datakilder for å kunne besvare problemstillingen. For å kunne bedre klassifisere de forskjellige datakildene som denne informasjonen er hentet fra, så defineres disse som primære, sekundære og tertiære kilder. Disse beskrives av Blaikie (Blaikie & Priest, 2019) på følgende måte:

- Primær - Dette er data som er innsamlet forskerne direkte selv.
- Sekundær - Data som har blitt innsamlet av noen andre og brukt i ubehandlet form. Dette blir ofte henvist til som rådata.
- Teritær - Data som er innsamlet av en tredjepart, analysert og publisert.

Primærkilder som ligger til grunn for oppgaven er dokumentanalyser, litteraturstudier og Semistrukturert intervjuer. Sekundær samt tertiære kilder som er brukt i vesentlig grad spørreundersøkelser gjennomført av tredjepart, som for eksempel (listen er ikke uttømmende):

- «Risiko» Årlig risiko rapport fra Nasjonal sikkerhetsmyndighet.
- «Nordmenn og digital sikkerhetskultur» Årlig rapport og survey gjennomført av Norsk senter for informasjonssikring (NorSIS)
- «IT i Praksis 2020» gjennomført av Ramboll

- «IT i Praksis 2020 Dashboard» Visuell fremstilling av data og indikatorsett ferdig analysert av Ramboll.
- «Mørketallsundersøkelsen» Årlig rapport fra Næringslivets sikkerhetsråd.
- «Koronasvindel i næringslivet». Spørreundersøkelse gjennomført for Næringslivets sikkerhetsråd
- «Hjemmekontor: Utbredelse og sentrale kjennetegn våren 2021». Studie gjennomført av OsloMET og arbeidsforskningsinstitutet AFI.

Som Blaikie (Blaikie & Priest, 2019) påpeker i så er det viktig å være observant på hvordan grunnlagsdata brukes, da bruk av sekundær og tertiær data så vil en kunne befinne seg i situasjon der en er for langt unna innsamlingen av grunnlagsdataen, at det vil være problematisk å vurdere kvalitet, validitet og relabilitet. Dette var elementer som løpende ble vurdert ved utarbeidelsen av denne oppgaven, spesielt utfra kildens troverdighet og rolle innen det aktuelle fagfeltet. Kildens troverdighet var ikke det eneste som ble vurdert, som en del av oppgaven og vurdering av kildene, så ble det bedt om innsyn i rådata tilhørende samtlige av rapportene nevne ovenfor. Det var kun rapporten tilhørende NSM og deres *Risiko* rapport, det ikke ble gitt innsyn i rådata på. Dette da disse kunne inneholde sensitiv informasjon, da denne rapporten dekker stort område fra et nasjonalt sikkerhetsståsted og som også er utenfor omfavnet til denne oppgaven. Dette for å videre gjøre en vurdere utfra validiteten og understøtte reliabiliteten til denne oppgaven.

4.3. Intervju og gjennomføringen av intervjuene

Intervjuene er gjennomført med en semistrukturert metodikk (Thagaard, 2018). Denne typen intervjustruktur er ifølge Thagaard (2018) en teknikk som oftest benyttes i kvalitative studier, og som oftest henvises til som kvalitative intervjuer (Thagaard, 2018). Thagaard omtaler at en må ha en viss struktur på intervjuene, da både generelle tema skal diskuteres, men også basert på en intervjuguide, slik at besvarelsen er sammenlignbar mellom informantene. Ved å ha en semistrukturert tilnærming ble det mulig å justere intervjuet i løpet av intervjusamtalen. Dette gir mulighet til å gå dypere i enkelte tema eller utsagn som blir gitt, men samtidig sørge for at de temaene som er viktig for problemstillingen blir belyst.

Valg av informanter

Valget av informanter er ett viktig moment i en kvalitativ studie. Dette spesielt siden en kvalitativ studie ofte har et begrenset antall personer eller enheter som studeres, kontra en

kvantitativ studie. Utvalget må være hensiktsmessig, slik at problemstillingen kan bli belyst med validitet og reliabilitet. Dette er en fremgangsmåte som defineres som en *strategisk utvelging (*Thagaard, 2018*)*. En velger med andre ord personer eller enheter som har de kvalifikasjonene eller egenskapene som er strategiske iht. problemstillingen (Thagaard, 2018).

Med utgangspunkt i oppgavens hypotese ble det kontakt et større utvalg av kandidater som ble ansett som relevante for oppgaven. En erfaring som ble gjort i denne tidlige fasen av prosessen, var at enkelte informanter ikke ønsket å delta, da de ikke oppfattet problemstillingen som relevant og at fra deres ståsted ikke var nødvendig å innføre andre/nye tiltak som følge av hybridkontoret. Dette gjorde det nødvendig å tilpasse utvelgelsen av kandidatene gjennom utarbeidelsen av oppgaven.

En annen erfaring som også ble gjort, var nødvendighet av å supplere med ytterligere kandidater etter som intervjuene ble gjennomført. Her henvis Thagaard (2018) til Mason (2018), som kaller dette en organisk praksis. Etter som intervjuene ble gjennomført, ble det tydelig at informasjonen informantene tilførte var i stor grad homogen og det var lite forskjell i dette. Basert på dette, ble det innhentet ytterligere informanter, men av en annen bakgrunn enn øvrige informanter. Dette var informanter med HR, HMS, HSEQ bakgrunn, og kunne belyse problemstillingen fra et annet ståsted. Disse bidro i stor grad til å validere problemstillingen ytterligere, og reliabiliteten ble understøttet med å se til rådata og andre datakilder som beskrevet i 4.2.

Organisasjonene som informantene representerer, sprer seg fra mindre lokale bedrifter til store nasjonale virksomheter. Hovedvekten ligger på virksomheter som ble sterkt påvirket med hjemsendelse og relevant for problemstillingen. I denne oppgaven utgjør dette i hovedsak blant annet teknologibedrifter innen kraft, telekom, bank og finans og annen konsulent virksomhet.

Informantens kode i oppgaven	Stilling	Ansvar / Rolle	Virksomheten
A1	CISO	Overordnet ansvar for informasjon- og cybersikkerheten i virksomheten. Både teknisk og styrende dokumentasjon iht. sikkerhetsledelse og internkontroll.	Stor virksomhet innen forsikringsbransjen
B1	Sjef for strategisk sikkerhetsledelse	Tilsvarende rolle og ansvar som A1.	Stor virksomhet innen støttetjenester og telekom
C1	Sikkerhetssjef	Ansvarlig for informasjons- og cybersikkerhet i virksomheten. Tilsvarende rolle som A1 og B1	Stor virksomhet innen telekom
D1	Director of HSEQ	Ansvarlig for styring av kvalitet, sikkerhet, ESG (Environmental, social and governance) og WHS (Workplace, Health and Safety)	Stor virksomhet innen konsulentbransjen
E1	Sikkerhetsleder	Leder for sikkerhet, her under regulatoriske krav, sertifiseringer (ISO), risk management og incident management.	Liten til mellom virksomhet innen programvare og utvikling.
F1	CISO	CISO (tilsvarende A-C) men bistår også virksomheten med salgsstøtte og ekstern rådgivning ifm. kunder av virksomheten.	Liten virksomhet innen sikkerhet og infrastruktur
G1	Direktør digitalisering og informasjonssikkerhet	Direktør med overordnet for flere forretningsenheter / avdelinger.	Stor virksomhet/avdeling innen kommunal sektor
I1	Senior Rådgiver HR og digitalisering	Informanten er senior rådgiver innen HR og digitaliserings tjenester. Samarbeider tett med flere små og mellom store virksomheter og representerer et større antall virksomheter.	Liten rådgivings virksomhet innen HR tjenester og digital transformasjon
J1	Manager People & Organisation	Leder HR avdeling for forretningsstøtte og eksekvering.	Stor virksomhet innen olje og gass sektoren.

Tabell 1: Liste over informanter og stillingsbeskrivelse

Intervjuguide

Intervjuetguiden tilsendt informantene i forkanten av intervjuene. Dette ville gi informantene mulighet til å være forberedt på hvilke spørsmål og tema som ville bli diskutert. For at disse spørsmålene skulle være av god nok kvalitet, til at informantene kunne gi gode og utfyllende svar, så ble det sett til veilederne utarbeidet av Digitaliserings direktoratet for gjennomføring av analyse vedrørende digital sikkerhetskultur (Digitaliseringsdirektoratet, 2021b). Den semi-strukturert metodikken som intervjuguiden bygger på, kan sammenlignes med «Tre-med-grener-modellen» som det henvises til av Thagaard (2018) og er utarbeidet av Rubin & Rubin (2012). Her diskuteres ett hovedtema (digital sikkerhetskultur), og hvor «grenene» representerer andre momenter som inngår i en digital sikkerhetskultur, som f.eks. risikoforståelse, kompetanse m.m. Dette er ifølge Thagaard (2018) en hensiktsmessig modell, når analysene av dataen skal sammenlignes rundt hva informantene har hatt av utsagn.

4.4. Validitet og relabilitet

For at resultatet av en studie skal ha troverdighet, er det viktig å kontinuerlig vurdere validiteten, relabiliteten og overførbarheten av den. Thagaard (2018) beskrives en anvendelse av disse definisjonene på følgende måte:

- Reliabilitet. Knyttes til spørsmålet om forskningen som er gjennomført har en viss pålitelighet.
- Validitet knyttes til forskningens gyldighet
- Overførbarhet kan vi knytte til generell vurderingen rundt om tolkninger gjort gjennom studien er representative også kan gjelde i andre sammenhenger.

For at det skulle være mulig å oppnå validitet ved gjennomføringen av denne oppgaven, ble ett bredt spekter av kilder valgt. Dette for å se om det kunne gjøres korrelasjoner mellom uttalelser fra informantene og om dette viser seg å stemme med annen forskning eller komparative studier innen dette området (Thagaard, 2018). Det er også viktig hvordan vi tolker de resultatene som er gjort i denne oppgaven og hvordan dette er med på å underbygge resultatets gyldighet. Som Thagaard (2018) påpeker, er dette et viktig spørsmål om vi f.eks. selv har en tilknytning til miljø en studerer eller om en er en utenforstående. Som en ansatte innen informasjon- og cybersikkerhet, besitter jeg en høy kunnskap om fagfeltet, og det var dermed et viktig moment at disse studiene ble gjennomført uten at dette skulle bidra til å påvirke resultatet eller funnen gjort. Det ble derfor ikke gjennomført intervjuer med informanter i nær arbeidsrelasjoner, som igjen kunne påvirket innholdet og utfallet av intervjuene. Dette er viktig for å ivareta validiteten av oppgaven, men validiteten til en studie omhandler også om tolkninger gjort kan bekrefte tolkninger gjort i andre ulike studier, og om de kan bekrefte hverandre (Thagaard, 2018).

Reliabilitet er tett knyttet til validiteten og et viktig element. Thagaard (2018, s. 187) presiserer følgende*: «Vi knytter reliabilitet til spørsmål om en kritisk vurdering av prosjektet gir inntrykk av at forskningen er utført på en pålitelig og tillitvekkende måte.».* Det som også påpekes av Thagaard (2018) er at en forsker må argumentere for reliabiliteten blant annet ved å redegjøre for hvordan informasjonen har blitt utviklet gjennom utarbeidelsen av oppgaven. Dette har jeg som student vært bevisst, og vært tydelig i hva som er informantenes påstander, hva som er sekundære kilder og hvilken rolle forfatter eller mandat som ligger til grunn for sekundær kildene. Dette for å være med å styrke reliabiliteten til oppgaven og dens funn. Som Silverman (2014, ved Thagaard 2018, s.188) argumenterer for, så kan en styrke reliabiliteten ved å gjøre forskningsprosessen gjennomsiktig. Som beskrevet i 4.2, samt i referanselisten, så gis det en fullstendig oversikt av alle kilder og hvordan disse er brukt i oppgaven. Slik at en utenforstående kan vurdere både forskningsprosess og metode trinn for trinn (Thagaard, 2018, s. 188). En slik transparens på hvilke kilder som brukes, kildenes

troverdighet og kvalitet vil på samme måte kunne bidra til å understøtte reliabiliteten til oppgaven (Thagaard, 2018).

4.5. Etiske perspektiver

Denne oppgaven og dens hypotese ser på en problemstilling som i all hovedsak er fra en arbeidsgiver perspektiv, og det er herfra informantene er samlet. Denne oppgaven har ikke gjennomført større spørreundersøkelser for å innhente større kvantitative data, men som beskrevet i 4.2, er det blitt brukt sekundære og tertiære kilder fra store spørreundersøkelser gjennomført av større nasjonale aktører.

Selv om jeg ikke på noe tidspunkt behandlet sensitive personopplysning, så var jeg i besittelse av informasjon som ifølge NSD (Norsk senter for forskningsdata, 2021) er personlige opplysninger som ville gjøre det mulig å identifiseres identiteten til informantene til denne oppgaven. Denne oppgaven publiserer ikke noe eller noen datakilder som vil gjøre det mulig for en tredjepart å spore hvem informantene eller deres virksomheter måtte være. Dette er en viktig del av prosessen med utarbeidelsen av denne oppgaven og viktig for meg i rollen som forfatter av oppgaven. For å bevare anonymiteten til informantene og deres virksomheter, ble det iverksatt flere tiltak.

- Ingen opptak ble gjort digitalt, og ble gjort med analog båndopptaker på ekstern enhet. Dette for å sikre at data ikke ble overført digital eller lagret digitalt.
- Opptaket ble **kun** bruk til transkripsjon av intervjuet, for å best mulig sikre korrekt dokumentasjon av utsagn gitt av informanten.
- Referat ble oversendt informant, slik at informanten kunne tilføye eller gjøre andre endringer.
- Når informanten hadde godkjent intervjuet, så ble opptaket slettet.

Dette for å på best mulig måte ivareta informants rettigheter og lovnader om anonymitet. Disse tiltakene ble gjort for å være iht. til instruks gitt av NSD, men også iht. til de forskningsetiske retningslinjene som publisert av De nasjonale forskningsetiske komiteene (2021). Informantene har rett til å trekke seg fra oppgaven om dette var ønsket. Informantene ble informert om denne muligheten, samtidig som det ble gitt en gjennomgang av omfang, oppgavens intensjon og hensikt. Siden denne oppgaven ble gjennomført mens det fremdeles var korona tiltak i Norge, ble de fleste intervjuene gjort digitalt. I forkant av intervjuene ble informantene tilsendt intervjuguiden og samtykke skjema. Da intervjuene var digitale, ble

enten samtykke mottatt digital med samtykke, eller muntlig samtykke som en del av intervjuet. Av andre tekniske tiltak, ble koblingsnøkler mellom datasett oppbevart på separate steder og sikret med kryptering.

5. Empiri og Funn

Dette kapitelet er strukturert og sortert etter forskningsspørsmålene og iht. informantintervjuene og dokumentanalysene. Kapitel 5.1 tar for seg de sikkerhetsutfordringer virksomheter i dag opplever som en følge av hybride kontorløsninger. Søkelyset er ikke bare på hybridperspektivet, men også generelt knyttet til hjemmekontor, samt sikkerhetsutfordringer som har oppstått som en følge av koronapandemien og den påfølgende nedstengningen. Kapitel 5.2 dreier seg om forholdet mellom de utfordringene som er avdekket i kap.5.1, og hvordan ansattes holdninger, adferd, kunnskap og kompetanse spiller en rolle for digital sikkerhetskultur. De funn som presenteres i kommende kapitel er oppsummert i tabell 4 og 5 på henholdsvis side 64 og 65.

5.1. Hovedfunn Forskningsspørsmål 1

«Hvilke digitale sikkerhetsutfordringer opplever/opplevde virksomheter som en følge av nedstengningen grunnet koronatiltakene og hybride kontorløsninger?»

Dette forskningsspørsmålet skal hvilke digitale sikkerhetsutfordringer virksomheter opplever som en følge av økt bruk av hjemme- og hybridkontor. Det gis ingen konklusjon, og informantene har forskjellige svar på hvordan de oppfatter hjemme- og hybridkontoret som en utfordring. Informantene vekleggerbekymringer rundt kulturaspekter og arbeidsprosesser, mer enn at selve hjemme- og hybridkontoret medfører en teknisk og digital trussel i seg selv. Som et gjentagende moment vurderes det dit hen at hvis den ansatte bruker en eller fem dager i uken hjemme, er utfordringene fra et teknisk ståsted de samme, og det dermed ikke er noen forskjell i hjemme- eller hybridkontoret. Utfordringene som trekkes frem som viktigst ligger i hovedsak innen områder som omfattes av adferd, holdninger og kompetanse hos ansatte. Dette er funn både hos informanter med teknisk bakgrunn, så vel som informanter fra HR- og HMS-perspektivet. De forteller også om en konkret bekymring knyttet til psykososiale aspekter ved utvidet bruk av hjemmekontor, og hvordan dette kan påvirke organisasjons- og sikkerhetskultur i negativ retning.

NSM, PST og andre myndigheter i Norge er imidlertid tydelige på at det er en økning i trusler ikke bare Norge som nasjon, men også virksomheter i Norge. Dette er ikke nødvendigvis som en direkte følge av hjemme- og hybridkontoret, men også som en følge av digitalisering og andre påfølgende endringer som f.eks. endringer i arbeidsprosesser m.m. Nedstengningen og

koronapandemien i seg selv har bidratt til å endre trusselbildet, mer enn hjemme eller hybridkontoret i seg selv.

De påfølgende delkapitellene vil i nærmere detaljer presentere disse funnene.

5.1.1. Overordnet trusselbilde

NSM og PST utgir årlige trusselvurderinger. PST har i en årrekke uttrykt en generell bekymring for vedvarende trusler og digitale angrep som kan påvirke nasjonens sikkerhet. Disse truslene i det digital rommet har fått større og større plass og vektlegges tyngre i PST sine rapporter nå enn tidligere. I PST (2021) sin trusselvurderingsrapport fra 2021, er PST tydelig på at arbeidet med å identifisere, avdekke og forbygge trusler i det digital rommet, nå griper inn i de fleste av PST sine oppgaver. Går vi tilbake til rapporten fra 2015 (2015), vektlegges den digitale sårbarheten vesentlig. PST (2021) er tydelig på at truslene i det digital rommet vil fortsette gjennom 2021 og ut i 2022 i uforminsket styrke, både i form av politisk motivert vold, ekstreme grupperinger, men også andre former for kriminalitet. Som det påpekes i samme rapport (Politiets sikkerhetstjeneste, 2021) , er trusselbildet noe mer usikkert på flere områder grunnet usikkerheten ved de langsiktige konsekvensene av koronapandemien, noe som gjør bildet mer komplisert og utydelig.

NSM uttalte i sin rapport helhetlig digital risikobilde 2020 (2020) at selv om koronapandemien har ført til flere ekstraordinære sitasjoner, også i det digitale rommet, så har pandemien ikke endret hovedlinjene i det digitale risikobildet for Norge. I helhetlige digitalt risikobilde for 2021 (Nasjonal sikkerhetsmyndighet, 2021a) gjentas mange av de samme påstandene som i rapporten for 2020, men NSM er tydeligere på at utstrakt brukt av hjemmekontorløsninger har skapt nye digitale sårbarheter. NSM gjentar (2021a) at denne utstrakte bruken og digitaliseringen har økt angrepsflaten, da mange av de midlertidige løsningene som ble introdusert, nå er kommet for å bli. Her referer NSM til dette «… som en ny normal hverdag». I en nyere rapport Risiko 2021 av NSM (2021b) påpekes der imot tre følgende endringer:

- Det digitale risikobildet for Norge er skjerpet
- Tydeligere risiko knyttet til sammensatte trusler
- Korona-pandemien har forsterket de eksisterende risikobildet.

Denne tydeliggjørelsen henger ifølge NSM nært sammen med, og reflekterer de endringene i sårbarhets- og trusselbildet samt utviklingen av nasjonale verdier. Dette har sammenheng

med økt digitalisering som en direkte effekt og behov grunnet pandemien og endringen i arbeidsmetodikker m.m. Digitaliseringen gjør at det oppstår tettere digitale verdikjeder, som igjen medfører en økning og et mer komplekst og skjerpet risikobilde ifølge NSM (2021). Flere aktører, her både nasjonale og internasjonale (FBI, 2021; Nasjonal sikkerhetsmyndighet, 2020, 2021b; United States. Cyberspace Solarium, 2020) påpeker hvordan den generelle digitaliseringen av samfunnet ikke bare bidrar til verdiskapning, velferd og trygghet, men også fører til en økt sårbarhets- og angrepsflate som trussel-aktører kan benytte seg av. NSM (2021) påpeker at «koronapandemien har gjort sårbarhetsbildet tydeligere med hensyn til norske virksomheters avhengigheter og leverandørkjeder».

Da ansatte ble sendt på hjemmekontor i mars 2020, måtte arbeidsgivere i utvidet grad tilby fjerntilgangsløsninger og for eksempel andre typer skytjenester. Dette er med på å endre og potensielt øke angrepsflaten, selv om denne endringen var nødvendig for å kunne ivareta produktiviteten gjennom nedstengningen (Nasjonal sikkerhetsmyndighet, 2021b). Nasjonalt cybersikkerhetssenter (NCSC) som er en del av NSM, observerte nemlig akkurat dette gjennom 2020 - hvordan avanserte aktører kartla og overvåket sårbarhet i fjernpåloggingssystemer, og som ble aktivt utnyttet ved senere anledninger gjennom angrep (Nasjonal sikkerhetsmyndighet, 2020).

Det er ikke bare endringen i tekniske løsninger som ble nødvendig på grunn av pandemien, men også en endring i samhandling når vi arbeider. Ifølge NSM (2021) gir dette større rom for sosial manipulasjon som forskjellige trusselaktører i stor grad har forsøkt å utnytte. Dette ser NSM (2021) og PST (2020) som en tydelig trend og det forventes å vedvare i uforminsket styrke. Dette er en endring fra tidlig pandemi, hvor fokus var spam / phising angrep av type «skattefradrag Korona» eller «Nye arbeidsinstrukser for hjemmekontor» (Andrade, Ortiz-Garcés & Cazares, 2020). Trend Micro (Andrade et al., 2020) så fra februar 2020 til mars 2020 en 220% økning i uønsket epost hvor trusselaktører brukte Korona som hovedfaktor i sitt forsøkt på utnyttelse.

Som et eksempel på hvilke trusler et hjemmenettverk kontinuerlig utsettes for i forskjellig grad, ble det satt opp en Honeypot (Deutsche Telekom, 2021) fra Deutsche Telekom. En honeypot, er i dette tilfellet en eller flere datamaskiner uten noen virkelig funksjon, annet enn å lokke til seg uønskede aktører, derav navnet. I en tidsperiode på 24 timer fra 21.10.2021 0700 til 22.11.2021 2021 0700, oppdaget dette systemet 49 311 forsøk på angrep eller annen type overvåkning/kartlegging.

Figur 6: Forsøk på angrep mot et hjemmekontor

Som en ser ovenfor i figur 6, kan en se at det er en vedvarende trussel som pågår mot «hjemmekontoret». Samme problemstilling tas også opp av NSM i Nasjonalt digitalt risikobilde (2021), hvor blant annet kompromitterte hjemmerutere brukes av trusselaktører som noder i videre angrep. Dette betyr at der arbeidsgiver tidligere hadde fullstendig kontroll på perimeter rundt infrastrukturen, vil hjemme- og hybridkontor bidra til å øke den potensielle angrepsflaten.

5.1.2. Sikkerhetsutfordringer og hendelser ved hjemme / hybrid kontoret

Gjennom informantintervjuene kom det frem flere funn knyttet til både digital og generelle sikkerhetsutfordringer som en følge av pandemien og bruken av hybrid/hjemmekontoret.

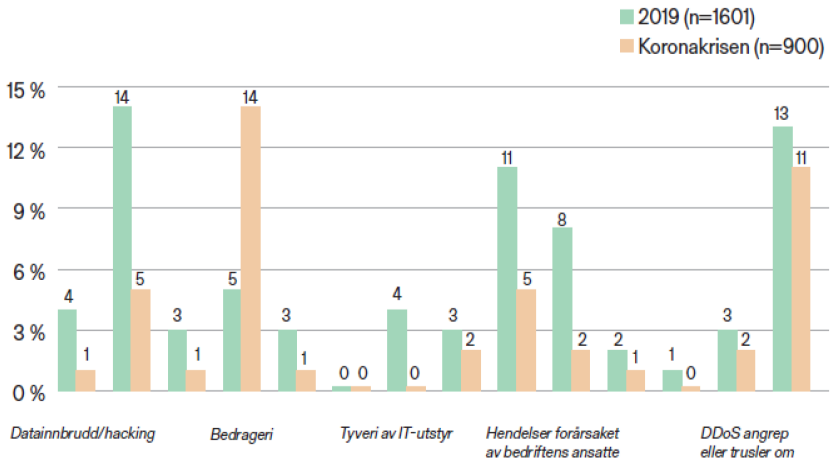
Ifølge flere av informantene har det ikke vært noen signifikant økning i antall tekniske hendelser som en følge av utvidet og/eller økt bruk av hjemme/hybridkontoret. Typen hendelser de ser en økning i, er ikke av teknisk art, men mer relatert til brudd på retningslinjer og prosedyrer. Dette er felles for flertallet av informantene og deres virksomheter.

På spørsmålet «*Har dere sett en økning i antall uønskede hendelser som en følge av økningen i bruken av hjemme/hybridkontor»* fordeler informanten i all hovedsak det samme. De fleste har ikke sett en vesentlig endring av uønskede hendelser fra ett digitalt eller teknisk perspektiv, men mer fra ett holdnings og adferds perspektiv hos den enkelte.

Informant	Kommentar
A1	«*det en ser nå - ikke i starten, men etter hvert er en økning i antall meldte policy brudd.»*
B1	*«… Ingen vesentlige økninger … Men det finnes andre «følge feil» på grunn av en slik utstrakt bruk av hjemme/hybridkontor. Dette har vært mer av fysisk og psykisk karakter»*
C1	«*Ikke i vesentlig grad. Vi så/ser en økning i spam o.l som blir stoppet av sentrale tjenester, men de fleste brudd er relatert til retningslinjer og arbeidsprosesser»*
D1	«*Nei, vi kan ikke se at dette (en økning). Det kan være mørketall basert på evt KPI som mangler, men vi har gjort flere øvelser for å identifisere uønskede hendelser relatert til et informasjonssikkerhets perspektiv»*
E1	«*Nei, vi har egentlig ikke registrert noen økning i antall uønskede hendelser som direkte følge av hjemme/hybridkontoret – Men vi ser et område der vi har en endring, og det gjelder utstyr mellom kontor og hjemmet. Der ser vi en økning i antall hendelser der ansatte har mistet utstyr som følge av utstyr de skal ha med seg til/fra hjemme/kontoret.»*
F1	*For informant F1 kan hverken vedkommende eller virksomheten se at det har hatt noen sikkerhetshendelser relatert til korona (hjemme/hybridkontor) de siste 18 månedene.*
G1	*Organisasjon ved informanten har ikke observert noen vesentlig endring på måleindikatorer for uønskede innen informasjonssikkerhet.* *Det er en registrert en vis økning utfra arbeidsmiljø utfordringer – Bedriftshelsetjeneste har rapportert en økning i antall forespørsler perioden hvor arbeidstakere har jobbet fra andre lokasjoner enn kontoret.*
I1	*Det er ikke registret noen vesentlig endring i antall alvorlige hendelser for informanten og de selskapene som informanten samarbeider med. Fra informanten sitt ståsted er det dog registret en større åpenhet enn tidligere (pre nedstengning) ved uønskede hendelser.*
J1	*Informanten har ikke fullstendig innsikt i dette, men fra et psykososialt / psykisk perspektiv har de sett en økning i antall uønskede hendelser.*

Tabell 2: Svar informanter «Har dere sett en økning i antall uønskede hendelser som en følge av økningen i bruken av hjemme/hybridkontor»

Disse utsagnene fra informantene samsvarer også med funn gjort i en ekstra korona-undersøkelse som ble gjort i sammenheng med mørketallsundersøkelsen til Næringslivets sikkerhetsråd for 2020 (Næringslivets sikkerhetsråd, 2020, s. 39). Denne rapporten viser blant annet at kun 8% av respondentene (n=900) har sett en økning, men samtidig ser 8 % en nedgang i antall IT-sikkerhetshendelser relatert til nedstemningen som følge av koronapandemien. 65% sier at de ser like mange hendelser som tidligere. Type hendelser som en ser en økning i er relatert til bedrageri, hvor det er en økning fra 5% til 14% sett fra 2019 (n=1601) og til 2020 (n=900).



Figur 7: Type hendelser under koronakrisen vs. hele 2019 – Alle bedrifter (Næringslivets sikkerhetsråd, 2020, s. 37)

Et funn gjort i sammenheng med type hendelser som har oppstått, var hva den identifiserte årsaken var. Her svarer 38% av de forespurt virksomhetene (n=454) at årsaken var mangel på sikkerhetsbevissthet hos de ansatte (Næringslivets sikkerhetsråd, 2020, s. 21)

Både NSM og PST at den økte digitaliseringen har bidratt til ett mer komplekst trusselbildet. Dette er bekymringer som deles av enkelte informanter:

Informant F1 «*Hvis en ser tilbake de siste 18 månedene, så har digitaliseringen fått en enorm økning og oppsving. Men med denne digitaliseringen, har det også oppstått en situasjon hvor det kan oppstå sikkerhetsutfordringer ifm av manglende bestillerkompetanse».* Med manglende bestillerkompetanse, menes det i denne sammenheng at virksomheter og ikke nødvendigvis besitter den kompetansen som er nødvendig for å kunne iverksette de rette tiltakene ved digitalisering av f.eks. virksomhetskritiske funksjoner og tjenester. Tilsvarende bemerkes av B1 «*En annen sikkerhetsutfordring er at utviklingen og digitalisering går litt for raskt. Endringene skjer for raskt, og en ender opp med at det snakkes om devops, secops, privops etc. etc. – uten at kompetanse rundt dette nødvendigvis er på plass. En får etablert en «falsk» sannhet, pga. manglende kompetanse.».* Dette påpeker også informant F1 «… *Digitaliseringen går for raskt, så trusler og trender ikke oppdages raskt nok.».*

5.1.3. Hybrid kontoret som en utfordring

Flere av informanter oppfatter hybrid kontoret som en mulig større trussel, enn sett opp mot *hjemmekontor*. Denne trusselen ligger ikke nødvendigvis direkte i ett digitalt eller teknisk perspektiv, men omhandler i større adferd og holdningene til den enkelte ansatte. Denne oppfattelsen tas opp av flere. Enkelte informanter som ble kontakt som en del av denne

oppgaven, ønsket ikke å delta – eksempelvis «*Hei! Veldig interessert i å støtte sånt, men akkurat denne tematikken syns jeg er litt kjedelig. Ser ikke så mye forskjell i kulturbehovet/metodikk i ny hverdag! Så kanskje jeg faktisk takker nei denne gangen»*. Dette sammenfaller også med svar gitt under intervjuene av informantene som deltok, da flere ser bare på hybridkontoret som hjemmekontor, og kun som noe som er større i skala sett fra ett teknisk perspektiv.

B1 påpeker at «… *dette (hjemme/hybridkontoret) har nok alltid vært en del av trusselbildet, men har nok som en følge av situasjonen vi befinner oss i, blitt forsterket. I utgangspunktet er det ikke noe som er noe nytt, men det er omfanget som er annerledes.»*

D1 «… *I utgangspunktet har du mye av de samme tingene, uavhengig om du er lite eller mye hjemme.»*

Informant I1 representerer ikke en enkelt organisatorisk enhet eller virksomhet. Informanten besitter en rolle hvor det ytes bistand til små og mellom store bedrift (størrelsesorden 5 til 120) innen HR tjenester og digitaliserings rådgiving. Informanten I1 ser ingen eller få diskusjoner på sikkerhet relatert til bruk av hjemme/hybridkontor. «*Flere anser ikke hjemmekontoret som en sikkerhetsutfordring eller at man ikke oppfatter risiko ved denne typen arbeidsform/lokasjon. Dette er også en observasjon om at det nødvendigvis ikke var mer refleksjon ang dette tema før korona, men heller ingen vesentlig endring på dette etter 12.mars.» (I1)*

I1 påpeker at dette har en viss sammenheng med at mange av disse bedriftene ikke er typisk «hjemmekontor» organisasjon/virksomheter, men av karakter produksjon. Disse har begrenset mulighet for å benytte seg av hjemmekontor historisksett, men det er en økning av bruken for administrativt personell. Når en tar opp temaet sikkerhet med disse virksomhetene/organisasjonene, så er det lettere å få en forståelse for dette og tilhørende risiko til dette, nå enn før korona. Men det er fortsatt ingen reelle diskusjoner som blir tatt automatisk ifølge informant I1.

For informant A1 blir hjemmekontor noe adhoc og noe som en gjør basert på kortsiktig behov. Hybridkontoret er for A1 (som i henhold til definisjonen som ligger til grunn i oppgaven) hjemmekontor satt i system. «*Hybridkontoret der imot, da ting blir satt i system på en annen måte. En får med andre ord de mer dagligdagse oppgavene ved siden av at du skal jobbe 8 til 16. Det er f.eks. større sjanse for at det oppstår en utglidning av fokus, og en ender opp med å gjøre ting en ellers ikke ville gjort på arbeidsgiver PC, men en forglemmer*

seg, da en sitter hjemme.». Denne refleksjonen om «utglidning av fokus» går igjen hos både B1, E1, H1, I1 og J1.

Flere av informantene innehar en informasjon- og cybersikkehets bakgrunn, og påpeker at hybridkontoret i større grad, med informasjonssikkerhet som utgangspunkt, vil hybridkontoret i større grad sette KIT prinsippet under press. KIT står for Konfidensialitet, integritet og tilgjengelighet. (CIA – Confidentiality, Integrity and availability).

Konfidensialiteten blir satt under press ved hjemme og hybridkontoret, da arbeidsgiver ikke lenger har kontroll og tilgang til styring på samme måten som ved arbeidssted. A1 «… *Dette blir annerledes når en er hjemme. En vet ikke på samme måte hvem er tilstedte og hvor når informasjon åpnes/leses.».* Tilsvarende bemerkninger gjøres av B1, D1.

Tilsvarende funn ser en i forhold til Integritet. Det er bekymring fra flere informanter (A1, B1, D1) at informasjon kan bli endret utilsiktet eller mulig av andre uvedkommende.

Tilgjengelighet blir en mer konkret problemstilling for hjemme og hybridkontor i større grad. Tilgjengelighet på kontoret er ikke like påvirket, da med tanke på alle ressurser m.m en har tilgjengelig der ifm backup, ekstra utstyr etc. På ett hjemme og hybridkontor er en mer utsatt og sårbar, da en ikke har disse mekanismene ifm. infrastruktur robusthet/resilience. Dette er ett moment som bemerkes av nesten samtlige informanter i en eller annen kontekst, uten at det nødvendigvis ble nevnt i en KIT(CIA) sammenheng. Samtlige virksomheter i denne oppgaven representert ved informantene har eller hadde startet på ett digitaliseringsløp for adopsjon av sky tjenester som Microsoft 365 eller lignende. Kompetanse m.m relatert til dette, vil bli videre presentert i kapitel 5.2.

5.1.4. Hybridkontoret - En psykososial utfordring

Ett element som utpeker seg, er utfordringen hybrid- og hjemmekontoret kan utgjøre mot det psykososiale arbeidsmiljøet. Informant J1 «… *En mister tilknytningen til folkene. Du merker det gjerne på at etter møter, så har en small talk når en er på kontoret. Mens på hjemmekontoret og når møtet er over – så skrues video av, og en mister dermed med interaksjonen i etterkant med den ansatte. Eksempelvis, så kan den enkelte overbevise arbeidsgiver at alt er i orden den timen møtet pågår, men realiteten er en annen.».* Flere informanter er innom denne problemstillingen, men i mindre grad for de informantene som er av mer teknisk / IT-sikkerhetskarakter, kontra de som befinner seg innen HSEQ og HR. Her er det tydelig forskjeller mellom informantene ved at IT-funksjoner har større fokus på de

sikkerhetstekniske aspektene og de utfordringer en finner, kontra HSEQ og HR som er mer bekymret for det psykososiale. Siden denne oppgaven har ett få-tall informanter innen dette segmentet (HSEQ og HR), så trekker dette også frem gjennom litteraturstudier. Statens arbeidsmiljøinstitutt (STAMI) har gjort en større analyse (Fløvik, Lunde, Vleeshouwes, Johannessen, Finne, Mohr, Jørgensen & Christensen, 2021) av tilgjengelig forskningsmateriale på blant annet arbeidsmiljø ved hjemmekontor, og deres kunnskapsoppsummering er ikke konkluderende , da det er noe svak og sprikende datagrunnlag. Ett av funnene er dog at utvidet bruk av hjemmekontor (herunder også hybridkontor) kan ha både en positiv og negativ effekt på flere psykososiale aspekter. Negativ effekter som ble påpekt er at arbeidstakere får en dårlig balanse mellom arbeid og fritid, manglende sosial støtte mellom kollegaer og en generell «utglidning av fokus» som det også ble referert til av informant A1, I1 og J1.

5.2. Hovedfunn forskningsspørsmål 2

«Hvordan kan den ansattes kunnskap, adferd og holdninger påvirke digital sikkerhetskultur i en hybrid kontorsituasjon?»

Dette forskningsspørsmålet skal kartlegge hvordan den ansattes kunnskap, adferd og holdninger vil kunne ha innvirkning på den digitale sikkerhetskulturen i hybride kontorløsninger. Her er det gjort flere funn som kan være viktige for videre arbeid med digital sikkerhetskultur ved hjemme- eller hybridkontoret. Samtlige informanter har en forståelse av at ansattes adferd, holdninger og kunnskap vil være avgjørende fremover, og at tekniske løsninger ikke vil være tilstrekkelig for klare å ivareta sikkerheten. Det som kommer frem, er at dette ikke nødvendigvis kobles opp mot digital sikkerhetskultur, men ses mer ifra et generelt sikkerhetskulturperspektiv. Ingen av informantene har direkte oppmerksomhet på digital sikkerhetskultur som et eget prinsipp i sikkerhetsarbeidet. Samtlige av informantene dekker flere av hovedmomentene knyttet til digital sikkerhetskultur, uten at dette nødvendigvis er bevisst. Informantene og virksomhetene de representerer har gjort små tilpasninger i sine kompetanse- og opplæringsprogram som en direkte følge av korona, nedstengningen og en mulig etablering av hybridkontoret. I studier gjennomført av offentlige instanser, har mange ansatte gitt uttrykk for at de har fått liten eller ingen opplæring for hvordan jobbe sikkert på hjemmekontoret. Det er i denne oppgave observert at det er et tydelig skille mellom de «tekniske» informantene og informanter med HR-/HMS- perspektiv. Flere informanter ser det ikke som nødvendig å gjøre større endringer, mens HR/HMS-

representantene i større grad påpeker viktigheten av å endre ledelsesmetodikker og -strukturer for at ledelse av ansatte på hjemme- og hybridkontor skal bli mer effektivt.

De påfølgende delkapitellene vil i nærmere detaljer presentere funnene gjort i sammenheng med forskningsspørsmål 2.

5.2.1. Kompetanse

Samtlige virksomheter som er en del av denne oppgaven, har kompetanse og opplæring i informasjonssikkerhet for sine ansatte, men ingen behandler digital sikkerhetskultur som ett eget område. Nivået og metodikk er av varierende grad og kompleksitet.

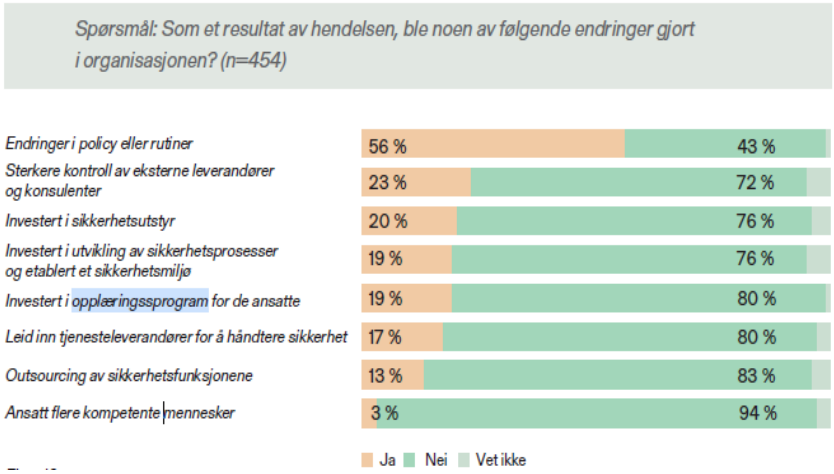
Flere av virksomhetene er enten sertifisert eller har fokus på ISO/IEC 27000 serien. Denne standarden har til hensikt å sikre en virksomhets informasjon og for å etablere et system for dette. ISO/IEC 27000 serien er en større serier, med flere underliggende rammeverk, hvor av ISO/IEC 27001 er en av den meste kjente. For å kunne inneha en 27001-sertifisering kreves det at en blir godkjent gjennom en revisjon som ser på flere kontrollpunkter som inngår i den (Norsk Standard, 2017). Disse skal ikke ettergås her, men ett viktig element som er til stede gjennom hele 27000 enten direkte eller implisitt er kravene til sluttbrukers kompetanse. Denne standarden nevnes, da flere av virksomhetene som er representert ved informantene har lagt opp sitt opplæringsløp innen informasjons- og cybersikkerhet iht. de kravene som er i denne standarden (ISO27001).

B1 påpeker at deres opplæringsfokus er «… *ISO 9001 og 27001 sertifisert og legger opp til et sikkerhetsrammeverk rundt NIST. Forpliktet oss selve til oss selv til å ha en spesiell opplæring, trening rundt informasjonssikkerhet, data, cybersikkerhet og ikke minst personvern.»*

F1 «… *Sikkerhet og kompetanse har alltid vært i fokus for virksomheten. Virksomheten har i økende grad strukturert kompetansehevning blant annet som følge av et ISO 27001 løp.»*

ISO/IEC 27000(1) er ofte i søkelys hos konsulentvirksomheter, eller virksomheter/selskaper av betydelig størrelse, da dette ofte er bransjekrav i en eller annen form og er de facto standard for de fleste som har fokus på informasjons- og cybersikkerhet i Europa og ellers internasjonal. NIST er (National Institute of Standards and Technology) Cyber security framework (CSF) er en tilnærming til ISO 27001 og ble utviklet som krav til føderale tjenester og departement i USA.

Ved mindre virksomheter (størrelse orden 5 til 120 ansatte) representert ved informant I1, er oppmerksomheten på informasjonssikkerhet mindre. Informant I1 «*I all hovedsak er det lite søkelys på dette i små og mellom store bedrifter. Gjerne har en virksomhet/organisasjonsleder vært på et kurs, og fått noen tips på at informasjonssikkerhet er nyttig.»*. Det er ikke gjort noen ytterlige undersøkelser ved intervju for å bekrefte denne påstanden fra I1 utover informantgruppen. Gjennom sekundærkilder og undersøkelser svarer ansatte i små og mellomstore bedrifter, at det er mindre fokus på opplæring. I mørketallsundersøkelsen for 2020 (Næringslivets sikkerhetsråd, 2020) svarer kun 19% (Figur 8) av virksomhetene at de har gjort organisatoriske endringer og investert i et opplæringsprogram for de ansatte i etterkant av en uønsket hendelse.



Figur 8: Organisatoriske endringer som følge av uønskede hendelser

Analyse av datagrunnlaget presentert i figur 8 tilhørende de representative virksomhetene, er det i stor overvekt virksomheter med ansatte mellom 5-19 og 20-99 ansatte.

NorSIS ved Nettvett (Nettvett, 2021) (og andre aktører) ser på kompetanse for de ansatte som en av de viktigste faktorene for å unngå uønskede hendelser innen den digitale sfære. Det er også ett av hovedmomentene innen digital sikkerhetskultur. Ingen av informantene i denne oppgaven kan bekrefte at digital sikkerhetskultur er ett eget moment som de har fokus på, da deres fokus er rettet mot sikkerhet og digital sikkerhet.

Som en del av økt bruk av hjemme og hybride kontorløsninger, identifiserer A1 og virksomhet VA1 veldig tidlig i nedstengningen, utfordringer relatert til den menneskelige faktoren ved uønskede hendelser. Dette som en følge av type uønskede hendelser de opplevde, ref. 5.1.2.

A1 forteller «… *Det ble veldig tidlig identifisert en utfordring relatert til den menneskelige faktoren* (ved uønskede hendelser)*, helt i starten av pandemi som en av de viktigste. Veldig tidlig ble det rullet ut ytterligere tekniske tiltak, men også søkelys på prosessene og menneskene for å imøtekomme den nye arbeidshverdagen.»*

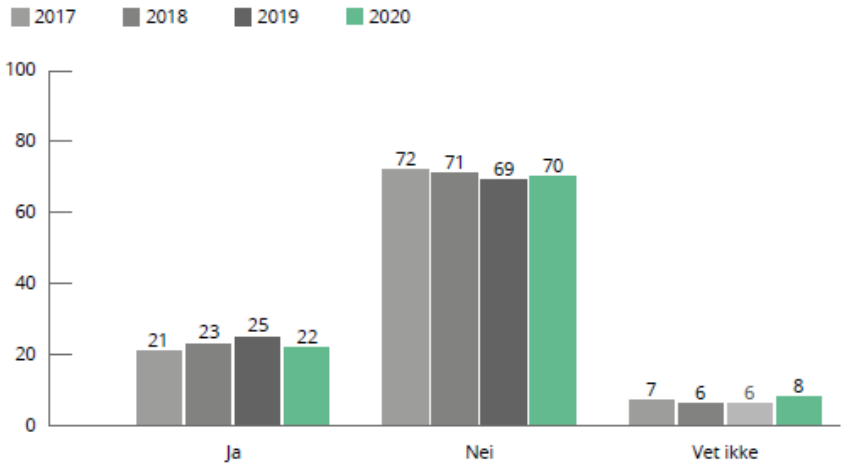
Ingen av informantene sier det er gjennomført større endringer rundt den digitale eller tekniske opplæringen som en følge av økt bruk av hjemme- og hybridkontor. Men som informant D1 påpeker «… *ingen direkte større endringer, men det er noe ekstra fokus på bevissthet. Har blant annet leid inn psykologer for å prate om viktige elementer og hvordan kan vi ivareta folk på hjemmekontoret. Denne integriteten og holdningene en vil at folk skal ha på kontoret, håper vi at ansatte tar med seg hjem eller andre steder de jobber …. Dette er den tingen vi er mest bekymret for, nemlig folkene.»* Denne utfordringen deles i varierende grad av de fleste av informantene. Informant D1, I1 og J1 er mer tydelig på dette området, da dette faller innenfor deres daglige rammer (HR og HSEQ). Informanter av karakter «IT-teknisk» påpeker liten eller ingen vesentlige endringer i opplæringsprogram.

Virksomhet VA1 og informant A1 har i flere år gjennomført årlige undersøkelser om sikkerhet og bevissthet rundt dette. De har gjennom flere år sett en klar økning i betydningen av ansattes forståelse av at sikkerhet er viktig. Det som er interessant, er at senere år, så kommer det også frem fra de samme undersøkelsene at færre ansatte føler seg kompetente nok og færre føler de har god nok kompetanse til trygg bruk av informasjonsteknologi og systemer. Samme virksomhet ser også at en ser at færre har tillitt til at kollegaer og ledere er overvåkne for den risiko de utsetter seg selv for og det er færre som syns ledelsen kommuniserer godt nok rundt sikkerhet og viktigheten av det. Det kan være en effekt av at folk nå (på tidspunktet av intervjuet 02.09.2021) sitter mer hjemme og alene, kontra det at man er på kontoret.

Alle virksomhetene gjennomfører eller tilbyr opplæring i informasjons og cybersikkerhet. Opplæringen skjer enten som en del av ansettelses-prosessen, gjennom styrende dokumentasjon, elektronisk læring eller self-service. Flere av virksomhetene har tatt i bruk Nano-learning. Her er det små opplærings momenter på gjerne 2-3 minutter maksimalt, i stedet for lengre kurs som den ansatte gjerne ikke har mulighet til å gjennomføre, men i raskere intervaller. Ingen av virksomhetene har eget fokus på digital sikkerhetskultur som et eget element i denne opplæringen.

I mørketalls undersøkelsen til NSR (2020), er det funn relatert til den ansattes kompetanse og opplæring. I denne rapporten sier 77 % av de forespurte virksomhetene (n=1601) at de har gjennomført aktiviteter som skal øke den ansatte bevissthet rundt sikkerhet i løpet av året som rapporten dekker (04.02 til 21.02 2020). Opplæringen som gjennomføres er i alle hovedsak basert på interne foredrag med 69% og 39% ved e-læring (n=1231).

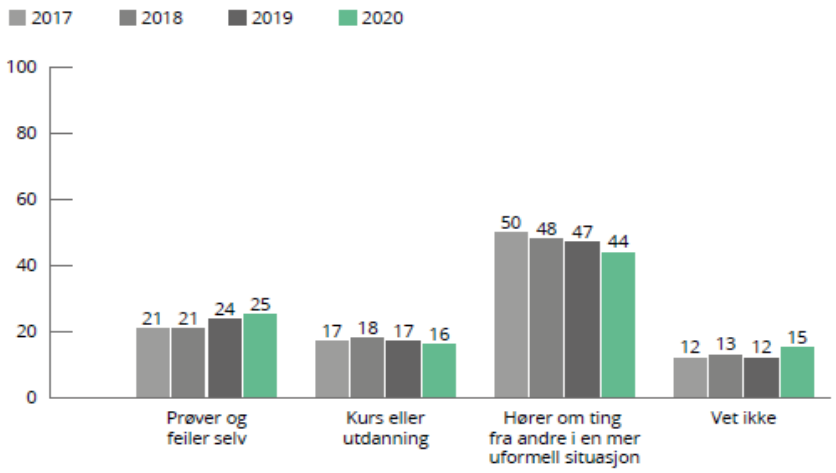
Ser vi til NSM sin rapport om nordmenn og digital sikkerhetskultur (2020), så svarer 70% av informantene at de ikke har mottatt noen form for organisert opplæring i digital sikkerhet i løpet av de siste to årene. Tilsvarende funn blir gjort på spørsmålet *har du fått organisert oppløring i informasjonssikkerhet i løpet av de siste to årene.* Dette under kan en se under representer ved figur 9.



Figur 9: «Har du fått organisert opplæring i informasjonssikkerhet de siste to årene?» (Norsk senter for informasjonssikring, 2020)

Et viktig moment i en læringsammenheng, er hvem en lærer av. Her viser rapporten (Norsk senter for informasjonssikring, 2020) at 35% lærer av seg selv og egen interesse, 20% prosent av eksperter, 8% av sjefer eller leder og tilslutt 25% av venner eller kollegaer. 12 % sier at de ikke vet.

Et videre interssant funn her, er hvordan informantene lærer (Figur 10). 25% sier de lærer av å prøve og feile selv. 16% gjennom organisert kurs eller utdanning, 44% ved at de hører om ting fra andre i en mer uformell situasjon, og tilslutt 15% sier de vet ikke. En grafisk oppstilling at disse tallene , sett opp mot tidligere år gir følgende resultat.



Figur 10: «Hvordan lærer du vanligvis om informasjonssikkerhet?» (Norsk senter for informasjonssikring, 2020)

Undersøkelsen (Norsk senter for informasjonssikring, 2020) er gjennomført av analyseinstituttet YouGov. Det er i uke 14-15 i 2020 gjennomført til sammen 1000 CAWI-intervjuer i et landsrepresenativt utvalg bestående av personer som er 18-74 år. Denne rapporten er med andre ord ikke nødvendigvis representativt fra et arbeidsgiver perspektiv, men gir et overordnet bilde av opplæring for nordmenn i digital sikkerhet generelt.

5.2.2. Holdninger og adferd

Per nåværende tidspunkt så finnes det lite forskning på menneskers holdninger og adferd utfra en digital sikkerhetskultur perspektiv ved bruk av hjemme- og hybridkontor i stor skala. Det er identifisert et fåtall komparative studier gjennom masteroppgaver, som til en viss grad ser på en tilsvarende problemstilling, men da kun utfra sikkerhetskultur og ikke det digitale aspektet av dette. Hovedtyngden av den informasjonen som presenteres i dette delkapittelet, er i vesentlig grad hentet inn fra informantene der dette er relevant, men også sekundærkilder ifm. empiriske studier gjennomført eksempelvis NorSIS.

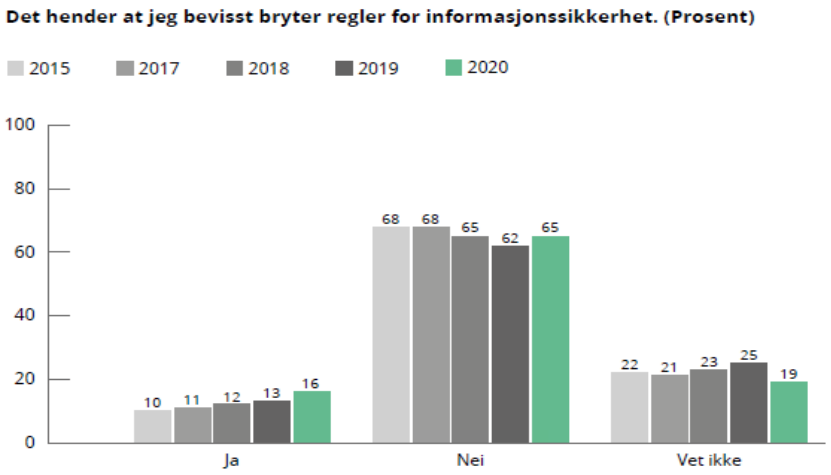
Et generell adferds funn relatert til hjemme- og hybridkontor som er gjengående hos flere informanter (A1, D1, G1, I1 og J1) er hvordan grensen mellom arbeid og fritid viskes ut. Dette bemerkes også av STAMI (Fløvik et al., 2021) som også legger merke til hvordan en slik situasjon kan være med på å skape uønskede situasjoner. Dette er ikke forankret direkte mot digital sikkerhetskultur, men disse påstandene vil kunne være gjeldende også innenfor dette området. Dette understøttes av J1 i en lengre kommentar:

«*… Utfordringen med adferd, er at adferd må regel-styres ... Det må styres i retning som motiverer til en positiv adferd som er ønsket (fra et arbeidsgiverperspektiv). Dette kan en*

gjerne dra relasjoner til phising testene. Den ansatte blir «latterliggjort» (om det ordet skal brukes) ved at den ansatte ble tatt i testen. Den følelsen den ansatte sitter igjen med i en slik situasjon kan bidra til en adferdsendring, da en slik opplevelse ikke er ønsket av den ansatte. Dermed oppstår en situasjon hvor en får endret adferd ifm. av regelstyringen. Dette vil igjen bidra til at en kan få en kulturell endring, med at mange vil følge denne typen adferd ved phising testen og det å bli «tatt»».

Virksomhet til A1 har gjennomført flere studier internt, der det ble blant annet sett på bevissthet. Denne studien viser at en av den viktigste endringsagent for dem, er nærmeste leder. For VA1 har det vært mye søkelys på dette området og de individene innenfor ledelse her. Disse skreddersyr sin egen opplæring, nettopp for de så at dette hadde en stor effekt på resten av organisasjonen og den ansatte holdninger og adferd. Som A1 påpeker «… *En skal være bevisst på at ledere så vel som medarbeidere besvarer denne spørreundersøkelsen gjennomføres internt. Og det er summen av respondentene som sier at dette (informasjonssikkerhet) er mer skummelt enn hva som er komfortabelt. Men en har uansett individer som tenker at dette går helt fint, og «gun'er på» og tenker at dette går fint. Her blir det naturlig å koble en slik holdning mot kompetansen, og en manglende forståelse av de risikoene de utsetter seg for».* A1 er her inne på flere områder innen digital sikkerhetskultur nemlig adferd, holdninger, risikoforståelse og kompetanse.

I Nordmenn og digital sikkerhetskultur 2020 (Norsk senter for informasjonssikring, 2020), er det flere elementer som undersøkes utfra et adferd og holdningsperspektiv og som er relevant for denne oppgaven.



Figur 11: «Det hender at jeg bevisst bryter regler for informasjonssikkerhet (Prosent)» (Norsk senter for informasjonssikring, 2020)

Som en ser over i figur 11, så er det 16% av respondentene som sier de bevisst bryter regler for informasjonssikkerhet. Dette med en økning på 3% fra forrige undersøkelse i 2019 (Norsk senter for informasjonssikring, 2019).

I en komparativ studie og masteroppgave *«Hvordan ivareta en god sikkerhetskultur på hjemmekontor?»* (Mydland & McCabe, 2021) ble det gjort flere tilsvarende funn. I denne oppgaven ble det avdekket via flere av dens informanter at flere ser at grenseskille mellom jobb og privatlivet blir visket ut. Dette sammenfaller med andre funn gjort hos A1, D1, I1, J1, men også undersøkelse gjennomført av STAMI (2021).

5.2.3. Sikkerhetskultur og digital sikkerhetskultur

Ingen av informantene uttaler at de har noe direkte oppmerksomhet på digital sikkerhetskultur ut ifra veileder til Digdir eller NSM v/Nettvett (Digitaliseringsdirektoratet, 2021b; Nettvett, 2021). Alle informantene har en tydelig og god forståelse av sikkerhetskultur og er bevisst på viktigheten av dette i en organisatorisk kontekst.

NSM har uttalt(Nasjonal sikkerhetsmyndighet, 2016) at alle virksomheter har en sikkerhetskultur, den er bare en del av en virksomhetskultur, dette påpekes også av informant A1 «… *Jeg tenker at det egentlig ikke er noe som heter sikkerhetskultur – det er i alle tilfeller snakk om en virksomhetskultur, hvor sikkerhet er et element i denne. Og det er viktig å jobbe inn dette elementet så det blir en integrert del av virksomhetskulturen mer enn noe som er "på siden" eller som oppfattes som noen andres ansvar.».* Dette støttes av B1, da B1 påstår at EN sikkerhetskultur ikke direkte kan defineres. Begrunnelsen for dette legges i at større virksomheter med stor sannsynlighet har flere sikkerhetskultur, basert på forskjellige geografiske lokasjoner, hvor lokale kulturelle forhold spiller inn. Her nevnes akkulturasjon som ett element. B1 at en ikke skal prøve å endre hvordan kulturene består, men man skal innføre en faktor/et element som er felles for alle, tilpasset de ulike subkulturene – Sammen utgjør dette en akkulturasjon, som igjen gjør at en kan få en overordnet sikkerhetskultur.

Informantene definerer sikkerhetskultur på følgende måte:

Informant	Kommentar
A1	*«Sikkerhetskultur kan defineres som bevisstheten du har til riktig håndtering av informasjon og at adferden din i omgangen med informasjonen. Ergo, hvor bevisst er du om bevisstheten til informasjonen og hvordan oppfører du deg.»*

D1	*Sikkerhetskultur kan defineres som: Kultur er summen av adferd, og adferd kommer av hvilke følelser som finnes. Følelser kommer av tanker. Og tanker kommer av sanser. Så hvis vi snur på det, - du sanser noe, som får deg til å tenke og det du tenker medfører en følelse. Dette vil skape en adferd, hvor summen av adferd er kultur.*
F1	«*Alle har en kultur, om så en god eller dårlig. Jobber med sikkerhet, prater sikkerhet, og tenker sikkerhet. Sikkerhetskultur blir noe du har i ryggraden.*
G1	*Summen av kompetanse, holdninger og adferd for den ansatte innenfor informasjonssikkerhet. Bevissthetsnivået til organisasjonen».*
I1	«*Sikkerhetskultur handler mye om å forstå hvilke handlinger som utgjør en risiko, og samtidig forstå hvilke handlinger som demper risiko. Det er også viktig å forstå hvilke valg en skal ta etter hvert».*
J1	«*Det blir i mange tilfeller en definisjons sak på hvilket nivå vi skal snakke om sikkerhet – Kultur hvor det er bevissthet rundt de farer og risikoer som finnes rundt deg. En tydelig definert forståelse for hva dette kan bety.»*

Tabell 3: Informantenes definisjon på sikkerhetskultur

På spørsmålet om hva informantene definere som en *god* sikkerhetskultur, er essensen i svarene i all hovedsak lik, nemlig at en god sikkerhetskultur er noe du ikke trenger å tenke over, men noe som ligger i ryggraden og at den ansatte skjønner hvorfor det er viktig.

Informantene ble stilt spørsmål om hvordan de anser sikkerhetskultur og digital sikkerhetskultur opp mot hverandre, eller om det bare blir to sider av samme sak. På dette spørsmålet anser informantene i hovedvekt at digital sikkerhetskultur bare er det samme eller en del av sikkerhetskulturen og ikke nødvendigvis en egen kultur artefakt.

5.2.4. Risikooppfattelse og forståelse

Risiko aspektene som informantene ble presentert i denne oppgaven, så både på hvordan de oppfatter risiko ved bruk av hjemme eller hybridkontoret, men også fra et tjeneste perspektiv. Som flere nasjonale aktører har påpekt i senere tid (Nasjonal sikkerhetsmyndighet, 2021a, 2021b; Politiets sikkerhetstjeneste, 2021), så har «den nye normalen» gjort at en har fått etablert noe permanente løsninger, basert på noe som gjerne i utgangspunktet var ment til midlertidige løsninger. Uten at dette er vurdert som en del av denne oppgaven, men det er nærliggende å tro at flere av disse løsningene er blitt permanente som en følge av den vedvarende nedstengningen av samfunnet. Hadde nedstengningen vært av en kortere periode hadde nok flere av disse tjenestene blitt dekommisjonert kontra det å bli permanente

NSM i sin siste rapport om nasjonalt digitalt risikobilde (2021) mener at det er for dårlig eller manglende forståelse av digital risiko i Norske virksomheter «*Flere og flere virksomheter erkjenner at cyberoperasjoner kan ramme alle og NCSC erfarer at stadig flere prioriterer det*

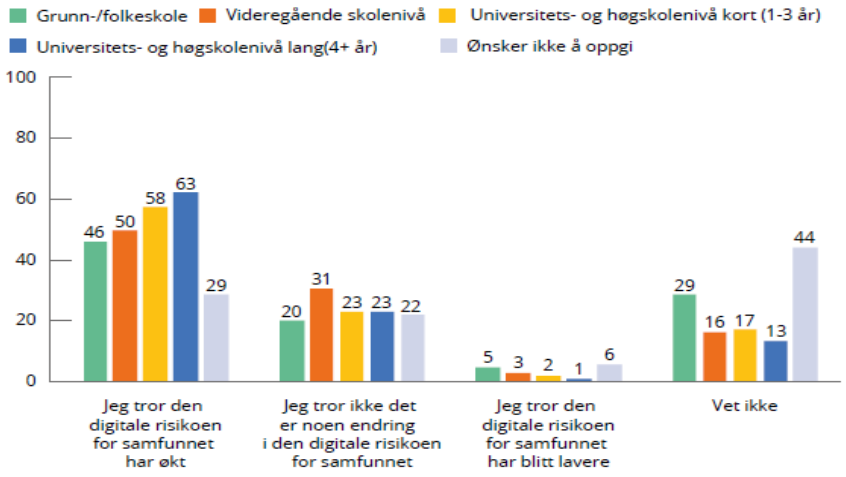
digitale sikkerhetsarbeidet. Vi ser likevel at mange norske virksomheter ikke har et forsvarlig sikkerhetsnivå for å beskytte viktige verdier. Økt bevissthet om digital risiko har ofte ikke blitt omsatt i handling. Dette bør være et tema i alle styrerom og ledergrupper.» NSM, 2021

Flere av informantene har ett veldig bevisst forhold til risiko. Som A1 påpeker «*Rent risikomessig er det en økt risiko for en økning i «trusler» eller uønskede hendelser når en er hjemme. For det endrer mye av adferdsmønsteret. Det blir også en økt risiko vedrørende tilgjengelig tiltak som en virksomhet at etablert for å beskytte en virksomhet. Mange av disse er bygget rundt «kontoret» og vil ikke i samme grad være like effektive eller tilgjengelig».* Denne påstanden deles av samtlige av informantene i varierende grad. De fleste ser på hjemme- og hybridkontoret som en utfordring med en tilhørende risiko ved bruken. I den sammenheng ble det stilt spørsmål om det var blitt gjort noen større risikovurdering ved nedstengningen og eventuelt gjennomført endringer rundt tilgjengeligheten av tjenester som de ansatte benyttet seg av. De fleste av virksomhetene til informantene hadde allerede eksponert de tjenestene som er nødvendig for en mobil arbeidsgruppe. Dermed var det ingen av informantene som bekreftet at de hadde gjort noen større risikoanalyser, men mer heller bare en revurdering av allerede eksisterende analyser for å undersøke om det var noen elementer som var oversett innledningsvis. En overvekt av virksomhetene hadde allerede en krisehåndteringsplan etablert. Flere av disse planene inneholdt allerede nødvendig planverk for hvordan fortsette forretningskontinuitet ved en krise scenario, hvor arbeidssted var utilgjengelige. Det var dette planverket som ble tatt i bruk av de fleste for å kunne imøtekomme nedstengningen. Dette kan kobles tilbake til utsagn gjort av flere informanter, om at hybrid- og hjemmekontor er ikke noe forskjellig teknisk sett, en snakker bare om en forskjell i skala og mengde.

Hos I1 observeres det en noe annen holdning blant de små virksomhetene I1 jobber med, dette er knyttet til risikoforståelse i situasjonen (nedstengningen) «*Mange av dem små og mellomstore har fått eller vært utsatt for trussel/hendelser, hvor ansatte tar med seg, sletter eller ødelegger informasjon (ingen diskusjon om dette var villet handling). Da oppstår det sikkerhetsdiskusjoner – Ikke nødvendig basert på en reflektert risikoforståelse, men dette fører ofte til at effekten blir at «alt» av sikkerhetsteknikk «skrues på», uten at dette nødvendigvis reflekteres gjennom en bevisst forståelse av hva de faktisk trenger – handler det faktisk om system eller holdninger?* I1 er også usikker på om det i det hele tatt tas noen større risikovurderinger for bruk av hybridkontor av små og mellomstore selskaper. Antagelsen er

her at det nok mest sannsynligvis er en «same» holdning blant en overvekt av de små og mellom store bedriftene.

I rapporten *Nordmenn og digital sikkerhetskultur* for 2020 (Norsk senter for informasjonssikring, 2020) som dekker et større spekter av informanter, sier 55% av dem at de tror den digitale risikoen for samfunnet har økt på spørsmålet *«Tror du korona-utbruddet medfører en endring i det digital risikobildet for samfunnet».* 26% tror ikke det er noen endring, og 3% tror den er blitt lavere. Ser et på utdanningen i forhold til forrige spørsmål, viser studien (Norsk senter for informasjonssikring, 2020) følgende fordeling basert på utdanning iht. forrige spørsmål og sammenheng med risikoforståelse.



Figur 12: Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for samfunnet (ut fra utdanningsnivå) (Norsk senter for informasjonssikring, 2020)

Det kommer også frem (Norsk senter for informasjonssikring, 2020) at 24% tror at den digital risiko har økt for seg selv, på spørsmål *«tror du at korona-utbruddet medfører en endring i det digitale risikobildet for deg selv?»*. En observasjon her er at 55% tror på en økning for samfunnet, men bare 24% tror på en økning for seg selv. Videre tror tilsvarende 52% ikke at det medfører noen endring. Sidestiller vi disse tallene fra rapporten (Norsk senter for informasjonssikring, 2020, s. 28-30) kan vi gjøre følgende observasjon:

Rapporten (Norsk senter for informasjonssikring, 2020) påpeker et interessant moment her, med det de kaller for «optimism bias», som tilsier «*... at farlige eller uønskede ting muligens kan komme til å hende andre, men ikke en selv. Den enkelte føler gjerne at de har en kontroll over de tingene som medfører digital risiko, selv om den reelle kontrollen kan være mye lavere enn en tror*» (Norsk senter for informasjonssikring, 2020). En effekt av en slik oppfattelse er at en gjerne undervurderer risikoer en står ovenfor. Som det påpekes av Bjergsjø et al. (2020) så viser forskning at en ved høyere grad av kompetanse har større

sannsynlighet til å overvurdere egne evne, og dermed tar større grad av risiko ved sin egen oppførsel og risikoakseptanse kriterier.

5.2.5. Ledelse

Flere av virksomhetene (kap.5.2.1) i denne oppgaven jobber med en systematisk tilnærming til informasjonssikkerhet ved blant annet ISO 27000 serien og NIST CSF. Ser vi direkte til ISO 27001 (Norsk Standard, 2017, s. 10) kapitel 5 og punkt 5.1 (paragraf D, F, G, H) , så sier denne:*(D) Formidle betydningen av effektiv informasjonssikkerhetsstyring og overholde kravene i ledelsessystemet for informasjonssikkerhet*

- *(F) Veilede og støtte personer slik at de kan bidra til virkningen av ledelsessystemet for informasjonssikkerhet*
- *(G) Fremme kontinuerlig forbedring; og*
- *(H) Støtte andre relevante lederfunksjoner til å vise sitt lederskap på en egnet måte for deres ansvarsområde*

Det er spesielt paragraf D, F, G og H som er interessant i denne sammenheng. Standarden er tydelig på ledelsen sitt ansvar ved informasjonssikkerhet.

I den sammenheng ble informantene spurt om ledelsens involvering ved sikkerhet og digital sikkerhetskultur, men også om det er blitt noen endringer som en følge av nedstengningen og introduksjon av hjemme- og hybridkontoret. Funn viser at ledelsen ved de fleste virksomhetene i denne oppgaven er bevisst sitt ansvar rundt dette, men ikke nødvendigvis er bevisst konseptet digital sikkerhetskultur. Oppmerksomheten ligger i overvekt på sikkerhetskultur.

Informant B1 *«På generelt grunnlag ja, men en kan spole tilbake bare tre år tilbake i tid, så var situasjonen en annen. Noe som har modent, generelt, over tid.»* og Informant G1 «*Absolutt opptatt av dette området, og har jevnlig gjennomganger på dette området innenfor informasjonssikkerhet.»*

Som en del av sitt arbeid har informant I1 vært i dialog med ledelse i forskjellige virksomheter både før og etter utbruddet av korona (og dermed hjemmekontoret), og informanten kunne lett se hvem/hvilke som hadde tilpasset og endret seg iht. den nye hverdagen. I1 beskriver hvor en hadde ekstroverte relasjonslederne, har disse ikke klarte å snu seg å bli litt mer introvert og litt mer strukturert og mer lyttende, så hadde disse falt

gjennom. De lederne som allerede var mer aktive på denne måten, hadde gjort det betraktelig bedre. I1 påpeker at leders adferd får nå en mye større betydning i forhold til digitalisering. Hvor en tidligere kunne «lene deg på den superbrukeren», dette kan en ikke lengre – da alle selv må ha den selvledelsen. Her må det nok vurderes andre kompetanse elementer som en må ha opplæring på, slik at en bedre kan forstå situasjonen. På samme måte som at brannmuren ikke stopper all søppel e-eposten, da en som ansatte må ha ett mye større forhold til den selv (Ref. kompetanse og risikoforståelse) – dette i seg selv, er et eksempel på nødvendigheten av kompetanse.

I andre komparativ oppgaver (Gunnes, 2021) er det gjort flere tilsvarende funn. Dette er funn som samsvarer med funn gjort i denne oppgaven. Disse er i all hovedsak relatert til ledelsens ansvar til å være gode forbilde ved blant annet bevisstgjøring og opplæring.

«*Hvordan ivareta god sikkerhetskultur på hjemmekontor» (Mydland & McCabe, 2021)* gjøres det tilsvarende funn. Der ser en at ledelse ved hjemmekontor for flere virksomheter har vært utilstrekkelig. Dette gjelder både kommunikasjon, og for eksempel perspektiver vedr

sikkerhet på hjemmekontoret. Et funn i den oppgaven beskriver hvordan en av dens informanter «*Jeg tror ikke sikkerhetskultur eller sikkerhetsstyring har en tilstrekkelig plass i virksomheten, den trekkes frem i "festsammenheng" for å høre fint og glansete. Noen ganger blir sikkerhetskulturen trukket frem når det passer seg, og andre ganger som et hår i suppen, ett hinder for gjennomføring av enkelte saker» (Mydland & McCabe, 2021)* . Dette funnet er tilsvarende med uttales fra I1 og J1 ved både kompetanse, ledelse og risiko tidligere beskrevet i tabellene under.

Eksempelvis påpeker NorSIS i en spørreundersøkelse fra 2021, at så mange som 47 prosent av respondentene, ikke har fått informasjon fra sin arbeidsgiver for regler og/eller rutiner om hva som er gjeldende for digital sikkerhet på hjemmekontoret (Norsk senter for informasjonssikring, 2021a). Som ansvarlig for sikkerhet, vil dette være ett eksempel på manglende ledelse ansvar for sikkerhet, men gjerne en manglende forståelse av hvordan hjemme- og hybridkontor kan utgjøre en risiko for virksomheten.

I tabellene 4 og 5 under, er det blitt oppsummert de funn som er gjort og presentert gjennom kapitel 5. Disse funnene representerer utsagn fra informanter og andre funn gjort i sammenheng med oppgaven. Tabellene er strukturert i henhold til de åtte punktene som utgjør en digital sikkerhetskultur. Det er disse funnene som vil bli drøftet og diskutert i kommende kapitel 6.

Overordnede trusselbilde	Sikkerhetsutfordringer ved hybridkontoret	Hybridkontoret som en trussel	Hybridkontoret – En psykososial utfordring
Det digitale risikobildet for Norge er skjerpet. Den økte digitalisering av blant annet verdikjeder er med å bidra til at det digitale risikobildet er skjerpet og har økt.	Det er ingen vesentlig økning i antall uønskede hendelser knyttet til hjemme- og hybridkontor fra et digitalt teknisk ståsted.	Hybridkontoret oppfattes ikke av informantene som en større sikkerhetstrussel enn hjemmekontoret.	HR og HMS informanter er tydelige på at hybridkontoret oppfattes som et psykosial utfordring. Dette fremkommer også i forskning gjennomført av offentlige instanser.
Pandemien og nedstengningen har bidratt til å forsterke det eksisterende risikobildet. En ser en kraftig og tydelig økning i eksempelvis phising o.l som bruker korona som et middel.	Det er identifisert en økning koblet til brudd av retningslinjer, prosesser og annet styrende dokumentasjon fra et informasjons- og cybersikkerhetsståsted.	Hjemmekontor, inkludert hybridkontor har alltid vært en del av trusselbildet ifølge informantene.	Informantene er bekymret for utglidning og problemer å skille mellom privat og jobb. Noe som en ser, oppstår med vedvarende og lengre perioder med hjemme- eller hybridkontor.
	Det er tydelig bekymring hos informantene, myndighetsorganer og andre aktører rundt hvordan kultur, adferd og holdninger kan og vil oppstå som en følge av utvidet og økt bruk av hjemme- og hybridkontoret.	Det er et avvik mellom informanter om hjemme- og hybridkontoret oppfattes som en potensiell sikkerhetsutfordring. CISO/sikkerhetssjefer har stort søkelys på det tekniske, men overser i en viss grad det psykososiale og kulturaspektet, som igjen er tydeligere for HR/HMS informantene.	
	Det er en generell bekymring blant informantene at digitalisering går for raskt, og at tiltak som utvikles ikke vil klare å holde tritt med utvikling. Dette påpekes tilsvarende av myndigheter og andre aktører.	Det er spesielt brudd på konfidensialitet og integritet (sett utfra CIA/KIT) som utgjør hovedtrussel ved hybrid kontoret	

Tabell 4 Oppsummering av funn del 1

Kompetanse	Holdninger og adferd	Sikkerhetskultur og Digital sikkerhetskultur	Risiko oppfattelse	Ledelse
Samtlige virksomheter har fokus på kompetanse, men ingen av virksomhetene har eget fokus på digital sikkerhetskultur.	Det er gjentagende funn blant informantene, samt i studier gjennomført av offentlige organer og andre komparative studier, at det er en klar utvisking av grensen mellom privatliv og jobb ved hjemme- og hybridkontoret.	Ingen av informantene har fokus på digital sikkerhetskultur som et separat tema, men det inngår som en del av arbeidet med en overordnet sikkerhetskultur.	Ingen av informantene hadde gjennomført nye risikoanalyser som en følge av nedstengning og etablering av hjemme- eller hybridkontor under pandemien.	Blant informantene er det en tydelig forståelse av viktigheten med god ledelse for at informasjons- og cybersikkerhet skal være mulig å ivaretas.
Større virksomheter har i større grad en strukturert tilnærming til kompetanse, kontra små og mellom store som har et mer adhoc fokus på (digital sikkerhet) kompetanse.	En utglidning av grenseskillet mellom privatliv og arbeid vil ikke bare kunne føre til uønskede hendelser, men også utfordringer knyttet til lojalitet og en innside problematikk, som en følge av dårligere eller lavere mulighet for kontroll og styring.	På spørsmålene om hva er sikkerhetskultur og hva er en god sikkerhetskultur, er svarene stabile og sammenlignbare uten større avvik eller spredning.	Flere av informantene og deres virksomheter hadde allerede gjennomført risikoanalyser, i og med at flere av dem allerede hadde adoptert og gitt muligheten til hjemmekontor for sine ansatte.	Funn viser informantene og øverste ledelse er både informert, involvert og forstår sin rolle i arbeid med sikkerhet og sikkerhetskultur. Ingen av informantene har eget fokus på digital sikkerhetskultur, men generell sikkerhetskultur.
Virksomheter gjennomfører liten eller ingen endringer i opplæringsprogram som følge av en uønsket hendelse – Nedstengning og en ustrukturert bruk av hjemme og hybridkontor ses på i denne sammenheng som uønsket.	Studier viser at regler for informasjonssikkerhet bevist brytes, og man ser en oppgang fra 13% i 2019 til 16% i 2020. Det er ikke identifisert om denne økningen skyldes hjemme- eller hybridkontoret, men økningen er størst fra 2019 til 2020 kontra foregående år.	En overvekt av informantene nevner viktigheten av korrekt eller god adferd i sammenheng med en god sikkerhetskultur.	Nasjonale aktører er bekymret for at den raskere digitalisering som enkelte virksomheter har gjort har medført at midlertidige digitale tjenester nå er blitt permanente, og at det dermed ikke er gjennomført tilfredsstillende risikoanalyser av de digitale tiltakene.	HR- og HMS-informantene utviser annen forståelse av behovet for å ta i bruk ledelsesmetodikker og hvordan disse må endres som en følge av utbredelse av hjemme og hybridkontoret, enn informantene med teknisk bakgrunn.
Studier gjennomført av en offentlig instans, viser at en stor overvekt (70%) av respondentene ikke har mottatt organisert opplæring i informasjonssikkerhet de siste 2 årene.			Funn gjort i offentlige studier, viser at det er en oppfattelse at den digitale risikoen har økt for samfunnet, men de samme respondentene oppfatter ikke at den samme risiko gjelder for dem i samme grad.	
De hendelsene som er blitt avdekket, kobles i stor grad opp mot den ansatte kompetanse, adferd eller holdninger – eller mangler ved disse faktorene			Funn gjort i offentlige studier, viser at oppfattelse og forståelse av risiko er større blant respondenter med høy utdanning enn med lavere utdanning.	
			Nasjonale aktører er bekymret for manglende forståelse av digital risiko i norske bedrifter.	

Tabell 5 Oppsummering av funn del 2

6. Drøfting

I dette kapitelet diskuteres de empiriske funn opp mot de teoretiske perspektivene som er valgt, og forskningsspørsmålene vil bli forsøkt besvart.

Dette kapittelet vil følge kapittel 5. Mengden elementer som tas opp anses som nødvendig for å kunne skape en god drøfting rundt digital sikkerhetskultur ved hybridkontorløsninger. Når det er sagt, så ble det tidlig tydelig hvordan mange av disse temaene er veldig tett koblet sammen, og det vil på flere stedet i drøftingen være referanser på tvers av kapittelet.

6.1. Sikkerhetsutfordringer på hybridkontoret

«Hvilke digitale sikkerhetsutfordringer opplever/opplevde virksomheter som en følge av nedstengningen grunnet koronatiltakene og hybride kontorløsninger?»

Det kommer frem gjennom oppgaven og andre sekundærkilder, at sikkerhet på hybridkontoret er noe uavklart og virksomhetene har gjerne et utydelig bilde av hva det kan bety for sikkerheten. Det at flere informanter valgte å trekke seg fra oppgaven fordi de ikke så nødvendigheten av å gjøre noen grep relatert til hybridkontoret, da de ikke kunne se at hybridkontoret medførte nødvendige endringer i metodikk eller tiltak kan muligens bekrefte denne noe uklare forståelsen risikoer forbundet med hybridkontor.

Sett fra en konfidensialitet, integritet og tilgjengelig (KIT) perspektiv, så trekker informantene i ulik grad frem at det er spesielt konfidensialitet og integritet som er utfordrende på hybridkontoret. Man mister vesentlige elementer av kontroll og styring av ansatte som jobber fra ett hjemme- eller hybridkontor, og det er lett å se for seg at disse to perspektivene kan bli utfordrende å håndtere.

Som både NSM (2021) og Meld. St. 5 (2020-2021) påpeker, så viser funn ved tilsyn at det er en manglende risikoforståelse blant norske virksomheter, inklusivt på det digitale området. Dette kommer frem i samtaler med informantene, at de ikke har en aktiv holdning til eller har gjort noen dypere analyser av hvilke risikoer hybridkontoret kan utgjøre på lengre sikt.

Enkelte virksomheter har valgt å hente sine ansatte «hjem» til kontoret igjen, som en følge av denne usikkerheten for hvordan eller om de skal tilby hjemme- eller hybridkontor andre har besluttet å videreføre en mer eller mindre hybrid løsning. Grunnlaget for «å hente arbeidstakere hjem» er hos flere av virksomhetene forankret i ideen om at *«kulturen og arbeidstedet skapes på kontoret»* og at de ønsker at de ansatte skal være mest mulig på

kontoret for å ivareta kulturen. Validiteten rundt dette utsagnet om kultur og arbeidsstedet kan diskuteres, men utfra det eksisterende teoretiske grunnlaget om hvordan kulturer, sub- og makrokulturer oppstår (Bang, 2020; Bolman et al., 2014; Schein & Schein, 2017; Schein & Schein, 2016) kan denne type tilnærming vurderes som relevant.

En overvekt av informantene anser ikke hjemme- og hybridkontoret som en vesentlig sikkerhetsutfordring, men det er tydelig at informantene i all hovedsak gjør denne vurderingen utfra et digitalt, teknisk perspektiv. NSM sier i sin årlige rapport *Risiko 2021* (2021) at Covid-19 har vært med på å forsterke det eksisterende risikobildet for Norge, men at hjemme og hybridkontor ikke har introdusert nye trusler av teknisk karakter.

Flere av informantene påpeker, så vil det teknisk sett ikke være forskjell på om en ansatt bruker en eller fire dager på hjemmekontor i uken, da utfordringene og tiltakene i utgangspunktet er de samme. Både informantene og NSM påpeker at de nye utfordringene er mer relatert til ansattes endrende adferdsmønstre og den økte digitaliseringen. Til en viss grad har også digitale arbeidsmåter og tjenester blitt permanente, med de konsekvensene manglende langsiktig planlegging eventuelt kan føre til. Dette bør påvirke vurderinger av både robustheten til det digitale området, så vel som styring av arbeidsformer og adferd. Som studien gjennomført av OsloMET (Holm Ingelsrud & Hoff Bernstrøm, 2021) viser, så angir en overvekt av respondentene at de ønsker en videreføring av hjemmekontoret, eller som mange nå definere det som «den nye normalen». Det blir dermed nærliggende å vurdere det dithen at hjemme- eller hybridkontoret er kommet for å bli i en eller annen form.

I denne oppgaven ser vi at et fåtall av virksomhetene har sett en økning i antall uønskede digitale hendelser der hjemmekontorløsningen blir sett på som årsaks givende. De fleste uønskede hendelsene som har oppstått, knytter man til brudd på retningslinjer, prosesser og andre typer arbeidsbestemmelser av forskjellige karakter (Næringslivets sikkerhetsråd, 2020). Det var et noe uventet funn, da det forelå en forventning fra min side med å finne en økning i uønskede hendelser relatert til det tekniske aspekt ved hjemme- eller hybridkontoret. Det har også over de siste xx årene blitt rapportert en økning i digitale trusler, blant annet bedrageriforsøk. Men informantene til denne oppgaven har vært tydelige på at for dem, fra et teknisk perspektiv, vil det være de samme tiltakene som må settes i verk uavhengig av antall dager på hybrid- og hjemmekontor, da teknologien uansett er den samme. Dette bekreftes muligens av det (Andrade et al., 2020; FBI, 2021) fant. Selv om man så en økning på flere hundre prosent med for eksempel spam, phising, med korona som en innfallsvinkel, så uteble

de store tekniske uønskede hendelsene. Uteblivelsen av de store tekniske hendelsene kan sannsynlig tilskrives at de ansatte fulgte etablerte prosesser for hvordan håndtere phising og spam da phising o.l er noe de fleste virksomheter har hatt søkelys på, og det er ofte inkludert den grunnleggende opplæringen til ansatte. For øvrig kommer det frem i offentlig tilgjengelig kilder som NSM (2021), NorSIS (2020) m.fl, er at usikkerheten ved de tekniske løsningene skaper en viss bekymring. På generelt grunnlag har det vært en stor økning i antall uønskede hendelser, men disse kan ikke kobles til hjemme- eller hybridkontoret som den utløsende faktor, noe som sammenfaller med det informantene sier.

Det pågår kontinuerlig automatiserte angrep fra forskjellige aktører, hvor IP-adresser som er direkte tilgjengelig fra internett blir utsatt for et kontinuerlig angrep (Figur 6, s.44). Angrepene retter seg ikke bare mot enheter som router, brannmur etc., men også IOT-enheter (internet of things). Trusselaktører skanner etter mulige endepunkter som er tilgjengelige via internett og som kan inneholde sårbarheter, eksempelvis på grunn av manglende oppdatering. Når en ansatt befinner seg på en kontorlokasjon blir slike endepunkter oppdatert av arbeidsgiver, mens når ansatte sitter hjemme kan disse endepunktene både være feil konfigurert, ha dårlige passord eller ikke være oppdatert. Dette kan utgjøre digitale sikkerhetstrusler. Det er viktig å påpeke at dette ikke er en ny trussel, den har alltid vært der, men det blir forsterket med at den ansatte nå i større grad sitter hjemme eller andre lokasjoner som kan være sårbare. Dette kan være med på å øke den angrepsflaten en trussel aktør kan benytte seg av i et angrep. Et slikt vellykket angrep kan videre bli utnyttet i en sammensatt trussel mot andre elementer i en verdikjede hos en virksomhet eller dennes kontakter (kunder m.fl.) Et konkret og nyere eksempel på dette, er Solarwinds som opplevde at en trusselaktør kompromitterte kildekoden til programvaren levert av firmaet, og som deretter ble solgt videre til andre (Department of homeland security, 2021). Dette er noe som bekymrer både NSM og PST (Norsk senter for informasjonssikring, 2021b; Politiets sikkerhetstjeneste, 2021) og man kan se at dette har fått større fokus fra 2020 til 2021 i rapportene til begge disse instansene. Trusselaktører angriper med andre ord ikke lenger bare hovedmålet sitt, men forsøker å benytte seg av utilstrekkelig sikkerhet hos eksempelvis underleverandører. Denne problematikken er informantene bevisst på, men som tidligere nevnt, hybridkontoret anses ikke som en større teknisk trussel eller risiko enn hjemmekontoret.

Til tross for, eller kanskje på grunn av, kommer det imidlertid ikke frem fra noen av informantene at det er gjennomført detaljerte risikoanalyser for utvidet bruk av hjemme-/hybridkontor. Dette er sammenfallende med NSM (Nasjonal sikkerhetsmyndighet, 2020)

sine funn knyttet til manglende risikoforståelse blant norske virksomheter. Det var varierende grad av forståelse rundt risiko og risikoforståelse som utkrystalliserte seg tidlig i dialogen med informantene, og dette vi ser også lignende funn i komparative studier (Gunnes, 2021).

Et stort tema i diskusjonen med informantene ble i flere av tilfellene utfordringer med ansattes holdninger og adferd til hvordan de kan jobbe trygt, sikkert og effektivt på en annen lokasjon enn det tradisjonelle kontoret. Dette kan ses i sammenheng med at de uønskede hendelsene som ble rapportert var mer knyttet til brudd på prosedyrer enn til tekniske svakheter. Funnene gjort i denne oppgaven peker i retning av at utfordringene ved hjemme- og hybridkontoret ikke bare ligger i det tekniske perspektivet. men også er relatert til kulturelle aspekter, den ansattes adferd og holdninger og lederatferd og -strategi.

For å svare på forskningsspørsmålet, så kan en si nedstengningen, koronatiltakene og hybridkontoret har bidratt til å øke både risikonivået og digitale sikkerhetsutfordringer for norske virksomheter. Utfordringene har til en viss grad teknisk karakter, men også den menneskelige faktoren må tas med i vurderinger og tiltak.

6.2. Vedlikehold av digital sikkerhetskultur ved hybride kontorløsninger.

«Hvordan kan den ansattes kunnskap, adferd og holdninger påvirke digital sikkerhetskultur i en hybrid kontorsituasjon?»

Gjennom forstudien og prosjektskissen til denne oppgaven, oppstod det tidlig en hypotese om at enkelte elementer av den digitale sikkerhetskulturen vil utprege seg som mer relevante enn andre. Dette dannet utgangspunktet for problemstillingen.

I kapitel 3.6, ble strukturen for digital sikkerhetskultur og dens åtte hovedkomponenter presentert. Disse kan summeres og kategoriseres i følgende elementer:

- Holdninger til digitalisering og digital sikkerhet
- Risikoforståelse
- Holdninger til styring og kontroll
- Sikkerhetsadferd
- Kunnskap, læring og interesse.

En sammenstilling av disse kategoriene og hvordan de sammen danner en digital sikkerhetskultur kan en også se i figur 4 på side 29.

6.2.1. Holdninger til digitalisering og digital sikkerhet

Som teorier påpeker (Bang, 2020; Reason, 1997) er en kultur noe som oppstår gjennom felles verdier, holdninger og mål. Schein (2009) påpeker videre at *«Kultur er et mønster av grunnleggende antakelser utviklet av en gitt gruppe etter hvert som den lærer å mestre sine problemer med ekstern tilpasning og intern integrasjon».* Man snakker med andre ord om artefakter som oppstår mellom mennesker i en grupper eller annen type fellesskap der man har interaksjoner – f.eks. på et arbeidssted. Et spørsmål som med dette blir tydelig, er hvordan skal en jobbe med kultur i en hybrid hverdag hvor folk sitter spredd og med potensielt store geografiske avstander? Det er mange elementer som må vurderes her, og i den videre drøftingen vil vi se på dette fra et digitalt sikkerhetskulturperspektiv.

Store deler av den norske arbeidsstokken var fra våren 2020 til høsten 2021 på hjemmekontor, i sånn omlag563 dager. Gjennom alle disse dagene samarbeidet ansatte i mange virksomheter kun gjennom digitale kanaler. De jobbet gjerne tettere med færre antall mennesker, og interaksjonen ble ofte begrenset til små grupperinger. Mens man tidligere i hovedsak hadde vært samlet på en eller noen få lokasjoner, og hvor subkulturene gjerne var større (Kaufmann & Kaufmann, 2015; Schein, 2009; Schein & Schein, 2017) oppstod det som en følge av nedstengningen et mulighetsrom for at mikrokulturer kunne vokse frem i større grad enn tidligere. Som Schein (2009) sier så er mikrokulturer mindre grupperinger som jobber tett sammen ut ifra prosjekt, nødvendighet eller lignende. Der en tidligere hadde grupperinger/avdelinger med sin egen subkultur så hadde en nå fått flere mikrokulturer. I disse mikrokulturene oppstår det egne måter og rutiner for hvordan man samarbeider og samhandler på best mulig måte. Det skaptes dermed ikke en sikkerhets-subkultur for en avdeling, men heller en fremvekst av mikrokulturer i mye mindre grupper, med egne «regler» for hvordan samhandle digitalt. En slik utvikling medfører potensielt en digital sikkerhetskultur fra en mikro kulturperspektiv. Dette kan videre føre til at det skapes en kultur som avviker fra den øvrige organisasjons- og sikkerhetskulturen og dermed skaper en mulighet for at det lettere kan oppstå uønskede hendelser.

6.2.2. Risikoforståelse

Gjennom intervjuene med informantene og andre komparative kilder kommer det frem at risikooppfattelsen er til stede, men i varierende grad. Eksempelvis er alle informantene innforstått med at det er forbundet risiko med bruken av hjemme- og hybridkontoret. Få av

informantene vurderer hybridkontoret ut ifra ett langsiktig perspektiv og hvilken risiko denne bruken kan ha på lengre sikt. Man oppfatter ikke hybridkontoret slik sett som forskjellig fra hjemmekontoret, man snakker bare om en forskjell i skala og mengde. De langsiktige aspektene drøftes og reflekteres det rundt i større grad av informantene som ikke har et teknisk utgangspunkt eller grunnlag. Risikooppfattelse og forståelse er absolutt til stede hos samtlige av informantene, men som Sjöberg og Drottz-Sjöberg (2008) påpeker, så oppfattes risiko forskjellig fra individ til individ og basert på deres egen kompetanse og erfaringer. Her er det en vesentlig forskjell på hvordan informantene med teknisk bakgrunn oppfatter risiko og hvordan HR/HMS informantene ser andre aspekter også, i dette tilfellet en større grad av psykososiale elementer og utfordringer.

Som både NSM (2021), PST (2021) og andre instanser er tydelig på, har den økte takten og graden av digitalisering medført ett mer komplisert trussel bilde og en økt angrepsflate. Risikoen forbundet med dette deles av at et flertall av informantene. Bekymringen for at digitaliseringen går for raskt deles av flertallet, men det settes ikke inn i en kontekst av hjemme- og hybridkontoret. Dette kan være av flere årsaker, uten at oppgaven gir noe direkte svar på dette, men usikkerheten og bekymringen deles av informantene. Videre, som tidligere beskrevet, var det ingen av informantene og deres virksomheter som anga at de hadde gjort nye eller utvidede risikoanalyse av forhold knyttet til hjemme- eller hybridkontoret. De fleste hadde bare gjennomført mindre re-vurdering av eksisterende risikoanalyser gjerne utarbeidet i sammenheng med introduksjon av nye digitale samhandlingsløsninger som Microsoft 365, «for å se om vi hadde glemt / oversett noe» som kunne være relevant for situasjonen de befant seg i ved nedstengningen. ISO 31004 (Norsk Standard, 2013) sier «…. *En risiko oppstår eller endres når beslutninger tas. Siden det nesten alltid er noe usikkerhet assosiert med beslutninger eller når beslutninger tas, så vil det nesten alltid være risikoer til stede …».* Av dette kan man påstå at å ikke ta en beslutning er også å ta en beslutning.

Deler av hypotesen for denne oppgaven omhandler den ansattes holdninger, adferd og kompetanse, digital sikkerhetskultur på hybridkontoret. Sett i lys av denne hypotesen kan man vurdere det dithen at virksomhetens kan kompetanse rundt risikovurderinger, oppfattelsen av disse og hvordan disse kan påvirke virksomheten være avgjørende for det videre i arbeidet med digital sikkerhetskultur og generelt sikkerhetsarbeid. Oppfattelsen etter intervjuene og gjennomgang av datagrunnlaget er at virksomhetene har en vei å gå før de kan påstå at de har en tilfredsstillende forståelse av det totale risikobildet som følger hybridkontorløsninger. En slik forståelse vil være nødvendig for å bedre kunne gi ansatte

riktig kompetanse, slik at den ansatte kan ta mer kvalifiserte avgjørelser i den digitale sfæren når de arbeider fra hybride kontorløsninger.

6.2.3. Synet på styring og kontroll

Jacobsen og Thorsvik (2016) forteller at «*ledelse er en spesiell atferd som mennesker utviser i den hensikt å påvirke andre menneskers tenkning, holdning og atferd».* Det er ledelsen sitt ansvar å etablere strategien, visjonen, og retningen for virksomheten gjennom kontroll og styring. Dette gjelder ikke bare for hvordan verdiskapningen skal oppnås - også sikkerhet og sikkerhetskultur er et ledelsesansvar og ledelsesansvar trekkes frem i de fleste teorier om sikkerhetskultur (Nettvett, 2021; Norsk Standard, 2017; Perrow, 1999; Reason, 1997; Westerman, Soule & Eswaran, 2019). En del av hypotesen til denne oppgaven er rettet mot den ansatte adferd, holdninger og kompetanse innen digital sikkerhetskultur ved hybride kontorløsninger. Det som er viktig å ta med seg videre er det faktum at den ønskede adferden, holdningene og kompetanse ikke er mulig å tilrettelegge for, å styre eller endre, med mindre det finne et tydelig eierskap hos ledelsen. Bergsjø et al. (2020, s. 43) er klar på dette og påpeker følgende;

«Arbeid med digital sikkerhetskultur er ledelsens ansvar, men arbeidet innebærer at alle som er en del av fellesskapet bidrar. Siden sikkerhetskultur består av så mange ulike dimensjoner, betyr det arbeidet med slik kultur også må være helhetlig»

Ifølge informantene viser ledelsen en forståelse for at sikkerhet er viktig, og at det arbeides dedikert og blir satt søkelys på sikkerhetskultur. På spørsmål om de anså sikkerhetskultur og digital sikkerhetskultur som det samme eller noe ulikt, var det en delt enighet om at den digital sikkerhetskultur er en del av den organisatoriske sikkerhetskultur. Ingen av informantene kunne bekrefte et direkte fokus på digital sikkerhetskultur som et eget moment.

Som en av informantene påpekte, så er sikkerhetskompetanse noe virksomhetsledelsen ikke nødvendigvis besitter. Dette gjelder spesielt i små og mellomstore bedrifter, som har begrenset med midler til å sette søkelys på sikkerhet i utvidet grad. Som en informant sa: «*Gjerne har en virksomhet/organisasjonsleder vært på ett kurs, og fått noen tips på at informasjonssikkerhet er nyttig.».* Selv om situasjonen nødvendigvis ikke er gunstig, så har det vært en modning på området, og sikkerhet er mer på dagsorden i ledergrupper og i styrer enn for bare ett par år siden. Som en annen informant påpeker om ledelsens eierskap og forståelse av sikkerhetskultur «*På generelt grunnlag ja, men en kan spole tilbake bare tre år*

tilbake i tid, så var situasjonen en annen. Noe som har modent, generelt, over tid.». Det er tydelig at informantene og deres virksomheter har en strategi for sikkerhet og sikkerhetskultur, men en bevisst tilnærming til digital sikkerhetskultur som en egen faktor, er tilsynelatende fraværende.

Utglidning i lojalitet og innside problematikken

Et element som kommer frem fra flere nye rapporter utarbeidet av myndighetsorganer i Norge (Nasjonal sikkerhetsmyndighet, 2021a; Norsk senter for informasjonssikring, 2021b; Politiets sikkerhetstjeneste, 2021), er en økende bekymring for illojale arbeidstakere og en generell innside problematikk. I risiko 2021 (NSM, 2021a) beskrives en innsider, som en nåværende eller tidligere ansatt, konsulent eller innleid som har hatt legitim tilgang til en virksomhet. Denne tilgangen kan utnyttes av eksterne aktører via vedkommende som er innsider, og utnyttes i kriminelle aktiviteter eller er av statlige aktører. Dette kan utgjøre en trussel mot Norge som en suveren nasjon, eller mot enkeltvirksomheter.

Det disse rapportene (Nasjonal sikkerhetsmyndighet, 2021a; Norsk senter for informasjonssikring, 2021b; Politiets sikkerhetstjeneste, 2021) viser, er at illojalitet og innsideproblematikken har økt de senere år. At dette potensielt vil utgjøre en risiko for ansatte som bruker hybride kontorløsninger i stor grad, er åpenbart. Dette kan man observere gjennom nyere forskning (Holm Ingelsrud & Hoff Bernstrøm, 2021), som viser at ansatte mister evne til å skille mellom privatliv og jobb. Denne problemstillingen er også nevnt i kapitel 6.1, da en slik utglidning på sikt kan bidra til at det oppstår overtid en redusert følelse av virksomhetstilhørighet og en generell lojalitet til arbeidsgiver. Et av tiltakene som anbefales av NSM i deres rapport (2021a) er at det gjennomføres tiltak for å øke sikkerhetsbevisstheten til ansatte og ikke minst tiltak for å etablere en god sikkerhetskultur. En ser med andre ord at styring og kontroll fra ledelsen kan spille en avgjørende rolle med tanke både på en god sikkerhetskultur, men også med tanke på den digitale sikkerhetskulturen ved hybride kontorløsninger.

Ledelse av ansatte på hybridkontor

Ledelsesperspektivet har gjennom denne oppgaven vist seg å bli sentralt, og det reflekteres også i den grunnleggende hypotesen. Problemstillingen *Hvilke elementer ved digital sikkerhetskultur bør virksomheter prioritere ved hybride kontorløsninger?* tar utgangspunkt i antakelsen om at arbeidsgivere vil måtte fokusere og arbeide annerledes med den digitale sikkerhetskulturen på hybridkontoret kontra det tradisjonelle kontoret. Det vil stilles andre,

og gjerne høyere, krav til ledelsen. Som det kommer frem både i de empiriske funnene og i drøftingen, spiller ledelsen en helt sentral rolle og vil være avgjørende for hvordan en arbeidsgiver skal lykkes i sitt arbeid med digital sikkerhetskultur ved hybride kontorløsninger. Man vil ikke klare å opprette holde den adferden eller holdningene som ønskes uten en tydelig ledelse. Da er det avgjørende for en arbeidsgiver å tilrettelegge for dette på en effektiv måte. Utfordringen til flere virksomheter vil for øvrig ligge i behovet for å endre ledelsesmetodikk og -tilnærminger for å oppnå ønsket effekt.

Utfordringer knyttet til ledelsesmetodikker ble spesielt tydelig i dialogen med informantene som ikke hadde en teknisk bakgrunn eller representerte en IT-funksjon. HR og HMS informantene var i større grad innforstått med utfordringen knyttet til ledelse av ansatte på hybridkontor. Som informant I1 var tydelig på «*Ledere måtte over på en mer strukturert dialog (for ansatte på hjemmekontoret). Det finnes eksempler på at leder «glemte» å snakke med sine ansatte på fjorten dager. Da de ikke har den rette strukturen på plass (for å håndtere en slik situasjon). Disse lederne har tidligere hatt en oppfattelse (følt) hvem som har hatt et behov / sett hvem som har hatt ett behov – Dette forsvinner når en sitter på hjemmekontor. En må dermed ta et mer aktivt grep om situasjonen.»*

Det skal sies, at enkelte av de «tekniske» informantene, også diskutere dette til en viss grad, men dette var i hovedsak informanter som var organisert i en struktur utenfor IT-funksjonen. Hybridkontoret stiller med andre ord andre krav til ledelse enn hva man har erfaring med fra tidligere. I en situasjon der hjemmekontor benyttes en gang iblant, så vil det ikke nødvendigvis være behov for endret lederadferd og -metodikker, men ved hybridkontoret er det klare indikasjoner på at ledere må håndtere situasjonen annerledes.

Utstrakt brukt av hybridkontoret føre til at man får et større antall mikrokulturer man må forholde seg til. En kan med andre ord ikke bare lede på et «overordnet nivå», men man må se enkeltindividene på en annen måte, ref. informanten over. Ser vi til teorien om situasjonsbestemtledelse av Blanchard og Hersey (Jacobsen & Thorsvik, 2016; Kaufmann & Kaufmann, 2015; Store Norske leksikon, 2021b), så legger den til grunn at ledelse må gjennomføres ulikt i ulike situasjoner, med utgangspunkt i både oppgavens art, men også med utgangspunkt i den ansattes egenskaper og relasjon til lederen. Et hybridkontor kan sies å være en slik situasjon som i større grad krever fleksible ledere, hvor den enkelte ansatte ledes ut ifra den situasjon og behovet hen har. En leder for ansatte på hybridkontor, må i større grad identifisere de forskjellige behovene til en ansatt, og tilpasse om de skal være deltagende,

overtalende, delegerende eller instruerende i sin lederstil – tilpasset den ansattes modenhet og behov. En slik tilnærming kan tenkes å i større grad imøtekomme problematikken med at den ansatte får en utglidning i lojalitet og firmatilhørighet ved at de for eksempel føler seg sett av nærmeste leder. For noen ledere vil en slik tilnærming kunne være utfordrende, og det er også en av utfordringene ved denne teoretiske tilnærmingen. Kaufmann & Kaufmann (2015) påpeker blant annet utfordringen ved at ledere må ha evne til å tilpasse sin lederstil utfra de betingelsene som gjelder under de gjeldende forholdene og situasjonen som råder.

Et eksempel på ledertilnærming som kan bli utfordret er nødvendigheten av at det eksisterer en grunnleggende tillit til arbeidstakere på hjemme- og hybridkontor. For at ansatte skal kunne arbeide fra et hjemme- eller hybridkontor, fordrer dette at arbeidsgiver har tillit til at arbeidstaker faktisk utfører sine oppgaver iht. gjeldende arbeidsavtaler. Samtidig er utglidningen av fokus, lojalitet og den manglende følelsen av firmatilhørighet, som tidligere nevnt, en utfordring som må tas alvorlig fordi dette potensielt kan lede til sikkerhetsutfordringer.

Tillit er både ett viktig moment i den digitale sikkerhetskultur, men også ifølge Bård Kuvaas (Kuvaas, 2017a, 2017b). Kuvaas (2017a, 2017b) mener at det er viktig å skape ett grunnlag for indre motivasjon hos den ansatte. En indre motivasjon danner grunnlag for en adferd som drives av et indre ønske om tilfredsstillelse, interesse, glede eller en oppfattelse av mening med de arbeidsoppgavene man har. Ansatte som drives av en ytre motivasjon (eksempelvis der økonomisk fordel er et insentiv) vil oftere kunne tenkes å bli offer for utglidning i lojalitet og tilhørighet, og dermed gi potensiale for uønsket adferd som for eksempel atferd relatert til innsideproblematikk.. Man kan se at et bevisst forhold til ledelse og ledelsesmetodikk kan gagne og understøtte ivaretakelse av både en god digital og generell sikkerhetskultur.

6.2.4. Sikkerhetsadferd

Reason (1997) sier at en god sikkerhetskultur er en informert sikkerhetskultur. En slik informert kultur sikkerhetskultur har søkelys på, og er rapporterende, rettferdig, fleksible og lærende. Samtlige av informantene drøfter dette i intervjuene, men de er klar over at det er ett stort lerret å bleke. Det vil ta tid, og vil kunne være krevende. Selv om Reason (1997) satte søkelys på organisatoriske uønskede hendelser, så er teoremet til Reason veldig gjeldende også for en og digital sikkerhetskultur, i et hybridkontor perspektiv. Som Reason (1997) fremhever, så er en fleksibel kultur viktig, og fleksibilitet er også et kjennetegn ved det å arbeide hybrid. En organisasjon blir mer robust om den er endringsvillig, og under

pandemien har man måttet kunne endre seg fra å være et hierarkisk til en mer flat organisasjonskultur. Det er også denne tilpasningsevne som vil kunne være avgjørende for om en organisasjon i det hele tatt vil kunne gjennomføre og tilby hybridkontor på en sikker og effektiv måte. Reason sin teori, er bare en av mange teorier det vil være viktig å se nærmere på. Westrum (2009) ser i større grad på sikkerhetskulturen utfra informasjonsflyten. Westrum (2009) sier blant annet at en organisasjon vil slutte å fungere om informasjonsflyten uteblir.

Skal en fatte en beslutning, vil en trenge informasjon. Westrum (2009) har definert tre typer sikkerhetskulturer, den patologiske, byråkratiske og den generative. Det er denne generative (s.23) sikkerhetskulturen, og hvordan den behandler informasjonsflyten som er med å på å forme sikkerhetskulturen og vil kunne bidra til å gjøre den til en god kultur. Som Westrum sier «*When there is lack of dialog, unpleasant things can happen". (Westrum & Adamski, 2009)*. Der en tidligere hadde ansatte tilgjengelig og fast på kontoret, med etablerte og tydelig kommunikasjonsrutiner så er dette ikke nødvendigvis like mye et problem. Har en dog ansatte som i stor grad arbeider hybrid, vil dette kunne by på utfordringer. Dette er også noe som kommer frem både fra informantene, men også fra f.eks. Mørketallsundersøkelsen (Næringslivets sikkerhetsråd, 2020) og komparative studier (Gunnes, 2021) hvor det kommer tydelig frem at kommunikasjonen fra leder til den ansatte på hjemme- eller hybridkontoret gjennom nedstengingen har vært mangelfull, og flere har følt seg forlatt og ei heller fått instrukser på hvordan de skal forholde seg til situasjonen. Kommunikasjon utpreger seg som en utfordringer i teorier som beskriver god digital sikkerhetskultur. Dette kan muligens henge sammen med at rammeverket rundt en digital sikkerhetskultur (Digitaliseringsdirektoratet, 2021b, 2021c; Nettvett, 2021) ikke er utviklet med tanke på en hybrid kontorhverdag.

Rapporten til NorSIS på digital sikkerhetskultur viser et meget interessant funn for 2020, og det er at 16% (en oppgang fra 13% i 2019) bevisst bryter regler for informasjonssikkerhet. Men samme rapporten viser også en oppgang fra 62% til 65% i samme periode. En gruppe som sier de ikke vet, går fra 25% til 19%. Om dette er en indikasjon på en negativ utvikling, vil en kun få et tydeligere svar på når rapporten for Nordmenn og digital sikkerhetskultur lanseres i slutten av november 2021. Uavhengig av dette, er så er det foruroligende at en kan se en økning i beviste brudd av informasjonssikkerheten.

Det er imidlertid verdt å merke seg at de tekniske uønskede hendelsene uteble selv om det ble kartlagt at informantene anga en økning i antall brudd på retningslinjer og prosesser.

Utfordringen slik en informant til denne oppgaven ser det, så ligger mye i det å ha ett kontor hjemme og ett kontor hos arbeidsgiver gir en utglidning av fokus, adferd eller holdning. Dette ser en også i studien til OsloMET (Holm Ingelsrud & Hoff Bernstrøm, 2021). Det ligger mye i sinnsstemningen til den enkelte ansatte og som vedkommende gjerne utvikler/har på de forskjellige lokasjonene. Mye av dette ligger nok i det at når ansatte er hjemme, har de en iboende trygghetsfølelse for at de befinner seg hjemme, og dermed gjerne er mindre overvåkne. Garden går gjerne ned. Den ansatte bruker gjerne enheter tilhørende arbeidsgiver annerledes når de sitter hjemme enn når de sitter på kontoret. Det kritiske blikket til den ansatte kan med andre ord bli noe mindre ved arbeid hjemme. Eksempelvis at en gjerne gjør mer «diverse» når en sitter hjemme og jobber, da garden som sagt senkes, og en ikke har de samme øynene over skuldrene fra andre kollegaer hjemme. Adferden og holdningene til den ansatte kan dermed utvikle seg i en negativ retning, da muligheten for kontroll og styring ikke er til stede på samme måten ved hjemmekontoret.

En stor del av en digital sikkerhetskultur fordrer at den ansatte utviser gode holdninger og en adferd som er i tråd med ønsket oppførsel. Det må tas aktive grep fra ledelse (kap.6.2.3), slik at de tydelig kan arbeide med å få frem den adferden som er ønsket.

Bergsjø et al. (2020) påpeker, så er arbeidet med en digital sikkerhetskultur et ansvar som ligger på ledelsen. Men ledelsen alene kan ikke få dette til. For at en skal lykkes med arbeidet rundt en digital sikkerhetskultur, så må også felleskapet bidra. En sikkerhetskultur, består av mange ulike dimensjoner, noe som betyr at arbeidet må være helhetlig (Bergsjø et al., 2020). Ser vi tilbake til en virksomhets subkulturer (kapitel 3.2), så består denne av 3 nivåer artefakter, verdier og grunnleggende antagelser (Schein, 2009). Det er spesielt verdier og grunnleggende antagelser som vil spille en rolle på den ansattes sikkerhetsadferd. Verdiene som en ansatt har, representeres som oftest gjennom en organisasjon verdier, målsetnings, visjoner m.m. Det er med andre ord verdigrunnlaget til virksomheten. Grunnleggende antagelser omhandler noe som ikke er taktilt. Det er gjerne hva en ansatte mener er riktig, hva som læres de nyansatte. Den kulturen som sitter mellom veggene til en virksomhet (Schein, 2009; Schein & Schein, 2017). Dette illustrer ansvaret som ligger virksomhetens ledelse for å aktivt jobbe med å skape ett grunnlag for en god sikkerhetskultur i en virksomhet. Det gjøres ikke over natten, og vil krever mye arbeid. Viktigheten av dette ansvaret som ligger på ledelsen, er at hybridkontoret vil potensielt kunne sette sikkerhetskulturen under press og bidra til en utvikling av en adferd som ikke er ønsket. Schein og Schein (2017) beskriver hvordan en subkultur kan utvikle seg på en slik måte at den kommer i direkte konflikt med

den overordnede organisasjonskulturen som virksomhetsledelsen jobber med. Ved hjemme- og hybride kontorløsninger vil det være viktigere enn noen gang at ledelsen (Schein, 2009) er til stede og har en forståelse av hvordan subkulturer fungere, og ikke minst som drøftet tidligere, problematikken med mikrokulturer som kan oppstå i et hjemme- eller hybridkontor perspektiv.

Det kan diskuteres om adferd sammen med ledelse er et av, om ikke det viktigste element i den digitale sikkerhetskulturen sett i lys av et hybridkontor. Men da er det viktig å være bevisst at adferd må ofte ses i sammenheng med den ansatte kompetanse, da adferd ofte har sitt utsprang derfra.

6.2.5. Kunnskap, læring og interesse

Både NorSIS (2020) og Bergsjø et.al (2020) er tydelig på at interesse for teknologi og IT er avgjørende for å få til god læring. Et interessant funn fra informantene og andre studier (Gunnes, 2021), viser at veldig få virksomheter gjennomførte endringer eller tiltak i form av opplæring for sine ansatte som ved start av pandemien måtte begynne å jobbe hjemmefra. Ser en til rapporten Nordmenn og digital sikkerhetskultur (2020) så oppgir hele 70% at de ikke har mottatt organisert opplæring i informasjonssikkerhet i løpet av de siste to årene. Samme rapporten (Norsk senter for informasjonssikring, 2020) viser også at 25% lærer enten gjennom å prøve å feil selv og 40% sier de lærer fra andre i en mer uformell situasjon. I en kontekst hvor en da gjennom store deler av 2020, hadde ansatte som ikke fikk organisert opplæring, og i vesentlig grad prøvde seg frem selv eller sammen med kollegaer kan dette gi grunnlaget for å påstå at man har skapt en tilstand der det lettere kan oppstå uønskede hendelser.

Skal den ansatte kunne identifisere en risiko eller trussel, så må den ansatte gjøres i stand til å gjøre dette med den rette kompetansen. I sammenheng med nedstengingen og hjemsendelse av de ansatte til hjemmekontoret, var det som nevnt få av virksomhetene representert ved informantene som gjennomførte noen konkret endring i sine opplæringsprogrammer. De fleste hadde allerede programmer og kilder som tilbys de ansatte, slik at den ansatte kan øke sin kompetanse. Dette gjøres enten via obligatorisk kvartalsvis/årlige kurs, men også som et tilbud den ansatte kan benytte seg av ved eget ønske/behov. Det som noe overraskende kommer frem, var at få endret sitt opplæringsprogram til å bedre være tilpasset ansatte som i vesentlig grad nå enten jobbet eller fremover ønsker å jobbe fra et f.eks. hybridkontor. En er her tilbake til risikoforståelse for hva et hybridkontor kan føre med seg av risiko, enten det

være forbundet med tekniske utfordringer, det psykososiale aspektet eller utfordringer konkret relatert til en digital sikkerhetskultur (Nasjonal sikkerhetsmyndighet, 2021a; Norsk senter for informasjonssikring, 2020; Næringslivets sikkerhetsråd, 2020) og hvordan denne settes under et annet press i en hybridløsninger kontra en kontorlokasjon. Alle virksomhetene i denne oppgaven representert via informantene, har som nevnt et opplæringsprogram, men den er tilsynelatende ikke tilpasset brukere av et hybridkontor i større grad. Grunnlaget for at ansatte skal være i stand til å ta god avgjørelsen i et hybridkontor situasjon, der hvor barrierer som en finner på kontoret ikke er til stede, ligger i nivået av kunnskapen. Kunnskap medfører mer informerte valg og beslutninger, noe som vil kunne bidra til bedret sikkerhet og adferd hos den ansatte.

7. Konklusjon

Etter nedstengingen og langvarig bruk av hjemmekontor for mange, står vi nå ovenfor *«den nye normalen»*. I denne nye normalen har hybridkontoret oppstått som begrep. Utgangspunktet for denne oppgaven var å se nærmere på om det var enkelte elementer av den digitale sikkerhetskulturen i en virksomhet, det ville være nyttig å ha økt oppmerksomhet på.

Hvilke elementer ved digital sikkerhetskultur bør virksomheter prioritere ved hybride kontorløsninger?

Det som kommer frem gjennom oppgaven er at kompleksiteten ved hybridkontoret vil kreve nye og andre organisatoriske grep, som mange virksomheter ikke hat att enda. Mange mangler et klart rammeverk for hvordan hybridkontor skal tilbys fra et organisatorisk ståsted. At en slik type arbeidsform er kommet for å bli, er det stor sannsynlighet for. Om dette vil bli definert som hjemme- eller hybridkontor gjenstår å se. Uavhengig av hva kontorløsningen vil bli definert som, vil det være risiko- og sikkerhetsutfordring forbundet med denne typen arbeid som en virksomhet og dens ledelse må være klar for å håndtere.

Innenfor digital sikkerhetskultur er det spesielt tre områder som utpeker seg som viktige i et hybridkontor kontekst.

Ledelsens rolle i en digital sikkerhetskultur: Rollen til ledelsen og dens tilstedeværelse vil være viktig i arbeidet med en digital sikkerhetskultur i en hybrid hverdag. Man bør blant annet arbeide med å etablere en forståelse og aksept hos ansatte for *hvorfor* dette arbeidet er viktig. Ledelsen må gå foran som gode eksempler, og tillit, god kommunikasjon, tydelige strategier, visjoner og verdier vil være grunnleggende faktorer. Dette bør etableres gjennom hele organisasjon, fra toppen og ned til «gulvet». I arbeidet med en god digital sikkerhetskultur er man avhengig av at alle bidrar, og det må derfor skapes en kultur som er tuftet på åpenhet, proaktivt arbeid, villighet fra hele virksomheten til å lære av sine feil og at alle har en stemme som blir hørt. På samme måte som en god sikkerhetskultur er alles ansvar, vil digital sikkerhetskultur også være alles ansvar. Videre bør ledelsen legge til rette for at ansatte kan forstå hva som er forventet av dem; hvis man ikke blir fortalt at man gjør noe «galt», så vil man fort fortsette med sin adferd i god tro.

Kompetanse: De ansattes kompetanse er avgjørende i arbeidet med digital sikkerhetskultur. For at de ansatte skal kunne være i stand til å forstå *hvorfor* og *hvordan* må de ansatte gis den kompetansen som er nødvendig for å innfri kravene. Kompetansehevingstiltakene må f.eks.

sette søkelys på grunnleggende konsepter som hva risikoene er, hva feil valg og handlinger faktisk kan medføre, men også innføring i retningslinjer og prosedyrer. Og for øvrig vil mest sannsynlig mange virksomheter tjene på å oppdatere sine retningslinjer for å tilpasse dem en hybrid arbeidshverdag. Slik vil det bli mulig for ansatte å analysere, forstå og vite hvordan de skal kunne jobbe *trygt, sikkert* og *effektivt* på et hjemme- eller hybridkontor

Adferd: Menneskers adferd er basert på det de har erfart eller lært. Det er gjennom økt bevisstgjøring og kompetanseheving mulig å utvikle de riktige holdningene. Men adferd kommer ikke alene av bevisstgjøring og kompetanse. Det vil kreve at ledelsen er til stede og er i tett dialog med de ansatte som jobber i en hybridkontor-kontekst. Det er mange gode grunner til at ledere vil tjene på å være tilgjengelig, tett på og tydelig i sin kommunikasjon, samt legge til rette for å skape de rette insentivene for ansatte.

Interessant nok kan det synes som at digital sikkerhet i konteksten av hybridkontor handler mer om å forme mennesker og atferd enn om teknologiske tiltak. Funnene i denne studien antyder at de teknologiske tiltakene for digital sikkerhet i seg selv, og styrken av dem, ikke endres betydelig av økt frihet til å utføre arbeidet utenfor de tradisjonelle kontorlokalene. Men når man endrer konteksten og omgivelsene mennesker jobber i, hvem de påvirkes av i arbeidshverdagen, og også lener seg på systemer som i større grad betinger tillit til at den enkelte handler og tar beslutninger sunne beslutninger for seg selv og virksomheten så må virksomhetene ta nye grep. Menneskelige faktorer kan se ut til å få større betydning for det digitale risikobildet, og da må risikoreduserende tiltak som retter seg mot menneskelige styrker og svakheter tas i bruk. Virksomheter som benytter hybridkontor vil tjene på å utforske hvordan de kan bygge en digital sikkerhetskultur ved å tilrettelegge for at ansatte blir gitt riktig kompetanse, forstår hvilken adferd som reduserer risiko og at ledere tar utgangspunkt i at nye organisatoriske utfordringer krever nye metoder og ledelsesstrategier.

8. Referanseliste

Akademikerne. (2021). *To av tre vil fortsette med hjemmekontor etter koronakrisen*. Hentet 08.12.2021 fra https://akademikerne.no/2020/to-av-tre-vil-fortsette-med-hjemmekontor-etter-koronakrisen

Andrade, R. O., Ortiz-Garcés, I. & Cazares, M. (2020, 27-28 July 2020). Cybersecurity Attacks on Smart Home During Covid-19 Pandemic. 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4),

Aven, T. & Renn, O. (2010). *Risk Management and Governance : Concepts, Guidelines and Applications* (1st ed. 2010. utg., Bd. 16). Springer Berlin Heidelberg : Imprint: Springer.

Bang, H. (2020). *Organisasjonskultur* (5. utgave. utg.). Universitetsforlaget.

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

Blaikie. (2010). Designing Social Research.

Blaikie, N. & Priest, J. (2019). *Designing social research : the logic of anticipation* (3rd edition. utg.). Polity Press.

Bolman, L. G., Thorbjørnsen, K. M. & Deal, T. E. (2014). *Nytt perspektiv på organisasjon og ledelse : struktur, sosiale relasjoner, politikk og symboler* (5. utg. utg.). Gyldendal akademisk.

Datatilsynet. (2021, 30.07.2021). *Iverksette styringssystem for informasjonssikkerhet, .* Hentet 08.12.2021 fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

De nasjonale forskningsetiske komiteene. (2021). *Forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teologi*. Hentet 08.12.2021 fra https://www.forskningsetikk.no/retningslinjer/hum-sam/forskningsetiske-retningslinjer-for-samfunnsvitenskap-humaniora-juss-og-teologi/

Dell Technologies. (2020a). *75 prosent har fremskyndet digitalisering under korona, .* Hentet 08.12.2021 fra https://www.delltechnologies.com/no-no/blog/75-prosent-har-fremskyndet-digitalisering-under-korona/

Dell Technologies. (2020b). *Digital transformation Index 2020, .* https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/briefs-summaries/dt-index-2020-executive-summary.pdf

Denzin, N. K. & Lincoln, Y. S. (2018). *The SAGE handbook of qualitative research* (5th. utg.). Sage.

Department of homeland security. (2021). *Solarwinds - Emergency Directive 21-01*. Hentet 08.12.2021 fra https://cyber.dhs.gov/ed/21-01/

Deutsche Telekom. (2021). *T-Pot*. Hentet 08.12.2021 fra https://github.com/telekom-security/tpotce

Digitaliseringsdirektoratet. (2021a). *Begrep: Informasjonssikkerhet*. Hentet 08.12.2021 fra https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet

Digitaliseringsdirektoratet. (2021b). *Veileder for kartlegging av digital sikkerhetskultur*. Hentet 08.12.2021 fra https://www.digdir.no/informasjonssikkerhet/veileder-kartlegging-av-digital-sikkerhetskultur/2142

Digitaliseringsdirektoratet. (2021c). *Veileder i kompetanse- og kulturutvikling innen digital sikkerhet*. Hentet 08.12.2021 fra https://www.digdir.no/informasjonssikkerhet/veileder-i-kompetanse-og-kulturutvikling-innen-digital-sikkerhet/2141

Direktoratet for forvaltning og økonomistrying. (2021). *Hvordan lede medarbeidere som sitter på hjemmekontor?* Hentet 08.12.2021 fra https://arbeidsgiver.difi.no/strategisk-hr-og-ledelse/koronaviruset-slik-bor-statlige-arbeidsgivere-forholde-seg/ledelse-under-koronakrisen/hvordan-lede-medarbeidere-som-sitter-pa-hjemmekontor

EenerWE Partner. (2017). *Alle satser på digitalisering, men ikke like mange vet hva det betyr*. Hentet 08.12.2021 fra https://enerwe.no/digitalisering-mynewsday-preben-carlsen/alle-satser-pa-digitalisering-men-ikke-like-mange-vet-hva-det-betyr/143853

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

FBI. (2021). FBI: Internet Crime Report 2020. *Computer fraud & security*, *2021*(4), 4-4. https://doi.org/10.1016/S1361-3723(21)00038-5

Fløvik, L., Lunde, L.-K., Vleeshouwes, J., Johannessen, H. A., Finne, L. B., Mohr, B., Jørgensen, I. L. & Christensen, J. O. (2021). Arbeid hjemmefra, helse og arbeidsmiljø. En systematisk kunnskapsoppsummering. I. Statens arbeidsmiljøinstitutt.

Forskrift om arbeid som utføres i arbeidstakers hjem. (2002). *Forskrift om arbeid som utføres i arbeidstakers hjem.* (FOR-2002-07-05-715). https://lovdata.no/dokument/SF/forskrift/2002-07-05-715

Grenness, T. (2020). *Slik løser du metodeproblemene i bachelor- og masteroppgaven* (1. utgave. utg.). Cappelen Damm akademisk.

Gunnes, T. (2021). Digital sikkerhetskultur i samfunnskritiske funksjoner - en studie av hva som kjennetegner digital sikkerhetskultur innen finans-, kraft- og jusitissektoren. I. Nord universitet. https://hdl.handle.net/11250/2789352

Holm Ingelsrud, M. & Hoff Bernstrøm, V. (2021). *Hjemmekontor: Utbredelse og sentrale kjennetegn våren 2021*. Arbeidsforskningsinstituttet - OsloMet. https://hdl.handle.net/11250/2756692

Jacobsen, D. I. & Thorsvik, J. (2016). *Hvordan organisasjoner fungerer* (4. utg. utg.). Fagbokforl.

Justis og beredskapdepartemenet. (2019). *Nasjonal strategi for digital sikkerhet*. Hentet 08.12.2021 fra https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

Justis og beredskapsdepartementet. (2020). *Meld. St. 5 (2020-2021) - Samfunnssikkerhet i en usikker verden*. https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf

Kaufmann, G. & Kaufmann, A. (2015). *Psykologi i organisasjon og ledelse* (5. utg. utg.). Fagbokforl.

Kommunsektorens organisasjon. (2021). *Pandemien har satt fart på digitaliseringen i kommunene*. Hentet 08.12.2021 fra https://www.ks.no/fagomrader/forskning-og-utvikling-fou/forskning-og-utvikling/pandemien-har-satt-fart-pa-digitaliseringen-i-kommunene/

Kreuter, M. W. & Strecher, V. J. (1995). Changing Inaccurate Perceptions of Health Risk: Results From a Randomized Trial. *Health Psychol*, *14*(1), 56-63. https://doi.org/10.1037/0278-6133.14.1.56

Kuvaas, B. (2017a). I *Tilitsbasert ledelse*. https://www.youtube.com/watch?v=lTI64TB3F_A

Kuvaas, B. (2017b). *Tilitsbasert ledelse virker*. Hentet 08.12.2021 fra https://www.bi.no/forskning/business-review/articles/2017/03/tillitsbasert-ledelse-virker/

Mydland, T. & McCabe, C. (2021). *Hvordan ivareta god sikkerhetskultur på hjemmekontoret?, .*

Nasjonal sikkerhetsmyndighet. (2016). *Alle organisasjoner har en sikkerhetskultur!, .* Hentet 08.12.2021 fra https://nsm.no/hold-deg-oppdatert/meninger/alle-organisasjoner-har-en-sikkerhetskultur

Nasjonal sikkerhetsmyndighet. (2019). *Råd og anbefalinger om passord*. Hentet 08.12.2021 fra https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord

Nasjonal sikkerhetsmyndighet. (2020). *Helhetlig digital risikobilde 2020*. https://nsm.no/getfile.php/134267-1601027852/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2020_1609_LR.pdf

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

Nasjonal sikkerhetsmyndighet. (2021b). *RISIKO 2021– helhetlig sikring mot sammensatte trusler*. https://nsm.no/getfile.php/136419-1616673370/Demo/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf

NBER - NATIONAL BUREAU OF ECONOMIC RESEARCH. (2021). *WHY WORKING FROM HOME WILL STICK*. https://www.nber.org/system/files/working_papers/w28731/w28731.pdf

Nettvett. (2021). *Digital sikkerhetskultur*. Hentet 08.12.2021 fra https://nettvett.no/digital-sikkerhetskultur/

Norsk akademis ordbok. (2021). *Hjemmekontor*. Hentet 08.12.2021 fra https://naob.no/ordbok/hjemmekontor

Norsk akademisk ordbok. (2021). *Hybrid*. Hentet 08.12.2021 fra https://naob.no/ordbok/hybrid_2

Norsk forening for arbeidsmedisin. (2021). Hjemmekontor. https://www.legeforeningen.no/contentassets/8109477866e44efb9329474733318b9f/ramazzini-01.2021.pdf

Norsk senter for forskningsdata. (2021). *Fylle ut meldeskjema for personopplysninger*. Hentet 08.12.2021 fra https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger

Norsk senter for informasjonssikring. (2016). *The Norwegian Cyber Security Culture 2016*. https://norsis.no/download/14669/

Norsk senter for informasjonssikring. (2019). *Nordmenn og digital sikkerhetskultur 2019*. https://norsis.no/download/17647/

Norsk senter for informasjonssikring. (2020). *Nordmenn og digital sikkerhetskultur 2020*. https://norsis.no/download/19381/

Norsk senter for informasjonssikring. (2021a). *Ett år med hjemmekontor: Mange bedrifter har for dårlige rutiner for å unngå kontokapring og hacking*. Hentet 08.12.2021 fra https://norsis.no/ett-ar-med-hjemmekontor-mange-bedrifter-har-for-darlige-rutiner-for-a-unnga-kontokapring-og-hacking/

Norsk senter for informasjonssikring. (2021b). *Trusler og trender 2021*. https://norsis.no/download/20115/

Norsk Standard. (2013). ISO 31004 Risikostyring - Veiledning til implementering av NS-ISO 31000. I.

Norsk Standard. (2017). ISO 27001 - Ledelsesystemer for informasjonssikkerhet. I.

Næringslivets sikkerhetsråd. (2020). *Mørketallsundersøkelsen 2020*. https://www.nsr-org.no/uploads/documents/Publikasjoner/Morketalls-2020-web.pdf

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. I.

Pedersen, K. S. & Ottestad, M. (2019). *Digital sikkerhetskultur i Norge - En studie av dokumenter utarbeidet av nasjonale aktører.* [Master, Universitet i Stavanger]. http://hdl.handle.net/11250/2628428

Perrow, C. (1999). *Normal Accidents - Living with High-Risk Technologies*.

Politiets sikkerhetstjeneste. (2015). *Trusselvurdering 2015*. Hentet 08.12.2021 fra https://www.pst.no/globalassets/artikler/trusselvurderinger/trusselvurdering-2015.pdf

Politiets sikkerhetstjeneste. (2021). *Trusselvurdering 2021*. Hentet 08.12.2021 fra https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/

Reason, J. (1997). *Managing the Risks of Organizational Accidents* (Kindle Edition. utg.).

Repstad, P. (2007). *Mellom nærhet og distanse : kvalitative metoder i samfunnsfag* (4. rev. utg. utg.). Universitetsforl.

Schein, E. H. (2009). *The corporate culture survival guide*. Jossey-Bass.

Schein, E. H. & Schein, P. (2017). *Organizational culture and leadership* (Fifth edition. utg.). Wiley.

Schein, E. H. & Schein, P. A. (2016). *Organizational Culture and Leadership*. John Wiley & Sons, Incorporated.

Schiefloe, P. M. (1999). *Kultur*. Allforsk. https://urn.nb.no/URN:NBN:no-nb_digibok_2009030604032

Sjöberg, L. & Drottz-Sjöberg, B.-M. (2008). RISK PERCEPTION BY POLITICIANS AND THE PUBLIC. *Energy & Environment*, *19*(3/4), 455-483. http://www.jstor.org.ezproxy.uis.no/stable/44397211

Standard Norge. (2018). ISO 31000 Risikostyring - Prinsipper og retningslinjer. I.

Statens arbeidsmiljøinstitutt. (2021). *STAMI med ny rapport om virkningene av hjemmekontor*. Hentet 08.12.2021 fra https://stami.no/stami-med-ny-rapport-om-virkningene-av-hjemmekontor/

Store Norske leksikon. (2019). *Digitalisering*. Hentet 08.12.2021 fra https://snl.no/digitalisering

Store Norske leksikon. (2021a). *Hybrid*. Hentet 08.12.2021 fra https://snl.no/hybrid

Store Norske leksikon. (2021b). Sitauasjonsbestemt ledelse. https://snl.no/situasjonsbestemt_ledelse

Thagaard, T. (2018). *Systematikk og innlevelse : en innføring i kvalitative metoder* (5. utg. utg.). Fagbokforl.

United States. Cyberspace Solarium, C. (2020). Cyberspace Solarium Commission. I. United States. Cyberspace Solarium Commission.

Westerman, G., Soule, D. L. & Eswaran, A. (2019). Building Digital-Ready Culture in Traditional Organizations. *MIT Sloan Management Review*, *60*(4), 59-68.

Westrum, R. (2014). The study of information flow: A personal journey. *Safety science*, *67*, 58-63. https://doi.org/10.1016/j.ssci.2014.01.009

Westrum, R. & Adamski, A. J. (2009). *Organizational Factors Associated with Safety and Mission Success in Aviation Environments*.

9. Vedlegg

9.1. Vedlegg 1 – Samtykkeskjema

Samtykkeerklæring

Jeg studerer master i risikostyring og sikkerhetsledelse ved Universitetet i Stavanger. Masteroppgaven min omhandler digital sikkerhetskultur i sammenheng med hybride kontor løsninger. I denne sammenheng ønsker jeg å intervjue nøkkelpersoner som innehar spisskompetanse og/eller besitter relevante stillinger. Spørsmålene vil sette søkelys på sikkerhetsledelse, sikkerhetskultur og digital sikkerhetskultur, trusler og sårbarheter samt kompetanse og opplæring.

Oppgaven vil mulig bli publisert på internett, av den grunn anonymiseres all informasjon som på noen måte kan identifisere deg eller din organisasjon/virksomhet. Alle koblingsnøkler vil bli lagret separat og i systemer supplert av Universitetet i Stavanger.

Jeg ønsker å ta opptak av samtalen for å skape en bedre dialog under selve intervjuet. Opptaket vil bli gjennomført med en analog tilkoblet opptaker, slik at igjen digital indikator kan benyttes for å identifisere deg eller din virksomhet. Alle opptak blir slettet/destruert så fort intervjuet er transkribert. Masteroppgaven har en foreløpig innlevering 21.11.2021. Når denne innlevering en fullført vil også alle notater m.m fra intervju også bli destruert/slettet.

Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Referat fra intervjuet vil bli oversendt til godkjennelse, slik at du kan gjøre evt endringer/tillegg om ønskelig.

Samtykke

Jeg har mottatt informasjon om studien, og er villig til å delta:

(Signatur informant, sted og dato)

9.2. Vedlegg 2 – Intervjuguide

Intervjuguide

Innledning

Praktisk informasjon vedr prosjektet

a. Samtykkeskjema
b. Selve intervjuet samt bakgrunnen for nøkkelkonsepter.
    - Hjemmekontor vs. Hybride kontorløsninger

Bakgrunn

1. Hva er din stilling i organisasjon?
2. Hvor er stilling innplassert, og hva er dine arbeidsoppgaver?

Trusler og sårbarheter

3. (På hvilken måte) anser du at dette trusselbildet har endret seg som en følge av Korona og fremtredelsen av hybrid/hjemmekontoret?
4. Anser du hybridkontoret som en større trussel/risiko for sikkerhetskulturen enn hjemmekontoret (ref. forskjell i definisjon)?
    - Hvis ja, på hvilken måte og hva ser du på som de/den største trusselen?
5. Som en følge av korona og økt bruk av hjemme/hybridkontor - har du/dere på noen måte vært «tvunget» til å endre tilgjengeligheten (fra hvor/når) av tjenester som brukes av de ansatte?
    - Eksempelvis, systemer som tidligere kun har vært tilgjengelig fra kontorlokasjoner.
6. I hvilken grad ble det gjennomført risiko / trussel vurdering av tjenestene som ble endret og/eller publisert?
    - Hva var til slutt utslagsgivende/avgjørende for at det ble gjennomført?
7. Har dere sett en økning i antall uønskede hendelser som en følge av økningen i bruken av hjemme/hybrid kontor?

Kompetanse og opplæring

8. NorSIS og flere andre aktører påpeker kompetanse som en av de viktigste faktorene for å unngå uønskede hendelser, men et hovedmoment innen digital sikkerhetskultur. Hvordan er dette tilrettelagt i din organisasjon?
    - Er det lagt opp til egen opplæring med fokus digital sikkerhet(kultur)?

9. Hvordan evt. har dere endret opplæringen som følge av hjemme/hybridkontor?
    - Endret som i annet fokus området – Type phising etc.
10. Har, og i så fall hvordan har arbeidet med digital sikkerhetskultur endret seg som en følge av Korona/hybridkontoret?
11. Hvordan foregår opplæringen og hvordan er den tilgjengelig for den ansatte?
    - Eksempelvis Self-service, online, on-demand etc.
12. Hvor ofte / hvor mye tid får den ansatte bruke på opplæring / kompetansehevning?

Sikkerhetskultur og digital sikkerhetskultur

13. Hvordan definerer du sikkerhetskultur?
14. Hva anser du å være en god sikkerhetskultur?
15. Anser du sikkerhetskultur og digital sikkerhetskultur som to sider av samme sak, eller er det to forskjellige områder?
    - Evt. Hvorfor, hvordan?

Ledelse, sikkerhet og risikooppfattelse

16. Hvordan jobber toppledelse med sikkerhetskultur / digital sikkerhetskultur?
    - Er de bevisst sitt ansvar og sin rolle i dette?
17. I hvilken grad opplever du at toppledelsen er differensiere mellom digital sikkerhetskultur eller vil du si at toppledelsen oppfatter digital sikkerhetskultur kun som sikkerhetskultur?
    - Har dette endret seg (fra ledelse) som en følge av økt hjemmekontor/hybridkontoret?

    Hvilke evt. (nye) retningslinjer har ledelsen gitt for videre sikkerhetsarbeidet sett utfra en hjemme/hybridkontor problematikk?

Avslutning

18. Noe som du ønsker å tilføye?