Cybersikkerhet

Et spill i kontinuerlig utvikling

Siren Dysvik

Masteroppgave i kriminologi
Institutt for kriminologi og rettssosiologi
Juridisk fakultet

UNIVERSITETET I OSLO

VÅR 2021

Cybersikkerhet

Et spill i kontinuerlig utvikling

Cybersikkerhet – Et spill i kontinuerlig utvikling

Siren Dysvik

http://www.duo.uio.no/

Trykk: Reprosentralen, Universitetet i Oslo

Sammendrag

Tittel: Cybersikkerhet – Et spill i kontinuerlig utvikling
Forfatter: Siren Dysvik
Hovedveileder: Helene O. I. Gundhus
Biveileder: Martin Nøkleberg
Levert ved: Institutt for kriminologi og rettssosiologi (UiO)

Cyberkriminalitet er en stadig voksende trussel og i ferd med å bli et reelt samfunnsproblem. Den teknologiske utviklingen har ført til at tradisjonell kriminalitet kan begås på nye måter, for eksempel ved bruk av internett. Cyberspace- miljøet hvor denne typen kriminalitet foregår åpner for tilkobling mellom flere enheter, fjerner geografisk avstand og gir mulighet for anonymitet og et høyt fortjenestepotensial. Fenomenet har videre ført til at cybersikkerhet har blitt en av topp-prioritetene på sikkerhetspolitiske agendaer over hele verden.

Formålet med denne avhandlingen er å undersøke hvordan gass- og oljeselskapet Wintershall Dea forebygger cyberangrep samt hvilke opplevelser og forståelser ulike grupper ansatte har av arbeidet. For å oppnå dette har fremgangsmåten bestått av individuelle intervjuer med syv informanter som innehar stillinger tilknyttet cybersikkerhet (eksperter), i tillegg til en spørreundersøkelse av vanlige ansatte som ikke er eksperter på området. Metoden har altså vært en kombinasjon av et kvalitativt og kvantitativt datamateriale for å besvare problemstillingen. Oppgavens funn presenteres hovedsakelig i lys av et teoretisk rammeverk som kan knyttes til teorier i kriminologien.

Funnene viser at fokuset på cybersikkerhet er større enn noen gang. Omfanget av trusler og mulighetene for nye typer trusler gjør at det er viktig for ekspertene å til enhver tid holde seg oppdatert på trusselbildet og utvikle kompetansen sin for å holde tritt med trusselaktørene. Sik blir det en konstant jakt etter sikkerhet. I den sammenheng uttrykkes det at det er en livsstil å arbeide med cybersikkerhet. Cyberangrep bli stadig mer målrettet og avansert på grunn av teknologiens hurtige utvikling. Dermed kan ekspertene aldri vite hvilken trussel de står ovenfor og kan utsettes for. Oppgavens funn illustrerer at ekspertene anvender en barrieretankegang med både tekniske og menneskelige barrierer for å forebygge cyberangrep. Det største fokuset er på de menneskelige barrierene og forstås i sammenheng med at cyberkriminelle de siste årene

har rettet søkelyset mot mennesker og det faktum at den menneskelige faktor er en større sårbarhet enn noensinne. Ansatte ses i denne sammenheng som «det svakeste punkt» og det brukes store ressurser på å lære dem opp i sikker atferd på internett og skape en bevissthet blant dem. Et stort fokus rettes mot å skape en god sikkerhetskultur i selskapet og faktorene tillit, dialog, ledelse og opplæring anses som særlig viktige. Funnene indikerer at det er krevende å lære opp ansatte i cybersikkerhet. De ansatte synes å forstå at cybersikkerhet er viktig og at cyberkriminalitet kan ramme alle. Slik sett virker ansatte å forstå risikoen cyberangrep utgjør. Likevel viser funnene at flere ansatte ikke gjør det de bør for å være sikre på nett blant annet ved at de bruker samme passord flere steder, ikke bytter passord jevnlig, og er usikre på hva de skal se etter for å gjenkjenne svindelforsøk. Avhandlingens funn tyder også på at flesteparten av de ansatte opplever en god sikkerhetskultur. Likevel fremkommer det at flere vegrer seg for å ta kontakt med IT-teamet og dette kan ha konsekvenser for om de rapporterer egne og kollegers brudd som igjen kan føre til uoppdagede angrep.

Å jobbe med cybersikkerhet synes å være et arbeid som aldri tar slutt. Ekspertene må stadig være oppdatert på trusselbildet og utvikle sin kompetanse for å holde tritt med potensielle lovbrytere som stadig finner nye måter å angripe på. Samtidig må ekspertene drive konstant opplæring av ansatte slik at de også er oppdatert på trusselbildet og forstår alvorligheten av cyberangrep. Slik ser cybersikkerhet ut til å være et spill i kontinuerlig utvikling og et kappløp mellom sikringssiden på den ene siden og trusselsiden på den andre.

Forord

Først og fremst vil jeg rette en stor takk til Wintershall Dea som inngikk et samarbeid med meg om min oppgave. En spesiell takk til Ole Martin Dahle, helse- miljø og sikkerhetsdirektør i selskapet, som har vært min kontaktperson. Jeg vil også takke alle informantene fra selskapet som stilte til intervju og deltok i spørreundersøkelsen. Uten dere hadde ikke dette blitt en oppgave. Jeg setter stor pris på deres delte tanker, kunnskap og erfaringer.

Tusen takk til hovedveileder Helene O. I. Gundhus. Jeg er svært takknemlig for ditt engasjement, din kunnskap og tilgjengelighet samt oppmuntrende tilbakemeldinger fra start til slutt. En ekstra spesiell takk til biveileder Martin som kom inn halvveis i prosjektet. Takk for at du satt deg inn i oppgaven på kort tid og for at du alltid har vært tilgjengelig siden. Dine gode innspill og råd har betydd veldig mye!

Jeg vil også takke familie og venner for all støtte og forståelse det siste året, både gjennom oppturer og nedturer. En spesiell takk til mamma og storesøster Kathrine for gode råd, hjelp og gjennomlesing. Til slutt vil jeg rette en stor takk til mine kjære studievenner ved IKRS, spesielt Marita og Helene. Denne prosessen hadde vært mye tyngre uten dere!

Oslo, juni 2021
Siren Dysvik

Innholdsfortegnelse

Figuroversikt

1 Introduksjon

Den teknologiske utviklingen går i et hurtig tempo og ny teknologi tas i bruk hver dag. Dette gir virksomheter gode muligheter for effektivisering og tilrettelegging. Men digitalisering fører også med seg trusler og sårbarheter som ikke er ønskelige (NSM, 2020). Utviklingen og avhengigheten av den globale informasjonsteknologiske infrastrukturen – cyberspace – har ført til at verden er sårbar på en ny måte (Muller, 2016). Samtidig som teknologi blir smartere og ny teknologi tas i bruk hver dag, økes mulighetene for potensielle lovbrytere til å utføre dataangrep. Slike angrep kan ramme både stater, bedrifter og individer, og har de siste årene blitt bedre organiserte og mer kostbare, og oppfattes dermed som farligere (Muller, 2016).

Et økende problem for private og offentlige virksomheter er at de på ulike måter blir utsatt for dataangrep. I 2019 ble Hydro rammet av et omfattende cyberangrep som påvirket hele selskapets globale organisasjon. Den totale kostnaden av angrepet er estimert til rundt 550-650 millioner norske kroner (Hydro, 2020). I 2017 ble det danske shipping-selskapet Mærsk utsatt for et dataangrep som kostet selskapet mer enn 2 milliarder kroner (Mark, 2019). Norske etterretningsmyndigheter advarer samtidig om en økning i digitale trusler rettet mot norsk industri og hendelser de siste årene viser at petroleumssektoren er blant de mest utsatte (Lysneutvalget, 2015). Digitaliseringen av denne sektoren foregår kontinuerlig og internett fører til flere enheter med digitale sårbarheter (Lysneutvalget, 2015). Slike angrep har store konsekvenser for selskaper. I 2018 brukte norske bedrifter 1,3 milliarder kroner på å rydde opp etter hackerangrep. Næringslivets sikkerhetsråd tror tallet er langt høyere, og at det digitale trusselbildet mot norske bedrifter er økende (Nilsen og Mjaaland, 2018). De siste årene er det observert en dreining fra angrep mot datamaskiner og nettverk, til angrep rettet mot enkeltpersoner (NSR, 2020: 78). Ettersom ansatte i organisasjoner oppgis som den største årsaken til sikkerhetsbrister som kan føre til dataangrep (Da Veiga, 2020) er kunnskap om trusler hos ledere og ansatte viktigere enn noen gang (NSR, 2020: 78).

Til tross for at det er en økning i kartlegging av omfang, er det ut fra min kunnskap lite empirisk forskning på temaet i norsk kontekst. Dette gjelder spesielt hvordan private bedrifter jobber med å forebygge cyberkriminalitet. For aktører som jobber med cybersikkerhet blir det viktig å anvende en risikotankegang for å være i forkant av truslene, for å slik kunne forebygge dem. I

tillegg blir det viktig å være i forkant på kompetanse for å møte kompleksiteten. Aktørene som jobber med cybersikkerhet må hele tiden være på banen for at kunnskapen deres ikke skal være udatert. Samtidig utvikler potensielle lovbrytere stadig nye metoder for å gjennomføre angrep ettersom teknologien stadig utvikler seg. Slik sett ser det ut til å være et spill i kontinuerlig utvikling mellom aktørene på sikringssiden og aktørene på trusselsiden. Denne masteroppgaven vil utforske hvordan sikkerhet håndteres og styres i en privat bedrift.

1.1 Problemstilling

I lys av det ovennevnte er jeg i denne oppgaven interessert i å undersøke fenomenet cyberkriminalitet gjennom å intervjue ansatte i gass- og oljeselskapet Wintershall Dea og deres arbeid med å forebygge den type kriminalitet gjennom cybersikkerhet. Fokuset er rettet mot hvilke menneskelige og organisatoriske faktorer som påvirker forebygging og cybersikkerhet. Utgangspunktet for oppgaven ligger i problemstillingen:

> *Hvordan forebygger Wintershall Dea cyberangrep? Og hvilke opplevelser og forståelser har ulike grupper ansatte av arbeidet?*

Wintershall Dea er valgt fordi cybersikkerhet er sentralt i en av Norges største gass-og oljeprodusenter. Selskapet er Europas ledende, uavhengige gass- og oljeselskap med aktiviteter over hele verden. Bedriften leter etter og produserer naturgass og råolje og har virksomhet i hele verdikjeden, fra leting via feltutbygging til produksjon og salg. Norge er et kjerneområde for Wintershall Dea og blant Europas viktigste energileverandører (Wintershalldea, 2020). Det er to grupper som er sentrale bidragsytere til empirien i avhandlingen. I Wintershall Dea Norge har IT-avdelingen det primære ansvaret for cybersikkerheten i selskapet. IT består av 7 ansatte og ca. 15 innleide som jobber med IT-drift og support. Ansatte i denne avdelingen vil utgjøre en gruppe av ansatte som undersøkes. I tillegg vil helse- miljø- og sikkerhetsavdelingen bidra med empiri om den overordnede beredskapen selskapet har rundt sikkerhet, inkludert cybersikkerhet. En siste sentral gruppe som bidrar inn i empirien gjennom en spørreundersøkelse, er vanlige ansatte, som ikke er eksperter på området. Til sammen skal dette gi data som kan si noe om hvordan cyberkriminalitet forebygges og håndteres gjennom fokus på cybersikkerhet.

1.2 Oppgavens oppbygging

Oppgaven er delt inn i seks kapitler. I kapittel to vil bakgrunn og tidligere forskning presenteres. Her vil det redegjøres for fremveksten av internett før fenomenene cyberkriminalitet og cybersikkerhet presenteres. Deretter vil det vises til noen spesifikke trender hva angår forskningsfokus innen disse to feltene. Til slutt i kapittelet vil mørketallsproblematikken innen utbredelsen av cyberkriminalitet gjennomgås.

I kapittel tre vises det først til litteratur om hvordan risiko og sikkerhet kan forstås i det moderne samfunn. Dette vil fungere som et bakteppe som videre kan bidra til å forstå hvordan cyberkriminalitet kan forebygges. Andre del av kapittelet presenterer oppgavens teoretiske rammeverk. Her beskrives først Michel Foucault (1991) sitt governmentality-begrep og David Garlands (1996) ansvarliggjøringsstrategi for å vise til ulike styringslogikker som kan anvendes av myndigheter for å styre og kontrollere samfunnet. Til slutt i kapittelet vil teori om kultur, sikkerhetskultur, nodal governance og situasjonell kriminalitetsforebygging presenteres for å belyse ulike mentaliteter og logikker for hvordan cyberkriminalitet kan styres og forebygges.

I fjerde kapittel vil studiens metode legges frem. For å innhente empiri er det anvendt flermetodedesign som betyr at oppgaven består av både et kvalitativt og et kvantitativt datamateriale. Her vil studiens fremgangsmåte og gjennomføring beskrives og valgene som er tatt begrunnes. Deretter vil analyseteknikkene som er benyttet presenteres før etiske refleksjoner og problemstillinger vurderes.

Kapittel fem er oppgavens analysekapittel. Her vil oppgavens empiriske materiale drøftes gjennom analyse og diskusjon. Kapitelet er delt i to deler. Første del presenterer hvilket trusselbilde Wintershall Dea må forholde seg til samt hvordan deltakerne i prosjektet forstår risiko og tusler i forhold til cyberkriminalitet. Andre del går dypere inn på hvordan de som jobber med cybersikkerhet forebygger cyberkriminalitet samt ansattes opplevelse av dette arbeidet.

Til slutt vil oppgavens hovedfunn trekkes frem og sammenfattes i kapittel seks, hvor jeg vil legge frem noen avsluttende refleksjoner. Avslutningsvis vil jeg også vise til hvilket bidrag oppgaven har gitt, samt forslag til mulige studier videre.

2 Bakgrunn og tidligere forskning

Fremveksten av cyberkriminalitet kan plasseres til veksten og utviklingen av internett (Yar og Steinmetz, 2019) som igjen kan forklare hvorfor cybersikkerhet har fått et stort fokus i samfunnet (Muller, 2016). Dermed vil dette kapittelet først redegjøre for fremveksten av internett før fenomenene cyberkriminalitet og cybersikkerhet beskrives. Deretter vil tidligere forskning presenteres for å redegjøre for eksisterende kunnskapsstatus innen feltene. Her vil det vises til noen spesifikke trender hva angår forskningsfokus. Til slutt vil mørketallsproblematikken innen cyberkriminalitet gjennomgås.

2.1 Fremveksten av internett

Siden midten av 1990-tallet har internett blitt et faktum for mennesker over hele verden, spesielt for de som bor i den vestlige industrialiserte verden (Yar og Steinmetz, 2019: 3-4). Tingenes internett er et raskt voksende fenomen som introduserer nye sårbarheter og risikoer (Norris mfl., 2015; Renaud mfl., 2020). *Tingenes internett, loT* eller *Internet of things* er et samlebegrep som handler om hvordan internett anvendes «for å koble sammen stadig flere autonome komponenter til et komplekst system». Alt som kobles til internett får muligheten til å kommunisere med hverandre og videre dele informasjon fra innebygde sensorer (NOU 2015: 13: 46). Digitalisering har på den ene siden gjort hverdagen til individer enklere samtidig som det er en driver for innovasjon, økonomisk vekst og produktivitet. På den andre siden skaper teknologien også nye sårbarheter og utfordringer (NOU 2015: 13: 43). De siste årene har internetts kriminelle dimensjoner fått stor oppmerksomhet, og cyberangrep har blitt en dagligdags forekomst (Renaud mfl., 2020). Utviklingen av internett har ført til at flere mennesker i dag blir ofre for cyberkriminalitet enn for tradisjonell kriminalitet (NOU 2015: 13: 56).

2.2 Cyberkriminalitet

I den digitale verden blir cyberkriminalitet ansett som en stadig større trussel (Europol, 2021). Cyberkriminalitet (eller IKT-kriminalitet) kan defineres som “Enhver kriminell aktivitet som finner sted i eller ved å bruke elektronisk kommunikasjon som for eksempel internett» (Yar og Steinmetz, 2019: 264). IKT-kriminalitet er i ferd med å bli et reelt samfunnsproblem. Blant annet har den teknologiske utviklingen ført til at tradisjonell kriminalitet kan begås på nye måter, for eksempel ved bruk av internett, som gjør det vanskeligere å oppdage lovbruddet samtidig som det har et høyt fortjenestepotensial (NOU 2015: 13: 56). De siste tiårene har flere

land i det vestlige samfunnet opplevd et fall i kriminalitet (Tonry, 2014). En mulig forklaring på fallet er at det har skjedd en forskyvning fra tradisjonell kriminalitet til cyberkriminalitet (Caneppele og Aebi, 2017).

Det er vanlig å skille mellom cyber-enabled (dataaktivert) kriminalitet og cyber-dependent (dataavhengig) kriminalitet (Kranenbarg, 2021: 196). Dataaktivert kriminalitet er tradisjonelle lovbrudd der IKT brukes i utførelsen av lovbruddet, for eksempel ulike former for svindel på nettet og overgrep mot barn (Selzer og Oelrich, 2021: 176). Dataavhengig kriminalitet er lovbrudd som ikke kan utføres uten bruk av informasjons- og kommunikasjonsteknologi, for eksempel hacking av datasystemer (Selzer og Oelrich, 2021: 176). Dupont og Whelan (2021: 2) beskriver cyberkriminalitet som et «umbrella concept» for å vise til at det er et stort felt som rommer mye. Blant annet opplever bedrifter trusler mot økonomisk ytelse og stabilitet; myndigheter snakker om cyberkrig og cyberterror; foreldre frykter for barnas sikkerhet på grunn av pedofile som opererer på sosiale nettverk på jakt etter ofre; knapt en datamaskin-bruker eksisterer som ikke har blitt utsatt for angrep av virus og andre former for skadelig programvare, og forsvarere av demokratiske rettigheter og friheter ser på internett som en trussel fra stater, overbevist om at internett gjør det mulig å overvåke og kontrollere innbyggere (Yar og Steinmetz, 2019: 4). Slik ser det ut til at cyberkriminalitet presenterer en rekke nye utfordringer for individuell og kollektiv sikkerhet, sosial orden og stabilitet, økonomisk velstand og politisk frihet (Yar og Steinmetz, 2019: 4; Dupont og Whelan, 2021: 2).

Noen hevder at cyberkriminalitet stort sett er det samme som «gammeldags» ikke-virtuell kriminalitet, bare at lovbryterne bruker noen nye nyttige verktøy, og kaller derfor cyberkriminalitet for «old wine in new bottles» (Grabosky, 2001). Andre mener derimot at cyberkriminalitet representerer en ny form for kriminalitet som er helt forskjellig fra kriminalitet som foregår i den «virkelige verden» (Wall, 2007). Blant denne siste gruppen fokuserer mange kriminologer på de sosialstrukturelle funksjonene i miljøet – cyberspace – hvor slike lovbrudd oppstår. Dette miljøet har stor innvirkning på hvordan sosiale interaksjoner kan finne sted – både lovlige og ulovlige – og dermed forvandler det potensielle omfanget av kriminell aktivitet. Cyberspace-miljøet har nye sosiale egenskaper. Det fjerner geografisk avstand, åpner for tilkobling mellom mange enheter og gir mulighet for anonymitet. Slik muliggjøres nye former og mønstre for ulovlig aktivitet. Det er en stor forskjell fra tidligere kriminalitet og dette gjør cyberkriminalitet særegent (Yar og Steinmetz, 2019). Cyberkriminalitet, gitt internetts globale natur, er et iboende territorialt fenomen. Kriminalitet

i cyberspace samler lovbrytere, ofre og mål og kan foregå fysisk i forskjellige land og kontinenter. Slik spenner lovbruddet seg over nasjonale og internasjonale grenser (Yar og Steinmetz, 2019).

Kriminelle som opererer i cyberspace er på jakt etter informasjon som er av verdi for dem (NSM, 2020: 23). For å oppnå sine mål leter de systematisk etter mennesker som på en eller annen måte kan gi tilgang til disse verdiene. Trusselaktørene kan finne personer som er villige til å gi dem tilgang, eller de kan utnytte folk for å få tak i informasjonen (NSM, 2020: 23). Norske virksomheter er mål for ulike typer nettverksoperasjoner (svindelforsøk). En av de vanligste svindelmetodene virksomheter utsettes for er *løsepengevirus*. NSM (2020: 24) definerer denne typen svindel som «en type skadevare som brukes til å kryptere filer hos virksomheter, og deretter kreve penger for å dekryptere dem». Forklart med andre ord lammer trusselaktører digitale systemer og krever løsepenger for å låse opp krypteringen. De siste årene har det vært en økning i slike utpressingsforsøk rettet mot virksomheter som har større betalingsevne enn enkeltpersoner. *Direktørsvindel* er en annen type nettverksoperasjon som trusselaktører benytter seg av. NSM (2020: 28) definerer denne nettverksoperasjonen som «at direktørens e-postadresse eller telefonnummer er brukt for å lure økonomiansatte til å overføre penger». En annen type svindelforsøk er *phishing* og innebærer massedistribusjon av e-post til enkeltpersoner, hvor avsender fremstår som en reell virksomhet eller noen mottaker stoler på. Målet med phishing er å overtale offeret til å frivillig avsløre sensitiv informasjon, for eksempel bankkontodetaljer eller brukernavn og passord til nettjenester. Avsender lurer offeret til å åpne et vedlegg eller klikke seg inn på en falsk nettside hvor vedkommende må logge seg inn. Informasjonen mottaker gir fra seg utnyttes deretter for å svindle den aktuelle personen (Yar og Steinmetz, 2019: 137). *Smishing* ligner på phishing, men istedenfor at svindelforsøket utføres via epost er det her snakk om svindelmeldinger som tilsendes på SMS. Meldingene inneholder gjerne linker til nettsteder som bedragerne har kontroll over og som de prøver å få mottakerne til å klikke seg inn på. På nettstedene lures personer, på samme måte som ved phishing, til å oppgi sensitiv informasjon som deretter brukes av svindlerne (NorSIS, 2020: 57).

2.3 Cybersikkerhet

Trusler og risiko knyttet til cybersikkerhet har de senere årene fått stor oppmerksomhet i samfunnet (Mark mfl., 2019; Dupont og Whelan, 2021), og cybersikkerhet har blitt en kompleks utfordring i det tjueførste århundre (Harknett og Stever, 2009). *Cybersikkerhet, Informasjonssikkerhet* eller *IKT-sikkerhet* kan ses på som «reaksjonen på en risiko og trussel mot den moderne, globale informasjonsteknologiske infrastrukturen, oftest kjent som internett» (Stevens, 2016 i Muller, 2016: 3). Dunn Cavelty og Suter (2012: 19, i Muller, 2016: 3) definerer cybersikkerhet som «Fraværet av trusler fra eller via informasjon- og kommunikasjonsteknologier og -nettverk». Det handler med andre ord om sikkerheten vi har både i og gjennom cyberspace.

Informasjonssikkerhet angår både individer, organisasjoner og samfunnet generelt. De siste årene har vi sett flere hendelser som utfordrer IKT-sikkerheten, blant annet angrepet på Hydro og Mærsk, og det er grunn til å tro at omfanget av slike utfordringer vil øke (Mark mfl., 2019). Regjeringer og organisasjoner distribuerer en rekke tekniske verktøy for å forbedre cybersikkerheten og for å avverge cyberangrep og det settes av betydelige midler til denne aktiviteten (Singh mfl., i 2013 i Renaud mfl., 2020). I Norge er digital sikkerhet et viktig satsningsområde for regjeringen, og det arbeides for at IKT-sikkerhet skal styrkes i hele samfunnet for å møte utfordringene på området. I januar 2019 la regjeringen fram en nasjonal strategi for digital sikkerhet og en nasjonal strategi for digital sikkerhetskompetanse (Regjeringen, 2019). Strategiene beskriver tiltak for til sammen omtrent 1,6 milliarder kroner. De siste årene har Norge opprettet ulike sikkerhetsorganer som jobber forebyggende med cyberkriminalitet. For eksempel har politiet opprettet sitt nasjonale cybersenter (NC3) som skal bidra til å bygge opp politiets kompetanse på kompleks kriminalitet på og mot internett. Andre eksempler på slike institusjoner er Norsk senter for informasjonssikkerhet (NorSIS), Nasjonal sikkerhetsmyndighet (NSM), Nasjonalt cybersikkerhetssenter (NCSC) og Næringslivets sikkerhetsråd (NSR).

Dupont og Whelan (2021) mener at fagfeltene cyberkriminologi og cybersikkerhet, som i dag er atskilt, har stort behov for større samarbeid på tvers av grensene slik at en kan unngå «solo»-tenkning. Siden begge fagfelt er opptatt av å studere skadevirkningene av kriminalitet på nett og hvordan disse reageres på, mener de det ville vært logisk å anta at feltene deler flere teoretiske og empiriske tilnærminger. Imidlertid forstås de i dag som to separate fagfelt blant

annet med differensierte forskningsspørsmål, datasett, og karriereveier. Dupont og Whelan (2021) mener at forskning innenfor begge fagfelt slik begrenses, og at et samarbeid vil være av nytte for fremtidig forskning for både cyberkriminologi og cybersikkerhet. I tillegg er det mulig å observere noen spesifikke trender hva angår forskningsfokus i dette «paraply-konseptet» cyberkriminalitet utgjør. For eksempel finnes det studier som er orientert mot de som begår kriminelle handlinger i cyber-rommet, og søker å kartlegge ulike kjennetegn for cyberkriminelle. Andre igjen dreier fokuset mer mot de som blir utsatt for cyberkriminalitet, altså ofrene. Et tredje fokusområde omfavner de polisiære responsene på cyberkriminalitet, altså hvordan ulike aktører arbeider mot å avdekke eller forebygge kriminaliteten. I det følgende ses det nærmere på sentrale forskningsbidrag innen disse tre områdene.

2.4 Forskning på gjerningspersonene

Selv om forskning på cyberkriminalitet utvikler seg raskt, mener Selzer og Oelrich (2021) at det mangler forskning på spesielt to felt: dataavhengig kriminalitet og rollen psykologiske faktorer spiller inn på hvem som driver med cyberkriminalitet. Derfor har de gjennomført en studie som tar sikte på å belyse dette ved å evaluere innflytelsen av negative og positive personlighetstrekk på cyberkriminalitet. I tillegg har de sett på moralsk utvikling som har vist seg å ha negativ påvirkning på kriminell aktivitet. Studien til Selzer og Oelrich (2021) finner at personer med høyere machiavellisme og psykopatisk score er mer sannsynlig å delta i cyberkriminell atferd enn personer med lavere score. Narsissisme ser derimot ikke ut til å være knyttet til cyberkriminell atferd (Selzer og Oelrich, 2021). Machiavellisme- personligheter er assosiert med rasjonalitet, overlegne analyseferdigheter og strategisk planlegging (Bereczkei og Birkas, 2014; Jones & Paulhus, 2014), som er nyttige egenskaper for å utføre cyberkriminalitet. Ettersom psykopati ser ut til å være en forklaring for flere kriminelle tendenser i tradisjonell kriminalitet, mener Selzer og Oelrich (2021) det er interessant å finne at denne relasjonen også er gjeldende for cyberforbrytere. Videre sier de at impulsiv atferd, tilsidesettelse av andres rettigheter og privatliv samt mangel på empati kan bidra til at personer ser cyberkriminalitet som et gyldig alternativ for å nå sine mål. De antar at kriminelle som scorer høyt på psykopati ganske enkelt kan «digitalisere» sin avvikende atferd fra tradisjonelle lovbrudd, og flytte sin kriminelle karriere til cyber-avhengig aktivitet.

Kranenbarg (2021) har undersøkt i hvilken grad lovbrytere som driver med dataaktivert kriminalitet kan skilles fra tradisjonelle lovbrytere, og hvilke motiver de har oppgitt for å begå dataaktivert kriminalitet. Undersøkelsen finner at kriminelle som utøver dataaktiverte lovbrudd

ser ut til å spesialisere seg. Dette fordi de som driver med dataaktivert kriminalitet sjelden også driver med tradisjonell kriminalitet. Kranenbarg (2021) sier videre at dette står i tråd med det hypotetiske skillet mellom tradisjonell kriminalitet og cyberkriminalitet. Antagelsen om at cyberkriminalitet er det samme som tradisjonell kriminalitet (Alleyne, 2011; Stephenson og Walter, 2012) kan derfor ikke verifiseres med dataene fra studien deres. I tillegg understreker studien at indre motiver var viktigst for alle lovbryterne som drev med dataaktivert kriminalitet, og at svært få kriminelle oppga økonomisk vinning som grunn for å begå cyberkriminalitet. Det sistnevnte står i motsetning til påstanden om at det er et skifte mot økonomiske motiver for å begå kriminalitet (Bernaards mfl., 2012). Lovbryterne indikerte at lovbruddene ble begått på grunn av kjedsomhet, nysgjerrighet, spenning eller andre iboende motiver (Kranenbarg, 2021). Selv om fokuset for denne oppgaven ikke er rettet mot de som begår datakriminalitet er forskning om gjerningspersonene interessant å se på ettersom flere studier mener denne gruppen representerer en ny gruppe lovbrytere (Brewer mfl, 2019). Den tekniske kompetansen som kreves samt utstyret som er nødvendig for å begå slike lovbrudd skiller seg fra forutsetningene for å begå tradisjonell kriminalitet (Yar og Steinmetz, 2019).

2.5 Cyberofre

Alle er potensielle ofre for cyberkriminalitet, noe som betyr at cyberkriminelle tilsynelatende ikke er så kresne og ikke velger hvem de vil angripe (van't Hoff-de Goede mfl., 2021: 22). Å utsettes for cyberkriminalitet kan oppleves som svært inngripende (Jansen og Leukfeldt, 2018). Eksperter på cybersikkerhet forsøker å sette inn tekniske tiltak som for eksempel antivirus og brannmurer for å redusere forekomsten av å bli offer for cyberkriminalitet, men slike tiltak har ofte kun en begrenset effekt, og å bli offer for slik kriminalitet spores stadig tilbake til menneskelig atferd (Leukfeldt, 2017). Derfor er det viktig å forske på hvordan mennesker bruker internett for å redusere forekomsten av cyberofre (Leukfeldt, 2017). Utrygg atferd på internett, som for eksempel bruk av svake passord, kan øke risikoen for å bli offer (Leukfeldt, 2014). En viktig forutsetning for å være sikker på internett er derfor at man utøver trygg atferd på nett, for eksempel ved å unngå usikre nettsteder og ikke klikke på upålitelige koblinger (van't Hoff-de Goede mfl., 2021). Bruk av sterke passord og regelmessige oppdateringer av programvarer anses også som trygg atferd på nett (Cain mfl., 2018). Kunnskap om hvordan mennesker kan forebygge cyberkriminalitet er imidlertid knapp og det er ukjent hvor godt internettbrukere beskytter seg mot denne typen kriminalitet (van't Hoff-de Goede mfl., 2021: 21). Crossler mfl. (2013) mener dette delvis skyldes det faktum at hvordan folk sier eller tror

de oppfører seg på internett ikke alltid er det samme som hvordan folk faktisk oppfører seg på internett.

Tidligere studier, basert på selvrapportert atferd og faktisk atferd i eksperimentelle settinger, har vist at mange kun oppfører seg trygt på internett i begrenset grad (van't Hoff-de Goede mfl., 2021: 23). Mens bruk av unike sterke passord er et viktig sikkerhetstiltak, har studier vist at 50-60% av passordene blir gjenbrukt på tvers av plattformer, og at mange mennesker deler passordene sine med andre (Cain mfl., 2018). Et annet eksempel på utrygg atferd på internett er at folk deler personlig informasjon på sosiale medier (Talib mfl., 2010), som kan brukes av cyberkriminelle til å for eksempel gjøre phishing mail mer troverdig. I studien til Talib mfl. (2010) delte for eksempel 62% av respondentene sitt fulle navn og e-postadresse, 45% delte fødselsdatoen sin og 7% delte full adresse på et sosialt nettverk.

Selv om trygg atferd på internett kan forhindre at man blir offer for cyberkriminalitet, er utrygg atferd på internett vanlig. Basert på to teorier som tidligere er brukt for å forklare atferd: Protection Motivation Theory (PMT) og COM-B rammeverket (Capability, Opportunity, Motivation, Behavior), har van't Hoff-de Goede mfl. (2021) kommet frem til tre faktorer de mener kan spille en viktig rolle for utrygg atferd på internett. Dette er motivasjon, kunnskap (dvs. bevissthet), og mulighet.

Motivasjon

Ifølge PMT-teorien er hvor godt vi beskytter oss påvirket av hvilken grad vi er motivert til å beskytte oss (Floyd mfl., 2000). Det sies at mennesker med høy beskyttelsesmotivasjon handler mer forsiktig og tar forhåndsregler for å beskytte seg (Crossler og Belanger, 2014). PMT-teorien mener også at beskyttelsesmotivasjon påvirkes av personers mestringsvurdering og trusselvurdering som begge inneholder flere komponenter (Floyd mfl., 2000). Komponentene i trusselvurdering er opplevd sårbarhet (vurdering av egen sårbarhet overfor trusselen) og opplevd alvorlighetsgrad (vurdering av trusselens alvorlighetsgrad). Komponentene i mestringsvurdering er responseffektivitet (om et tiltak vil være effektivt mot trusselen), selveffektivitet (om vedkommende er i stand til å implementere et effektivt tiltak), og responskostnader (om de estimerte kostnadene ved et tiltak er verdt det) (Van't Hoff-de Goede mfl., 2021: 25). PMT-teorien er tidligere brukt for å undersøke atferd på internett, og studier viser at estimert responseffektivitet, selveffektivitet og responskostnader ser ut til å være viktige indikatorer for trygg atferd på internett (Arachchilage og Love, 2014; Crossler mfl., 2017;

Crossler og Bélanger, Jansen og van Schaik, 2017; 2014; Workman mfl., 2008). Opplevd sårbarhet ser derimot ikke ut til å være relatert til trygg atferd på internett. Mennesker som anser seg selv som sårbare for angrep oppfører seg ikke annerledes. Boss mfl. (2015) fant i sin studie at frykt for å bli offer for cyberkriminalitet ikke så ut til å påvirke databrukere til å sikkerhetskopiere filene. De fleste studier finner derimot en sammenheng mellom opplevd alvorlighetsgrad og atferd på internett (Crossler mfl., 2017; Jansen, 2018; Jansen og van Schaik, 2017).

Kunnskap

Det teoretiske COM-B rammeverket antyder at i tillegg til motivasjon, er kunnskap eller bevissthet om sikker atferd en nødvendighet for trygg atferd på internett (Michie mfl., 2011). Tidligere studier som har undersøkt i hvilken grad kunnskap om IT og cybersikkerhet påvirker atferd på internett har gitt tvetydige resultater (Van't Hoff-de Goede mfl., 2021: 26). For eksempel fant Downs mfl. (2007) at personer som er i stand til å evaluere nettadresser samt forstår internettikoner og internettutrrykk kan være mindre sårbare for phishingangrep. I tillegg ser det ut til at mennesker som sier at de er IT-eksperter er mindre sannsynlig å utvise utrygg atferd på nett (Alohali mfl., 2018). Likevel fant Cain mfl. (2018: 43) at mennesker som anser seg selv som IT-eksperter oppfører seg mindre trygt på internett, og det ble heller ikke funnet noen forskjell i sikker atferd på nett mellom de som var opplært i cybersikkerhet og de som ikke var det.

Mulighet

Ifølge COM-B rammeverket er det ikke sikkert at motivasjon og kunnskap er nok for at folk skal oppføre seg trygt på internett (Van't Hoff-de Goede mfl., 2021). Mulighet er også nødvendig og referer til det sosiale og materielle miljøet som gjør atferd mulig eller umulig (Michie mfl., 2011). Det finnes derimot lite forskning på hvilken betydning mulighet har for atferd på nett (Van't Hoff-de Goede mfl., 2021). Det sosiale miljøet handler om hvordan menneskene rundt oss påvirker atferden vår. For eksempel fant Herath og Rao (2009) at sosial innflytelse fra nære kolleger og ledere kan ha stor påvirkning for sikker atferd på internett i organisasjoner. Det materielle miljøet handler om tilgjengelighet til økonomiske ressurser, tid og verktøy som støtter sikker praksis. Flere selskaper tilbyr ansatte verktøy som skal muliggjøre sikker atferd på internett (Van't Hoff-de Goede mfl., 2021). Slike verktøy og ressurser kan bidra til å styrke ansattes selvtillit til å vise ønsket atferd ved å øke tekniske og normative barrierer

(Herath og Rao, 2009). Dette er teori som ligger til grunn for situasjonell kriminalitetsforebygging som tas opp senere i oppgaven.

2.6 Policing

«Policing» brukes for å betegne et bredt spekter av regulatorisk praksis som overvåker sosial atferd og sikrer samsvar med lover og normative koder (Yar og Steinmetz, 2019: 217). Begrepet er mest tilknyttet politiet, den institusjonen i samfunnet som opprettholder lover på vegne av samfunnet og som skal skape sikkerhet. Politiet har vært svært involvert når det kommer til cyberkriminalitet, men institusjonens innsats har flere ganger blitt kritisert for å være utilstrekkelig i dette arbeidet (Yar og Steinmetz, 2019; Dupont og Whelan, 2021).

Ifølge Faubert mfl. (2021) er politibetjenters evne til å effektivt håndheve lover i den digitale verden et bekymringsområde. På grunn av de nye utfordringene som oppstår i den digitale verden stilles det spørsmål til politiets evne til å transformere seg til å drive digital politivirksomhet. Noen mener at regulering av cyberkriminalitet er mer effektivt når den overlates til private selskaper (Dupont, 2017; Holt, 2018). Yar (2005) hevder at cyberspace er mer regulert av private, uformelle og teknologiske voktere enn av formelle politbyråer. I samfunnsmedlemmers øyne har politiet imidlertid en «symbolsk plikt» til å beskytte dem mot alle typer kriminalitet, inkludert cyberkriminalitet (Wall, 2007). Det er derfor viktig at politimyndigheter spiller en rolle i kampen mot cyberkriminalitet for å beholde legitimiteten når det kommer til kriminalitetskontroll (Holt, 2018).

Det er lite kjent hvor ofte cyberkriminalitet registreres av politiet (CBS, 2018). Van der Laan og Tollenaar (2021) mener at antallet kan være relativt lavt av ulike årsaker. Det kan skyldes at personer som er offer for cyberkriminalitet ikke legger merke til det, at det ikke alltid anerkjennes, eller at ofre ikke rapporterer det til politiet (McGuire og Dowling, 2013). En annen mulig forklaring er at noen typer cyberkriminalitet heller registreres som tradisjonelle lovbrudd i politisystemer (van der Laan og Tollenaar, 2021). Informasjon om hvor ofte politiet registrerer cyberkriminalitet er viktig for at man skal kunne reagere tilstrekkelig på slik kriminalitet på et politisk nivå, og for at vi skal få mer kunnskap om cyberkriminalitet (van der Laan og Tollenaar, 2021).

Van de Weijer mfl. (2021: 318) har undersøkt et utvalg av små og mellomstore bedrifter (SMB-eiere) i Nederland og deres atferd når det kommer til rapportering av cyberkriminalitet. I studien

har de skilt mellom tiltenkt rapporteringsatferd og faktisk rapporteringsatferd. Respondentene ble spurt om motiver for å rapportere cyberkriminalitet eller ikke, og om tidligere erfaringer ved å rapportere cyberkriminalitet til politiet. Studien viser at flertallet av SMB-eierne ikke rapporterte til politiet dersom de ble utsatt for cyberkriminalitet. Dette står i tråd med tidligere studier (Veenstra mfl., 2015; Wanamaker, 2019). Kun 14,1% av respondentene som var offer for cyberkriminalitet rapporterte det til politiet. Studien finner også at når de samme respondentene ble spurt om ulike cyberkriminalitetshendelser, antydet et stort flertall at de ville rapportert slike lovbrudd til politiet. Studiens resultater viste også at den vanligste grunnen til å faktisk rapportere til politiet var alvorlighetsgraden til lovbruddet og type cyberkriminalitet. Resultatene fra studien indikerer at dataaktivert kriminalitet oftere blir rapportert til politiet, enn dataavhengig kriminalitet. Dette er også i tråd med funn fra tidligere studier blant innbyggere (van de Weijer mfl., 2019, 2020). Van de Weijer mfl. (2021) mener dette kan tyde på at ofre for slik kriminalitet tenker at politiet ikke er ansvarlige eller ikke har kunnskapen til å håndtere cyberkriminalitet selv om respondentene ikke nevnte dette som de viktigste årsakene til å ikke politianmelde lovbruddene.

Å drive med polisiær virksomhet innenfor cyberkriminalitet krever ekspertise. I private selskap og på individnivå utvikles det ofte en ekspertise og kunnskap på feltet. På denne måten vil private selskaper også inneha en sentral posisjon i det polisiære arbeidet opp mot cyberkriminalitet. På individnivå blir ikke hacking nødvendigvis bare brukt til kriminelle formål, men også til å søke etter sårbarheter som rapporteres slik at de kan utbredes (Yar og Steinmetz, 2019).

2.7 Utbredelsen av cyberkriminalitet: mørketallsproblematikk

Å få et realistisk mål på omfanget av cyberkriminalitet er utfordrende. Noen av disse problemene er velkjent for kriminologer. Offisiell statistikk over kriminalitet har for eksempel blitt kritisert som «sosiale konstruksjoner» som ikke nødvendigvis gir et objektivt bilde av de sanne, underliggende nivåene og mønstrene for lovbrudd (Yar og Steinmetz: 2019: 41). Det er flere grunner til dette. For det første avhenger slik statistikk av at lovbrudd rapporteres til politiet. Yar og Steinmetz (2019: 41) skriver også at en stor andel lovbrudd ikke rapporteres av en rekke årsaker: ofre kan være uvitende om at et lovbrudd er begått, de kan anse lovbruddet som for lite alvorlig til at de rapporterer det, og de kan føle at det er lite sannsynlighet at det vil resultere i en tilfredsstillende løsning.

Problemene med å måle kriminalitet blir forverret i forhold til cyberkriminalitet. For eksempel gjør det digitale rom det lettere for kriminelle å opptre i skjul og med lav risiko for å avsløres. Samtidig er rommet globalt og gir slik muligheten for å angripe mål over landegrenser (NSR, 2020: 44). Kriminelle handler i det såkalte «mørke nettet» hvor kjøp og salg av virusprogrammer og ulike verktøy for digitale innbrudd er lett tilgjengelige. Her kan aktører gjennomføre betalinger uten ettersporing ved hjelp av kryptovalutaer og løsepengekrav. Ifølge NSM har dette blitt et «fristed for kriminelle» (NSR, 2020: 44). Slike faktorer antyder at det faktisk kan være en massiv underrapportering av kriminelle aktiviteter på internett (Yar og Steinmetz, 2019: 42). I Norge finnes det ingen helhetlig statistikk over omfanget av digitale angrep (NOU 2015: 13: 263). Aktører som avdekker, håndterer og etterforsker digitale angrep fører som regel egen statistikk over saker de er involvert i, men dette samles ikke noe sted. Det gjør det vanskelig å få en helhetlig fremstilling og et korrekt bilde av IKT-trusselbildet, som igjen begrenser evnen til å både forebygge og håndtere digitale hendelser (NOU 2015: 13: 263).

Det er alvorlige problemer knyttet til underrapportering av cyberkriminalitet. Dette kan det være flere grunner til. For eksempel kan mange organisasjoner kanskje foretrekke å ikke erkjenne å være offer for dette på grunn av: 1) frykt for pinlighet; 2) tap av offentlig tillit, og 3) på grunn av potensielle juridiske forpliktelser (Yar og Steinmetz, 2019). Ifølge mørketallsundersøkelsen til næringslivets sikkerhetsråd er det stor usikkerhet knyttet til norske mørketall når det gjelder antall estimerte hendelser og når det gjelder kostnader som følge av hendelser (NSR, 2014). Norge taper årlig cirka. 20 milliarder kroner på grunn av IKT-kriminalitet alene. Det er dog vanskelig å estimere økonomiske tap knyttet til digitale sårbarheter. Yar og Steinmetz (2019) mener at denne underrapporteringen bør gjøre at vi behandler statistikk om cyberkriminalitet med forsiktighet. En av de største pågående utfordringene for både kriminologi og strafferettslige forhold til cyberkriminalitet er behovet for å utvikle grunnleggende, robuste indikasjoner på selve problemet. Til tross for vanskelighetene som er skissert ovenfor, mener Yar og Steinmetz (2019: 44) at det vil være feil å ignorere den tilgjengelige statistikken på tross av at den er begrenset. Hvis vi ønsker å få innsikt i omfanget av cyberkriminalitet, må vi bruke den dataen som er tilgjengelig. Det blir her et tilfelle hvor relativt svake data er bedre enn absolutt ingen data. Så lenge vi ikke betrakter disse målene og tallene som ubestridelige fakta, kan de være nyttige for å gi oss noen foreløpige indikasjoner på problemer med cyberkriminalitet (Yar og Steinmetz, 2019). Jeg vil i det følgende vise til ulike rapporter om cyberkriminalitet for å gi en indikasjon på hvorfor cyberkriminalitet har blitt gjenstand for bekymring.

Ifølge Global Economic Crime and Fraud Survey fra 2020 ligger cyberkriminalitet på andre plass av topp fire typer svindler i 2020 (PWC, 2020). Ifølge NorSIS sin rapport *trusler og trender* var løsepengevirus og phishing blant de ti største digitale truslene i 2020 (NorSIS, 2020). Likevel påpekes det at det største problemet når det kommer til cyberangrep faktisk er mennesker som gjør feil i systemer, og dermed hjelper trusselaktører til å utføre angrep (Norris mfl., 2015; Cain mfl., 2018: 36). Ifølge mørketallsundersøkelsen 2018 fra Næringslivets sikkerhetsråd skyldes mer enn halvparten av sikkerhetsbruddene i norske virksomheter menneskelig feil (NorSIS, 2020). Tallene som er presentert gir en viktig indikasjon på hvorfor trusselen om cyberkriminalitet har blitt en stor bekymring for blant annet organisasjoner og politikere i det moderne samfunnet.

3 Teoretiske perspektiver

I denne delen vil jeg presentere ulike teoretiske perspektiver og teorier som kan bidra til å forstå hvordan cyberkriminalitet forebygges i Wintershall Dea. Først vil jeg presentere litteratur som viser hvordan risiko og sikkerhet kan forstås i det moderne samfunn, fordi en slik kontekst kan anta å prege informantenes risiko- og sikkerhetsoppfatning av cyberkriminalitet.

Hvordan cyberkriminalitet bør og skal styres har fått et stort fokus i samfunnet og ført til at cybersikkerhet har blitt sentralt. I andre del av teorikapittelet vil jeg presentere det teoretiske rammeverket for oppgaven. Først vil jeg presentere Michel Foucault sitt begrep – governmentality – som handler om hvilke styringslogikker som kan anvendes av myndigheter for å styre og kontrollere samfunnet, som for eksempel cyberkriminalitet. Foucault har inspirert David Garland, som med sitt begrep – responsibilization – også er sentral for å se på styringslogikken til myndighetene. Til slutt i kapittelet vil jeg presentere teori om kultur, sikkerhetskultur, nodal governance og situasjonell kriminalitetsforebygging som kan belyse ulike mentaliteter og logikker når det gjelder hvordan cyberkriminalitet kan styres og forebygges.

3.1 Risiko og sikkerhet

Risiko og sikkerhet er to begreper som knytter seg til hverandre (Engen mfl., 2016: 41), og i olje- og gassektoren står både risiko og sikkerhet sentralt. Lysneutvalget (2015: 1) skriver blant annet at «Enhver aktivitet i olje- og gassektoren er forbundet med risiko forårsaket av trusler og sårbarheter». Utvalget skriver videre at dette også gjelder risiko grunnet digitale sårbarheter og uønskede hendelser, både tilsiktede og utilsiktede, kan ramme bedrifter og enkeltmennesker. Fremveksten av cyberspace har slik gjort verden sårbar på en ny måte. Blant annet har cyberangrep blitt både vanligere og farligere de siste årene, og den økende avhengigheten av cyberspace har gjort at sikring av cyberspace blir stadig viktigere. Slik har cybersikkerhet fått et stort fokus på den internasjonale sikkerhetsagendaen (Muller, 2016).

3.1.1 Forståelsen av risiko

De siste årene har flere forskere vært opptatt av hvordan risiko inngår i, blir fortolket og håndtert av samfunnet (Engen mfl., 2016: 110**)**. Risiko er noe som inntreffer, enten av naturlige årsaker

som for eksempel et jordskjelv, eller på grunn av planlagte og ikke-planlagte hendelser fra mennesker, som for eksempel dataangrep (Engen mfl., 2016: 80).

Det er vanlig å skille mellom et realistisk og et konstruktivistisk syn på risiko (Engen mfl., 2016: 78). Et «realistisk kunnskapssyn» benytter matematiske og statistiske modeller og beregningsmetoder for å forutsi muligheten for framtidige hendelser og konsekvensene disse medbringer (Engen mfl., 2016: 78). Dette perspektivet definerer risiko som et produkt av sannsynlighet og konsekvens (Engen mfl., 2016: 78). Det konstruktivistiske perspektivet er fremtidsrettet og tar utgangspunkt i hvordan vi som individer og kollektiv forstår, tolker og forteller om framtiden. Her er spørsmålet «hvordan risikoen blir opplevd og forstått, og hvordan den blir konstruert i samspillet mellom enkeltindivider, grupper, organisasjoner og institusjoner» (Engen mfl., 2016: 79). Gundhus og Jansen (2020: 95) sier at ettersom fremtiden er ukjent bør et intelligensprodukt ikke betraktes som et «sannhetsprodukt», men heller den beste vurderingen på den tiden. Det fremhever hvorfor det konstruktivistiske perspektivet er av sentralitet. Det handler om hvordan vi håndterer utfordringene det globale samfunnet står overfor, som for eksempel teknologiske systemer. Ericson og Haggerty (1997: 17) skriver at risiko refererer til ulike «kommunikasjonsregler, formater og teknologier som brukes for å håndtere farer». Det er vanskelig å si at dette er den reelle risikoen, men det er et tolkende blikk på det.

3.1.2 Forståelsen av sikkerhet

Hva sikkerhet er, hva det betyr og hva som skal gjøres for å garantere det, er mye diskutert (Bourbeau, 2015; Loader og Percy, 2012). Det er vanlig at kriminologer skiller mellom den objektive og den subjektive tilstanden av sikkerhet (Wood og Shearing, 2007: 4). Ifølge Zedner (2009: 14) forutsetter den objektive tilstanden av absolutt sikkerhet et absolutt fravær av risiko og trusler, og er lite sannsynlig da det alltid vil være mulighet for at nye trusler oppstår. Zedner mener derfor det er fornuftig å erkjenne at en absolutt sikkerhetstilstand vil være uoppnåelig. Forstått på denne måten handler objektiv sikkerhet om å være beskyttet fra trusler «enten gjennom nøytralisering, gjennom unngåelse eller gjennom ikke-eksponering for risiko» (Zedner 2009: 14). Objektiv sikkerhet kan med andre ord forstås som det samfunn, organisasjoner eller institusjoner opplever som trusler. Videre mener Zedner at objektiv sikkerhet kun gir mening hvis det defineres i relasjon til det som anses som en trussel.

Den subjektive tilstanden av sikkerhet handler om individers egen følelse av sikkerhet, og kan ta form som en absolutt tilstand eller en kvalifisert tilstand (Zedner, 2009). Den absolutte tilstanden av sikkerhet betyr at individer føler seg helt trygge. Den kvalifiserte tilstanden betyr at individer opplever frihet fra angst eller frykt fordi følelsen av usikkerhet har blitt dempet, og er den vanlige formen for subjektiv sikkerhet. Subjektiv sikkerhet kan videre samsvare med objektiv sikkerhet, men det kan også være lite relatert til nivået av den objektive trusselen. For eksempel fortsetter mange unge menn å være uredde selv om det statistisk sett er mest sannsynlig at de utsettes for voldelige overgrep (Zedner, 2009).

Sikkerhet forstås i denne avhandlingen i sammenheng med trusselen cyberkriminalitet. Sett i forhold til cyberkriminalitet virker en tilstand av absolutt sikkerhet lite sannsynlig da den teknologiske utviklingen fører til stadig nye muligheter for kriminelle. Dette poenget tas også opp av Zedner (2009) som skriver at det er en konstant «jakt på sikkerhet» i samfunnet. Det er derimot krevende å oppnå en absolutt sikkerhet, da det krever at en konstant må være på utkikk etter nye trusler. Det kan tenkes at en konstant jakt på sikkerhet vil få konsekvenser for aktørene som jobber med dette, som i denne oppgaven vil være ekspertene i Wintershall Dea. Ettersom potensielle lovbrytere hele tiden finner nye måter å angripe på kan det tenkes at ekspertene alltid må være forberedt og «jakte sikkerhet». Det vil være interessant å se hvordan ekspertene og ansatte opplever og forstår cybersikkerhet og cyberkriminalitet.

3.1.3 Risiko og sikkerhet i det moderne samfunn

Anthony Giddens og Ulrich Beck skriver begge om risikoer i det moderne samfunnet. Giddens (1997) mener at moderniteten er et tveegget fenomen som er preget av sikkerhet versus fare og tillit versus risiko. Det moderne samfunnets utvikling av institusjoner og deres globale utbredelse har gitt flere muligheter for samfunnsborgere til å leve et sikkert og rikt liv, men det har også ført til nye risikoer. Giddens mener at konsekvensene av moderniteten er et univers hvor risiko og farer har fått en ny karakter.

Beck (1992) karakteriserer det vestlige moderne samfunnet som et risikosamfunn. Han mener at den sosiale produksjonen av rikdom fører til den sosiale produksjonen av risiko, og at samfunnet vi lever i preges av usynlig risiko (Beck, 1992). Dette skiller seg fra det førmoderne samfunn hvor risiko ble definert som farer og trusler som kom utenfra og som var forbundet med skjebne og forbannelse (Engen mfl., 2016: 113). Ifølge Beck er risikosamfunnet en effekt av den vitenskapelige og teknologiske utviklingen drevet av kapitalistisk vekst (Rose mfl.,

2006). På grunn av økt globalisering og utvikling av teknologi har nye former for risikoer vokst frem (Rose mfl., 2006: 96). De nye risikoene fører til politiske og økonomiske spørsmål om hvordan risikoer skal styres, for eksempel hvordan cyberkriminalitet og cybersikkerhet skal styres.

Samfunnsmedlemmer ønsker sikkerhet, og man er på jakt etter teknologier for risikostyring som kan bidra til å håndtere frykten og angsten som vokser frem (Beck, 1992). Sikkerhet har blitt et sentralt tema i kriminologien og det forskes mye innenfor dette feltet, blant annet på «governing security». Zedner (2009) mener at den økte oppmerksomheten for temaet reflekterer den brede usikkerheten i det 21.århundre. Ifølge Wood og Shearing (2007: 5) er referansen til usikkerhet på den politiske arenaen nesten alltid basert på referansen til kriminalitet, og i økende grad, uorden. Med andre ord er det kriminalitet som truer objektive og subjektive «tilstander av å være trygge». Denne sammenhengen mellom usikkerhet og kriminalitet forsterkes også av kriminologer, hvor det sies at å kunne forstå kriminell atferd og dens forløpere vil gi et tryggere samfunn. Slik kan vi si at det er kriminalitet som lager rammen for hvordan man ser på sikkerhetsproblemer i samfunnet (Wood og Shearing: 2007).

Cyberkriminalitet er et godt eksempel på nye risikoer som har vokst frem som en konsekvens av teknologi og globalisering. Disse kriminelle aktivitetene ses som en stor trussel i samfunnet. På samme måte som «krigen mot terror» har vært med på å forme måten man håndterer sikkerhetsproblemer i samfunnet, ser vi at cyberkriminalitet kommer mer og mer på agendaen som noe som må styres (Wall, 2007). Et sentralt spørsmål som har vokst frem fra de nye risikoene i samfunnet er hvordan de skal styres for å forebygges (Wood og Shearing, 2007). For å finne ut hvordan cyberkriminalitet kan forebygges vil det være hensiktsmessig å videre se på ulike styringsstrategier.

3.2 Governmentality

Michel Foucault (1991) introduserte begrepet Governmentalitè (eng. governmentality) for å forstå hva som er spesifikt med maktutøvelsen i det moderne samfunnet. Han fokuserte spesielt på forholdet mellom to måter å styre på: ulike måter staten styrer befolkningen sin på, og teknologiene individer bruker for å forme selvet og sin egen subjektivitet (Garland, 1997: 174). Foucault argumenterte for at en ny mentalitet – governmentality – hadde blitt det vanlige grunnlaget for alle moderne former for politisk tanke og handling (Rose mfl., 2006). Han mente

at det har skjedd en utvikling av en rekke spesifikke styringsapparater, og at denne maktformen blir viktigere enn andre maktformer i vestlige land, som suverenitet og disiplin.

Det er flere måter å oversette governmentality-begrepet på. Neumann (2002: 10) oversetter begrepet til regjering. Denne oversettelsen får frem at det dreier seg om et fenomen som er relatert til det å regjere eller styre og minner samtidig om at «makt, og spesielt statens makt, utøves av noe annet enn en monolittisk stat, entydig styrt av en Regjering» (Neumann, 2002: 10). Governmentality kan også oversettes til «styringsmentalitet» for å få frem at «den regjeringen eller styringen det er snakk om, er knyttet opp til måten de styrende og de styrte tenker på – til deres mentalitet» (Neumann, 2002: 10). Ifølge Ericson og Haggerty (1997: 94) refererer styrings-begrepet til risikoteknologier og praksis for å sikre liberal selvstyring. De mener at styring i risikosamfunnet er rettet mot å gi sikkerhet, og at lengselen etter sikkerhet driver en umettelig søken etter mer og bedre kunnskap om risiko.

3.2.1 Regjering i Norge

Som tidligere nevnt utviklet Foucault regjeringsbegrepet for å forstå hva som er spesifikt med maktutøvelse i moderne samfunn. Neumann (2003) undersøker hvordan denne typen makt er relevant i en norsk kontekst på tidlig 2000-tallet. Fremveksten av regjering er knyttet til fremveksten av liberalismen. Neumann (2003) mener at maktutøvelsen, i den liberale staten Norge, skjer på avstand og foregår mindre direkte og at det slik oppstår en utvidet bruk av indirekte maktteknikker. I tråd med en nyliberal politisk rasjonalitet er det mest effektive og legitime at samfunnsborgere i størst mulig grad skal regjere seg selv. Fokuset i denne styringsformen er på forebygging istedenfor direkte styring (Neumann, 2003). Neumann (2002) skriver at regjering ikke bare er et spørsmål om at regjeringen styrer landet, men også om at hver enkelt av oss forventes å regjere oss selv. I tillegg handler regjering om at institusjoner og konkrete personer i samfunnet prøver å komplettere sin direkte styring med indirekte styring ved å komme med detaljerte instruksjoner om hvordan samfunnsborgere skal og ikke skal leve. For eksempel ble Norges innbyggere i en stortingsmelding i 2003 oppfordret til å være sin egen helseminister med budskapet «Den som kan gjøre mest for å påvirke egen helse, er deg selv» (Neumann, 2003: 9). Neumann mener at dette er et godt eksempel på en maktutøvelse som stadig blir mer utbredt i Norge.

Når det kommer til styring av cybersikkerhet kan vi også se at denne mentaliteten har relevans. I 2014 satt regjeringen ned et utvalg som skulle «foreslå konkrete tiltak for å styrke beredskapen

og redusere den digitale sårbarheten i samfunnet» (Lysneutvalget, 2015: 4). Resultatet av dette ble rapporten *Digitale sårbarheter Olje & Gass.* Ifølge rapporten er det norske tilsynsregime i olje- og gassektoren basert på egenregulering og videre en ansvarliggjøring av hver enkelt bedrift (Lysneutvalget, 2015: 4). Videre mener utvalget at for å bedre den digitale sikkerheten må myndighetene påvirke næringen blant annet gjennom å gi informasjon om trusselsituasjonen og stimulere til forebyggende tiltak. Samtidig mener Lysneutvalget at det er selskapene som har detaljkunnskap om virksomheten og at det derfor er de som best kan regulere digitale sårbarheter i selskapet sitt.

3.2.2 Ansvarliggjøringsstrategi

Governmentality- begrepet til Foucault har inspirert flere andre forskere, blant annet David Garland. Garland (1996) studerte hvordan kriminalitet styres i det moderne samfunnet og mente at kriminalitetskontrollen gradvis ble flettet sammen med en sikkerhetstankegang. I «the limits of the sovereign state» argumenterer Garland for at den høye kriminalitetsraten i det moderne samfunnet har ført til en rekke endringer. Blant annet har det ført til en ny måte for staten å styre kriminalitet på, som Garland kaller responsibilization strategy (ansvarliggjøringsstrategi). Strategien går ut på å fordele ansvaret for kriminalitetskontrollen utover i samfunnet. Dette innebærer at staten ikke lenger direkte styrer gjennom statlige organer som for eksempel politi og domstoler, men i stedet søker å styre gjennom å aktivere handlinger fra ikke-statlige byråer og organisasjoner. Staten forsøker med andre ord å overføre ansvaret for forebygging av kriminalitet til byråer, organisasjoner og enkeltpersoner og samtidig overtale dem til å handle hensiktsmessig (Garland, 1996: 452). På denne måten står ikke staten alene ansvarlig for sikkerheten i samfunnet, men samfunnsmedlemmer må også bidra i dette arbeidet. Individet søkes å gjøres til selv-regulerende individer. Staten skal fremdeles beskytte borgerne, men borgerne må samtidig være aktive deltakere i sikkerhetspolitikken. Involvering av andre aktører i politivirksomhet refereres ofte til som *plural policing* (Brodeur, 2010; Jones og Newburn, 1998), og er særlig relevant når det gjelder cyberkriminalitet hvor vi kan se et spesielt høyt nivå av involvering fra blant annet private organisasjoner (Yar og Steinmetz, 2019: 217). Den største delen av internettpolitivirksomhet utføres av organisasjoner lokalisert i den private, veldedige og frivillige sektoren samt av databrukeren selv som er «ansvarlig» for å sette inn tiltak som beskytter dem mot å bli offer for cyberkriminalitet (Yar og Steinmetz, 2019: 223).

Ansvarliggjøringsstrategien innebærer en rekke nye teknikker og metoder hvor staten «søker å få til handling fra private byråer og enkeltpersoner – enten ved å stimulere til nye former for

atferd, eller ved å stoppe etablerte vaner» (Riley og Mayhew, 1980: 15 i Garland, 1996). Det første trinnet i dette arbeidet er ifølge Hough mfl. (1980: 16 i Garland, 1996: 452) «å identifisere personer eller organisasjoner som har kompetanse til å redusere kriminelle muligheter effektivt, og å vurdere både om de har et ansvar for å gjøre det, og om dette ansvaret kan håndheves». Budskapet i denne tilnærmingen er at staten alene ikke er, og ikke effektivt kan være, ansvarlig for å forebygge og kontrollere kriminalitet. Innbyggere og enkeltindivider må erkjenne at de også har et ansvar i dette arbeidet, samtidig som de må overtales til å endre egen praksis for å redusere kriminelle muligheter samt øke uformell kontroll (Garland, 1996).

Når det kommer til styring av cybersikkerhet kan vi også se at denne mentaliteten har relevans. I Nasjonal strategi for digital sikkerhet (2019) står det at Norge i 2017 fikk sin første stortingsmelding som utelukkende handler om digital sikkerhet. Norges statsminister, Erna Solberg, skriver følgende i rapportens forord: «Vi har alle en felles interesse av, og et ansvar for, å sikre våre verdier (2019: 3). Solberg avslutter forordet sitt med en oppfordring til Norges innbyggere om å blant annet ta eierskap til den nye nasjonale strategien for digital sikkerhet samt bidra til at den følges opp. I likhet med Neumann sitt eksempel om den tidligere helseministeren som oppfordrer samfunnsborgerne til å ta ansvar for sin egen helse, ser vi her at dagens statsminister oppfordrer samfunnsmedlemmer til å ta ansvar for sin egen digitale sikkerhet. Denne ansvarliggjøringen av samfunnsborgere og organisasjoner vil bli nærmere undersøkt i analysedelen.

3.2.3 Nodal governance

Sikkerhetsforvaltning (governance of security) handler om reaksjoner på trusler eller sikkerhetsbrudd som har funnet sted samt det å forutsi og hindre fremtidige trusler (Johnston og Shearing, 2003: 9). Den viktigste teoretiske innflytelsen på begrepet er Foucaults forestilling om government (Wood og Dupont, 2006). Teoretikere som skriver om governance of security er enige i at det i dag er flere som produserer sikkerhet i samfunnet og kaller denne trenden for pluralisering. For å illustrere denne pluraliseringen fremmer Shearing, Johnston, Wood og Burris en *nodal governance*-tilnærming (Johnston og Shearing, 2003; Burris, 2004 i Wood og Dupont, 2006).

Nodal governance handler om hvordan det moderne samfunnet, og da spesielt sikkerhets-feltet, har blitt fragmentert. Med andre ord produseres sikkerhet i dag gjennom flere ulike *noder* (Wood og Shearing, 2003). Noder kan forstås som organisatoriske steder der kunnskaper,

kapasiteter og ressurser blir mobilisert for å styre et hendelsesløp for å skape sikre og trygge omgivelser. I litteraturen hevdes det at en kan identifisere fire sentrale karakteristikker som nodene innehar, henholdsvis mentaliteter, teknologier, ressurser og institusjonelle strukturer (Wood og Dupont 2006). I denne oppgaven er det særlig mentaliteter som vil være relevant både fordi det i denne oppgaven, som nevnt innledningsvis, fokuseres på de menneskelige faktorene som påvirker forebygging av cyberkriminalitet, og fordi mentaliteter kan ha relevans for å avdekke logikker til informantene. Med andre ord, hvordan informantene snakker og tenker om fenomenet som undersøkes.

Mentaliteter blir forstått som måter å tenke på- et mentalt rammeverk som former vår oppfattelse og tenkning om omgivelsene våre, og som et resultat påvirker hvordan vi handler i situasjoner vi møter (Nøkleberg, 2016: 58). Sett i sammenheng med nodal governance refererer mentaliteter til nodens måte å tenke om seg selv og omgivelsene rundt seg, særlig med fokus på hvilken rolle eller ansvar den har (Johnston og Shearing, 2003 i Nøkleberg, 2016: 58). Det å ha kunnskap om nodens mentaliteter er derfor viktig for å forstå Wintershall Dea sin atferd. Innen sikkerhetsforvaltningen er det spesielt to mentaliteter som trekkes frem som viktige. Det er henholdsvis en straffeorientert og en risikoorientert mentalitet (Wood og Dupont, 2006). Den straffeorienterte er opptatt av reaktive strategier basert på straff, reaksjon og gjengjeldelse i forhold til forbrytelser og er knyttet til straffesystemet. Den risikoorienterte er proaktiv fordi den fokuserer på å forebygge kriminalitet. En risikoorientert mentalitet har et mer fremtidsrettet fokus, og sentralt her er vektleggelsen av instrumentelle kalkuleringer for å redusere kriminalitet, farer og risiko (Johnston og Shearing, 2003 i Nøkleberg, 2016: 58). Ettersom denne oppgaven handler om å forebygge cyberkriminalitet vil det være den risikoorienterte mentaliteten som er relevant. Det vil være interessant å undersøke om Wintershall Dea sitt arbeid med forebygging kan kobles til denne mentaliteten. Mentaliteter gjenspeiler hvordan de innen en node tenker om dens formål og rolle i det bredere miljøet (Martin, 2013: 149). Slik kan mentaliteter og kultur kobles sammen ved å forstå aktørers mentalitet som en del av kulturen som utvikler seg. Ved å undersøke kulturen til et selskap kan man videre avdekke hvilke logikker og mentaliteter som anvendes.

3.3 Sikkerhetskultur

Sammenhengene mellom kultur, sårbarhet og sikkerhet har fått stor oppmerksomhet de siste tiårene (Westrum, 1993 i Engen mfl., 2016: 156). Organisasjonskultur viser til den kulturen

som utvikles blant individer i en bestemt organisasjon eller gruppe (Sagberg, 2020). Både organisasjonskultur og kultur er fenomener som er mye omtalt, men som det ikke er enighet i hvordan skal defineres. En retning innenfor organisasjonskultur er *bedriftskultur*. Her forstås kultur som en egenskap ved en organisasjon, og forskere innenfor denne retningen mener det er mulig å styre ansatte i en bedrift ved hjelp av en sterk bedriftskultur (Eriksson-Zetterquist mfl., 2015). Edgar Schein (1985: 9 i Eriksson-Zetterquist mfl., 2015: 209), som befinner seg innenfor denne retningen, definerer kultur som:

> a) et sett av grunnleggende antakelser b) som har blitt etablert, tatt opp eller utviklet i en viss gruppe c) underveis mens gruppen har håndtert problemer den har støtt på i forbindelse med ekstern tilpasning og intern integrasjon, d) og som har fungert tilstrekkelig bra til å bli oppfattet som gyldig og derfor e) læres videre til nye medlemmer som den f) korrekte måten å oppfatte, tenke og føle på i forbindelse med denne typen problemer.

På grunn av organisasjoners stadig økende avhengighet av IKT-systemer, har de aldri vært mer sårbare for cyberangrep (Alshaikh, 2020). Nylige sikkerhetsrapporter viser at en betydelig andel av brudd på datasikkerhet skyldes ansattes manglende overholdelse av organisatoriske retningslinjer for informasjonssikkerhet, og sikkerhetsforskere mener derfor at det er viktig å bygge en cybersikkerhetskultur for å endre holdninger, oppfatninger og innprente god sikkerhetsatferd (Alshaikh, 2020: 1). Turner, som også skriver om kultur, framhever hvordan delte antagelser og normer styrer den kollektive oppmerksomheten og atferd i møte med farer og trusler (Engen mfl., 2016: 157) og kan slik ses i sammenheng med sikkerhetskultur. Det hevdes at cybersikkerhetskultur kan forbedre ansattes sikkerhetsatferd (Zakaria mfl., 2007 i Alshaikh, 2020). Lysneutvalget trekker også frem kultur i virksomheter som viktig for å beskytte seg mot digitale trusler, og mener videre at sikkerhetskultur er en viktig faktor i dette arbeidet. I rapporten står det blant annet at: «En god kultur for å ta de digitale trusler på alvor er avhengig av den generelle sikkerhetskulturen» (Lysneutvalget, 2015: 17).

Det har vært mange forsøk på å definere begrepet sikkerhetskultur. Nasjonal sikkerhetsmyndighet definerer det som: «summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd» (NSM, 2021). Da Veiga mfl. (2020: 19) definerer cybersikkerhetskultur som:

> contextualized to the behavior of humans in an organizational context to protect information processed by the organization through compliance with the information security policy and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives.

Denne beskrivelsen trekker frem fire viktige faktorer for en god cybersikkerhetskultur. Disse er regelmessige initiativer for kommunikasjon og sikkerhetsopplæring samt trening og bevissthet. Denne tilnærmingen kalles for SETA (security education, traning og awarness), og hevdes av forskere som viktige for å forbedre cybersikkerhetskulturen og dermed beskytte organisasjoner mot sikkerhetshendelser knyttet til ansatte (Alshaikh, 2020). Sikkerhetskultur kan forbedre ansattes sikkerhetsatferd, og er derfor viktig for å forhindre cyberangrep som skyldes ansattes manglende overholdelse av organisatoriske sikkerhetspolitikker. Det krever en betydelig innsats av virksomheter å endre ansattes sikkerhetsatferd samt å få informasjonssikkerhet til å bli en naturlig del av deres hverdag. Derfor må en SETA-tilnærming gå utover årlig sikkerhetstrening og innta en bredere tilnærming for å klare å endre holdninger, oppfatninger, rutiner og antagelser samt utvikle nye ferdigheter. Virksomheter må derfor endre hvordan de implementerer sikkerhetstrening samt utvikle en cybersikkerhetskultur der sikkerhet er «alles ansvar», og hvor det å gjøre det rette ses som normen i selskapet (Da Veiga mfl., 2020). Denne tankegangen kan kobles til mentaliteten i ansvarliggjøringsstrategien. Som nevnt over ser vi at den nasjonale strategien for digital sikkerhet (2019) også skriver at cybersikkerhet er alles ansvar. For å få til en slik mentalitet, at alle blir ansvarlig for eget ansvar i organisasjoner, mener altså Da Veiga mfl. (2020) at man må sette fokus på kultur.

Kultur og ledelse henger tett sammen (Eriksson-Zetterquist, 2015). Schein mener at dannelse av en kultur først og fremst avhenger av lederne i organisasjonen. Det er ledere som setter standarden for hvordan man tenker og handler, og disse blir videre akseptert og fulgt av de ansatte (Schein, 2010 i Whelan**,** 2017). Et utgangspunkt for de fleste definisjoner av lederskap er at ledere har stor betydningen for hvordan virksomheter organiseres og for deres fremgang. Selv om dette synet på lederskap har vært problematisert de siste årene, legger fortsatt mange definisjoner vekt på at ledere blant annet bestemmer organisasjoners retning og strategi og leder endringsprosesser i den riktige retningen (Eriksson-Zetterquist, 2015). Ledelse er derfor en viktig faktor som påvirker selskapers cybersikkerhetskultur, og er relevant når jeg undersøker hvordan Wintershall Dea forebygger cybersikkerhet. Dersom ledere legger føringer på hvordan

ansatte ser på cybersikkerhet, vil de være en viktig faktor i arbeidet med å forebygge cyberkriminalitet. NSM ser at sikkerhetsengasjerte ledere har stor betydning for sikkerhetstilstanden i virksomheter. Hvis virksomheter har en ledelse som er fraværende i sikkerhetsspørsmål kan det føre til at avstanden til sikkerhetsarbeidet blir for stor. Det kan også føre til at det blir vanskeligere å beslutte, gjennomføre og evaluere tiltak som er relevante (NSM, 2020: 41).

Tillit er en annen faktor som påvirker selskapers sikkerhetskultur. For å skape og utvikle en god sikkerhetskultur er det viktig at det er gjensidig tillit mellom arbeidsgiver og ansatt, og mellom ansatte i organisasjonen. Samarbeid basert på gjensidig tillit er nødvendig for en effektiv sikkerhetskultur og for utviklingen av en informasjonssikkerhetskultur. Tillit mellom alle parter i en organisasjon kan føre til harmonisering av kunnskap, verdier og atferd hos både arbeidsgiver og ansatte og kan videre bidra til en vellykket utvikling av sikkerhetskulturen (Da Veiga, 2020).

3.4 Situasjonell kriminalitetsforebygging

Situasjonell kriminalitetsforebygging søker å redusere samfunnets onder og forbedre livskvaliteten ved å endre utformingen av produkter, systemer og miljøer. Dette kan variere fra enkle og billige tiltak til komplekse og dyre teknologier (Farrell, 2010). Den underliggende forutsetningen for perspektivet er at kriminelle er rasjonelle vesener som avveier kostnadene og fordelene ved sin atferd (Clarke, 1995 i Brewer, 2019: 18). Derfor må vellykkede kriminalitetsforebyggende tiltak innebære å designe og manipulere menneskelige miljøer for å gjøre lovbryternes beslutninger om å involvere seg i kriminalitet mindre attraktivt (Clarke, 1995 i Brewer, 2019: 18). Hvis det er lett å gjennomføre et innbrudd i en bil eller et hus er det større sannsynlighet for at flere lar seg friste til å begå innbrudd. Strategien har dermed en handlingsorientert tilnærming til forebygging hvor fokuset flyttes fra individet og til den kriminelle handlingen og vektlegger selve områdene og omgivelsene hvor kriminalitet finner sted (Brewer, 2019). Hvis lovbryteren som vurderer å gjennomføre innbrudd i et hus eller en bil ser at området er videoovervåket eller har alarm vil risikoen for å bli oppdaget oppleves større og kan slik påvirke valget om å gjennomføre lovbruddet.

I tillegg til å manipulere fysiske rom for å avverge muligheten for lovbrudd kan man også manipulere den virtuelle verden. Myndigheter, private selskaper og enkeltpersoner over hele

verden benytter et bredt spekter av tekniske verktøy i et forsøk på å redusere sannsynligheten for å bli ofre for cyberkriminalitet. Mange av disse verktøyene og prosedyrene faller inn under kategorien situasjonell kriminalitetsforebygging og bruk av slike tiltak har blitt den vanligste formen for intervensjon i arbeidet med å forebygge cyberkriminalitet (Brewer, 2019). Eksempler på slike teknikker er bruk av brannmur, passord og antivirusprogrammer samt systemer som oppdager svindel og fjerning av nettsider (Brewer, 2019: 20). Selv om kriminologisk forskning viser at situasjonelle forebyggende teknikker er nyttige for å forebygge tradisjonell kriminalitet er det fortsatt uklart om slike inngrep kan forhindre cyberkriminalitet. Brewer mener det finnes lite bevis for effektiviteten av sikkerhetsverktøy for å forebygge og redusere cyberkriminalitet. Når det gjelder effektiviteten av antivirusprogrammer viser det seg at de fleste produkter er i stand til å oppdage og forhindre de fleste skadelige angrep. Men det er fortsatt ukjent om andre situasjonelle forebyggingsteknikker som brannmurer og bruk av passord effektivt reduserer cyberkriminalitet. Brewer (2019) mener derfor at det er viktig å vurdere effektiviteten av disse strategiene i større grad når det kommer til anvendelse i digitale sammenhenger.

I dette kapittelet har jeg presentert litteratur som viser hvordan risiko og sikkerhet kan forstås i det moderne samfunn. Denne litteraturen vil benyttes for å undersøke hvordan ekspertene og ansatte i Wintershall Dea forstår risiko og sikkerhet. Videre har jeg presentert det teoretiske rammeverket for oppgaven ved å vise til Foucualt og Garlands styringslogikker *governmentality* og *ansvarligjøringsstrategi*. Disse illustrerer hvordan stater kan styre og kontrollere samfunn, og vil benyttes for å undersøke både hvordan cyberkriminalitet og cybersikkerhet styres i Norge, samt hvilke føringer dette har for hvordan Wintershall Dea jobber med forebygging av fenomenet. Videre har jeg presentert teorier om kultur, sikkerhetskultur og nodal governance som er viktige faktorer i forebyggingsarbeidet. Til slutt har jeg presentert perspektivet om situasjonell kriminalitetsforebygging som vil brukes for å undersøke om selskapet anvender noen av disse tiltakene i sitt forebyggende arbeid.

4 Metode

Målet med datainnsamlingen har ut fra oppgavens forskningsspørsmål og tema vært å innhente et materiale som belyser cybersikkerhet og cyberkriminalitet samt hvordan dette kan forebygges. I dette kapitlet vil jeg beskrive avhandlingens fremgangsmåte og redegjøre for hvilke data som er benyttet, samt begrunne valgene som er tatt. Metodekapittelet vil belyse forskningsmetoden og designet. Først vil kapittelet presentere hvorfor valget falt på å gjennomføre en avhandling med både kvalitativt og kvantitativt datamateriale, noe som defineres som et flermetodedesign. Deretter vil datainnsamlingsprosessen for det kvalitative materialet presenteres før gjennomføringen av intervjustudien beskrives. Etter dette vil jeg forklare hvordan datainnsamlingsprosessen for det kvantitative materialet ble gjort før jeg presenterer hvordan spørreundersøkelsen ble planlagt, utformet og gjennomført. Videre vil den analytiske fremgangsmåten for det kvalitative og kvantitative materialet beskrives før jeg til slutt presenterer oppgavens datakvalitet og etiske refleksjoner.

4.1 Flermetodedesign

Avhandlingen undersøker fenomenet cyberkriminalitet gjennom ansatte i selskapet Wintershall Dea sine opplevelser, erfaringer og forståelser med å forebygge den type kriminalitet gjennom cybersikkerhet. For å undersøke dette har jeg benyttet meg av flermetodedesign. Det betyr at oppgaven er en kombinasjon av kvalitative og kvantitative data gjennom individuelle intervjuer og elektronisk spørreskjema. For å besvare oppgavens problemstilling anså jeg flermetodedesign som hensiktsmessig da bruk av kvalitative og kvantitative studier kan utfylle og styrke hverandre (Skilbrei, 2019: 17).

Jeg var interessert i menneskers forståelser og meninger om fenomenet cybersikkerhet, samt hvordan selskapet opplever og beskytter seg mot cyberkriminalitet. Temaet er komplekst og har behov for detaljerte forklaringer. Når dette er tilfellet kan en kvalitativ tilnærming være relevant å bruke (Skilbrei, 2019). På bakgrunn av oppgavens problemstilling har jeg valgt å benytte meg av kvalitative intervjuer for å oppnå grundige og nøyaktige beskrivelser for å besvare forskningsspørsmålet (Ringdal, 2013). Det kvalitative datamaterialet baserer seg på syv individuelle intervjuer med ansatte i Wintershall Dea Norge. Disse informantene vil videre i oppgaven refereres til som *eksperter* for å tydelig vise skille mellom empirien fra de kvalitative intervjuene og den kvantitative spørreundersøkelsen. I tillegg til det kvalitative intervjuet har jeg gjort et litteratursøk og sett nærmere på et utvalg av dokumenter som har relevans for temaet.

Dette betegnes som «tilleggsdata», og kombineres med intervjuene for å beskrive offisielle intensjoner som er relevant for studien (Tjora, 2012). Følgende offentlige dokumenter er valgt ut: *Nasjonal strategi for digital sikkerhet* (Departementene, 2019), *Digital sårbarhet – sikkert samfunn* (NOU 2015: 13), og *Digitale sårbarheter Olje & Gass* (Lysneutvalget, 2015). Disse anvendes for å forstå konteksten Wintershall Dea opererer i og vil fungere som et bakteppe og innramming av intervjumaterialet.

I tillegg til det kvalitative materialet har jeg laget og sendt ut et elektronisk spørreskjema til ansatte i Wintershall Dea som jobber i Stavanger, Bergen og offshore. Hensikten med spørreskjemaet var å få innsikt i hvilken kunnskap ansatte som ikke jobber med cybersikkerhet har om temaet, for så å sammenligne svarene med informasjonen fra ekspertene. Det ville være interessant å undersøke om det er et gap, eller et spenningsfelt, mellom ekspertenes tanker rundt hva ansatte kan, og det ansatte gir uttrykk for at de kan. Dette var også interessant å studere da det kan være et viktig punkt i forhold til forebyggingsstrategien selskapet har til cyberkriminalitet. Spørreundersøkelsen ble særlig aktuell da intervjuer med ekspertene avdekket at selskapets cybersikkerhet avhenger av hvordan den enkelte ansatte ivaretar sikkerheten. Ansatte som har svart på spørreskjemaet vil videre i oppgaven refereres til som *respondenter* for å skille mellom empirien.

Det kvantitative materialet fungerer i denne oppgaven som et supplement til det kvalitative. Det vil si at hovedvekten ligger på det kvalitative innsamlede materialet. Ved bruk av flermetodedesign har innhentingen av empirien tatt lang tid og videre resultert i et omfattende metodekapittel. Dette anser jeg som en styrke for oppgaven.

4.2 Datainnsamlingsprosessen – Kvalitativt intervju

4.2.1 Utvalg 1: Individuelle intervjuer med eksperter

Jeg ønsket å skape forståelse og kunnskap om et fenomen som preger dagens samfunn, og har derfor benyttet meg av kvalitative intervjuer av informanter som står i denne situasjonen (Skilbrei, 2019). Jeg har gjennomført syv individuelle intervjuer med ansatte i Wintershall Dea som på ulike måter besitter en stilling hvor cybersikkerhet er en del av arbeidsdagen. Cybersikkerhet er et komplekst tema og trenger ofte tekniske og dype forklaringer. Noen av informantene jobber direkte med cybersikkerhet, andre mer perifert. Det vil si at informantene

besitter ulik kunnskap om temaet for oppgaven, og på denne måten kan gi ulik informasjon og forståelse.

Ettersom informantene jobber med cybersikkerhet på ulike måter valgte jeg å gjennomføre individuelle intervjuer. På denne måten håpet jeg at de individuelle fortolkningene skulle komme klarere frem enn hvis jeg hadde valgt å gjennomføre intervjuer med flere til stede (Skilbrei, 2019). På den andre siden kan gruppeintervjuer «gi tilgang til en gruppedynamikk med hensyn til meningsdannelse på en måte individuelle intervjuer ikke gjør» (Skilbrei, 2019: 69). Når deltakere i et gruppeintervju hører hverandres refleksjoner og erfaringer kan det påvirke hva de selv tenker og husker. Slik kan nye temaer som ikke var planlagt av forskeren på forhånd, komme frem (Skilbrei, 2019: 69). I og med at informantene besitter ulik kunnskap om cybersikkerhet kunne gruppeintervju gitt meg klarere ulikheter om temaet. Likevel falt valget på individuelle intervjuer. Dette var blant annet fordi jeg ikke ønsket at informantene som jobber direkte med cybersikkerhet og derfor sannsynligvis vet mer om temaet skulle «overskygge» deltakerne som jobber mer perifert med cybersikkerhet. Samtidig kunne et gruppeintervju ført til at de som jobber mer perifert med temaet ville fått vanskeligheter med å ta ordet, ved at de for eksempel hadde følt at det de tenker og erfarer ikke er like viktig sammenlignet med de som jobber direkte med cybersikkerhet.

4.2.2 Rekruttering og adgang til felt

Gjennom en bekjent ble jeg tipset om å ta kontakt med Ole Martin Dahle (heretter referert til som Dahle), som er helse- miljø- og sikkerhetsdirektør i Wintershall Dea. Min bekjent visste at selskapet har inngått samarbeid med masterstudenter tidligere. I desember 2019 tok jeg kontakt med Dahle for å høre om muligheten for et samarbeid. Jeg fikk raskt positiv respons og etter et par mailutvekslinger ble det avtalt at Dahle skulle være min kontaktperson fra selskapet. I april 2020 hadde jeg et videomøte med Dahle, en fra IT- avdelingen og en fra HR- avdelingen hvor jeg presenterte mine tanker rundt prosjektet. Jeg ønsket, som tidligere nevnt, å intervjue mennesker som har god kunnskap og erfaring med cybersikkerhet, og formidlet derfor at slike informanter kunne belyse problemstillingen for oppgaven. Dahle ønsket å gi meg et overordnet blikk over hvordan selskapet jobber med cybersikkerhet og tok utgangspunkt i dette samt mine ønsker da han foreslo informanter. Slik har jeg foretatt et strategisk utvalg av informanter til oppgaven. I møte diskuterte vi også hvordan spørreundersøkelsen kunne foregå, samt gikk gjennom en samarbeidsavtale som er signert av selskapet, min veileder fra UiO og meg (

Vedlegg F). I tillegg fikk vi avtalt hvilken periode intervjuene og spørreundersøkelsen skulle finne sted.

Å rekruttere gjennom en organisasjon gjorde prosessen både raskere og lettere for meg som forsker. Dersom jeg hadde tatt førstekontakt med potensielle informanter selv, er det sannsynlig at dette arbeidet ville tatt lengre tid samt at jeg kunne endt opp med informanter som ikke hadde kunnskap om avhandlingens tema. Det var likevel ikke garantert å få tak i ønskede informanter ved å rekruttere via en organisasjon, men jeg så det som større sannsynlig. Dette fordi Wintershall Dea er et stort selskap med egen IT-avdeling. Det var derfor sannsynlig at de som jobber i IT-avdelingen sitter med relevant innsikt og kunnskap om avhandlingens forskningsspørsmål.

Det er likevel viktig å nevne at å rekruttere gjennom en organisasjon kan by på ulike utfordringer (Skilbrei, 2019). Ettersom Dahle tok seg av utvelgelsen av informanter mistet jeg som forsker kontroll over denne prosessen. Dette kunne ført til at jeg hadde sittet igjen med andre informanter enn det jeg ønsket. For å unngå dette presiserte jeg hvilke informanter jeg var interessert i og hvorfor til Dahle. I tillegg kunne Dahle, som mellomledd, hatt et eget ønske om hvem som skulle delta i prosjektet for å for eksempel sikre Wintershall Dea sitt behov og perspektiv, og derfor gått vekk fra mine ønsker. Dersom de nevnte mulige konsekvensene hadde vært tilfellet for denne avhandlingen, kunne jeg som forsker sittet igjen med ett datamateriale som ikke er representativt for fenomenet som undersøkes. Jeg opplever imidlertid ikke at dette har vært tilfellet for denne oppgaven. Dahle ønsket å gi meg et helhetsbilde av selskapets arbeid med cybersikkerhet og har ut ifra det valgt informanter som har god erfaring med og informasjon om undersøkelsens fenomen. Gjennom intervjuene har jeg heller ikke opplevd at det er personer/roller jeg gjerne skulle intervjuet som jeg ikke har fått tilgang til. Jeg sitter derimot igjen med opplevelsen av at alle relevante roller har deltatt.

Ved å bruke et mellomledd i rekrutteringsprosessen måtte jeg også tenke over hvilke problemer det kunne skape rundt anonymitet og samtykke. I juni 2020 hadde jeg et oppfølgingsmøte med Dahle og samme person fra IT-avdelingen. Her diskuterte vi hvordan eventuelle informanter skulle få informasjon om forskningsprosjektet og forespørsel om å delta. Siden jeg ønsket å intervjue ansatte som jobber direkte med cybersikkerhet ville jeg at Dahle skulle sende ut informasjon til potensielle informanter. Det var viktig at deltakelsen var frivillig og at informantene ikke skulle føle at de måtte takke ja til et intervju selv om de jobber i et selskap

som samarbeider med et masterprosjekt (Skilbrei, 2019). Det er sannsynlig å tenke at den ansatte fra IT – avdelingen har en nærere relasjon til informantene, og at det derfor er større sannsynlighet for at noen hadde takket ja til å delta selv om de egentlig ikke ønsket. Ved at Dahle sendte ut informasjon håpet jeg å unngå dette. På den andre siden kan det også tenkes at man kan føle et press på å delta i et prosjekt når en direktør i selskapet sender ut informasjon.

Ettersom denne avhandlingen har behandlet og oppbevart personopplysninger måtte prosjektet meldes til Norsk senter for forskningsdata (NSD). Da NSD hadde godkjent prosjektet (Vedlegg B), sendte Dahle ut informasjon til aktuelle informanter, og ga meg kontaktopplysninger til disse personene. Deretter sendte jeg mail til hver enkelt for å høre om de ønsket å stille til intervju, og kontakten fra dette tidspunktet var kun mellom aktuelle informanter og meg. Det ble ikke videreformidlet fra meg til selskapet hvem som endte opp med å delta, og deltakerne ble informert om at det ikke ville ha en negativ påvirkning til arbeidsplass og arbeidsgiver dersom de takket nei.

4.2.3 Semistrukturert intervju og utarbeidelse av intervjuguide

I forkant av intervjuene utviklet jeg en intervjuguide med en liste over tema og spørsmål som jeg ønsket å stille. Jeg ønsket at informantene skulle snakke om konkrete temaer og erfaringer knyttet til cybersikkerhet og cyberkriminalitet, og benyttet meg av intervjuguiden for å pense dem inn på disse (Skilbrei, 2019). Temaene ble utviklet ved en deduktiv tilnærming, og var delt inn i fem følgende kategorier: *Bakgrunn og kompetanse*, *Forebygging*, *Svindel*, *Sikkerhet* og *Koronapandemien*. Rekkefølgen på spørsmålene varierte fra intervju til intervju for å oppnå bedre flyt og for å skape rom for at informantene kunne ta opp andre temaer og snakke fritt om disse (Skilbrei, 2019). Samtidig ble ikke intervjuguiden fulgt slavisk fordi jeg stilte oppfølgingsspørsmål dersom informantene sa noe jeg ønsket å følge opp eller kom inn på andre temaer jeg opplevde som spennende for oppgaven. Slik kan intervjustilen for denne avhandlingen omtales som semi-strukturert (Skilbrei, 2019: 127).

Informantene i denne avhandlingen besitter en del sensitiv informasjon som Wintershall Dea ikke ønsker skal lagres noe sted. Derfor ble intervjuene delt i to: en generell del hvor jeg tok lydopptak og en mer detaljert del hvor jeg noterte for hånd. De to første kategoriene: *Bakgrunn og kompetanse* samt *forebygging* ble tatt opp med lydopptaker slik at jeg kunne rette all oppmerksomhet til informantene (Thaagard, 2013). Denne delen refereres til som del en av

intervjuene. For å ta lydopptak brukte jeg *nettskjema-diktafon* appen fra UiO som er en sikker måte å ta opp intervjuer på, blant annet fordi opptakene umiddelbart krypteres på telefonen og man aldri kan lytte til opptak på mobilappen (UiO, 2021). De neste tre kategoriene: *Svindel, sikkerhet* og *koronapandemien* ble notert for hånd, og refereres til som del to av intervjuene. Ettersom det ikke ble brukt lydopptaker i del to har jeg valgt å kun bruke direkte sitater i analysen fra del en av intervjuene. Det skyldes at jeg ikke kan være helt sikker på at respondentene blir sitert riktig (Tjora, 2017: 168) og har resultert i at notatene fra del to ikke er like omfattende som materialet fra del en. Det er viktig å nevne at jeg likevel sitter igjen med opplevelsen av gode data fra både del en og del to av intervjuene.

Ettersom jeg intervjuet mennesker som jobber med cybersikkerhet og at temaet for oppgaven ikke innebar personlige spørsmål om deltakernes liv, så jeg det ikke hensiktsmessig å sende ut intervjuguiden på forhånd. I stedet ga jeg informantene informasjon om hva intervjuet skulle handle om gjennom informasjonsskrivet som ble sendt ut i forkant, samt i mailen som ble sendt for å avtale tidspunkt (Skilbrei, 2019: 128). I tillegg startet hvert intervju med å gå gjennom hvordan intervjuet ville foregå og hvilke kategorier det var delt inn i. I ettertid ser jeg at det kunne vært en fordel å sende intervjuguiden på forhånd fordi noen av spørsmålene var litt vanskelige å svare på. For eksempel fikk deltakerne spørsmål om hvordan de ville definere cybersikkerhet, og det tok litt tid for flere informanter før de fikk formulert et svar. Likevel opplever jeg ikke at dette har hatt konsekvenser for datamaterialet til oppgaven.

Dersom en intervjustudie består av intervjuer med informanter som representerer ulike grupper er det vanlig å utvikle flere intervjuguider (Skilbrei, 2019: 128). I ettertid ser jeg at jeg kunne hatt to ulike intervjuguider, en til de som jobber direkte med cybersikkerhet og en til de som jobber mer perifert med temaet. Dette fordi jeg opplevde at de som jobber direkte med cybersikkerhet hadde lettere for å svare på spørsmålene og mer å si gjennom intervjuet. Intervjuguiden til informantene som ikke jobber direkte med cybersikkerhet kunne bestått av samme tema, men spørsmålene kunne vært mer tilpasset det de jobber med (Skilbrei, 2019: 128). Slik kunne jeg fått et grundigere overblikk og et mer helhetlig bilde over selskapets organisering rundt cybersikkerhet, samtidig som det kunne gitt ny kunnskap rundt temaet for oppgaven. Likevel opplevde jeg at alle informantene var flinke til å gi utfyllende svar, selv der de ikke var så sikre på det de ble spurt om. I disse tilfellene rettet deltakerne spørsmålet inn til sitt arbeidsområde og snakket om cybersikkerhet i forhold til det. Jeg måtte på grunn av dette

som forsker også være flinkere til å tenke utover temaet. Til sammen kan dette ha gitt meg kunnskap jeg ellers ikke ville fått.

4.3 Gjennomføring av intervjustudien

4.3.1 Intervjusituasjonen

For å gjennomføre intervjuene fulgte jeg Tjora (2017) sine tre faser – oppvarming, refleksjon og avrunding. Hvert intervju startet med at jeg presenterte meg selv og forklarte hvordan intervjuet ville fungere. Selv om de var informert om dette i informasjonsskrivet ønsket jeg å gjenta informasjon om studien og deres rettigheter for å sjekke at intervjuobjektene hadde forstått informasjonsskrivet (Skilbrei, 2019). I ettertid ser jeg at jeg i starten av intervjuene burde vært tydeligere på hva jeg ønsket å få ut fra samtalen da et par av informantene spurte om dette. Deretter gikk jeg over til et par enkle og konkrete åpningsspørsmål som handlet om informantenes bakgrunn og kompetanse. Ved å starte på denne måten håpet jeg å skape en trygghet hos respondenten om at hen behersket situasjonen (Tjora, 2017: 146).

Etter åpningsspørsmålene gikk jeg over til fase to – refleksjonsspørsmål, hvor kjernen i intervjuet dannes. Spørsmålene i denne fasen gikk inn i dybden av temaet for oppgaven. I de første intervjuene var jeg nøye på å følge intervjuguiden. Dette skyldtes at jeg var usikker på meg selv som intervjuer. Etter hvert intervju ble jeg mer sikker på meg selv og klarte å løsrive meg fra intervjuguiden. Det førte til at samtalene ble friere og fikk bedre flyt. Samtidig ble det lettere å følge opp med spørsmål dersom informantene kom inn på andre tema, og slik få ny kunnskap jeg ikke ville fått hvis jeg hadde fortsatt å være så opptatt av å følge intervjuguiden. Semistrukturerte intervjuer gir større rom for improvisasjon og intervjueren får dermed større mulighet til å påvirke informanten. For å unngå dette hentet jeg oppfølgingsspørsmål fra en forberedt liste (Ringdal, 2013: 243). På tross av dette hendte det i flere tilfeller at jeg kom på disse underveis, alt etter hva informantene fortalte. I disse tilfeller kan det dermed tenkes at jeg ikke har klart å være så nøytral som ønsket, men at jeg i stedet har ledet samtalen inn på en bestemt vei. Ved å stille oppfølgingsspørsmål ønsket jeg å gi tilbakemelding på at det informanten sa var interessant og vise at jeg fulgte med i samtalen. Ettersom cybersikkerhet er et komplekst tema oppstod det noen ganger et behov fra meg om å få informantene til å forklare bestemte faguttrykk. Samtidig opplevde jeg at informantene er klar over kompleksiteten i det de jobber med da flere spurte meg om jeg forstod hva de mente, eller om jeg hadde hørt om det

før. Dette er et godt eksempel på at informantene mine var samarbeidsvillige og ønsket at jeg skulle forstå temaet i tillegg til å sitte igjen med et godt materiale.

Etter refleksjonsspørsmålene gikk jeg over til fase tre – avrunding. Her forsøkte jeg å avrunde intervjuet på en måte som kunne oppleves behagelig for informantene. Etter hvert intervju takket jeg for samtalen og spurte om det var noe informantene ønsket å gå igjennom eller tilføre. I tillegg ga jeg beskjed om at de gjerne måtte ta kontakt i ettertid dersom det skulle dukke opp spørsmål eller de kom på noe de ønsket å tilføre. I flere intervjuer fikk jeg tilbakemelding på at samtalen var nyttig også for informantene da de fikk reflektert over cybersikkerhet og arbeidsdagen sin på en ny måte, samt at de fikk tenkt over hvor viktig det de arbeider med er. Flere ga meg også tips til videre lesing og samtlige av informantene ville jeg skulle ta kontakt hvis det dukket opp noen spørsmål i ettertid. En av deltakerne anbefalte også et virtuelt kurs som skulle holdes av *Norsk informasjonssikkerhetsforum* (ISF) første september 2020. Jeg sendte forespørsel om å delta på kurset og fikk positiv respons. Kurset handlet blant annet om sikkerhetskultur og sikkerhetsatferd og var veldig lærerikt å delta på. For eksempel ble jeg introdusert for tiltaket *champion program* som organisasjoner kan implementere i arbeidet med cybersikkerhet. Dette begrepet anvendes i avhandlingens analysekapittel.

4.3.2 Tid og sted for intervju

Ekspertene fikk selv velge om de ønsket å gjennomføre intervjuet på selskapets lokaler eller over kommunikasjons – og samarbeidsplattformen Teams. Slik håpet jeg at de ville oppleve de valgte omgivelsene rundt intervjuet på en positiv måte (Tjora, 2017), og at det videre kunne hjelpe meg å få gode data. På grunn av Covid – 19 var intervjuobjektene på daværende tidspunktet vant til å ha møter og annen kommunikasjon over Teams. Dette kan forklare at seks av syv intervjuer tok sted over Teams samt bekrefte at deltakerne var komfortable med denne løsningen. Selv om jeg ikke var i samme rom som informantene fikk jeg likevel sett ansiktene til alle utenom i ett intervju hvor vedkommende ikke hadde fått satt opp kamera på hjemmekontoret sitt. Her opplevde jeg at det var vanskeligere å få bekreftelse på at intervjuobjektet forstod hva jeg mente fordi jeg mistet elementer som bekreftende nikk underveis. Ett av intervjuene tok sted på kontoret til den ansatte. Det var lærerikt å oppleve en slik intervjusituasjon samtidig som det var vanskeligere å notere underveis, spesielt i del to av intervjuet, da jeg kjente et større press på å ikke se for mye ned på notatarket mitt. Det resulterte i at notatene fra intervjuet ikke var like utfyllende som de andre.

Det var satt av 45 til 60 minutter på hvert intervju og informantene fikk selv velge dag innenfor en gitt ramme på tre uker. Tidsrammen skyldtes at jeg reiste til Stavanger for å gjennomføre intervjuene da to informanter ønsket å ha det på selskapets lokale. Ett av disse intervjuene ble flyttet til Teams, det andre ble holdt på selskapets lokale. Samtlige informanter satt av tid i løpet av arbeidsdagen sin. Derfor var jeg i samtalen tydelig på at dersom vi snakket over avsatt tid var det fullt forståelig om de måtte avslutte. Da noen av intervjuene passerte 60 minutter ønsket samtlige av disse informantene å snakke videre. Jeg opplevde at intervjuobjektene mine var svært interessert i og opptatt av cybersikkerhet. Dette kan skyldes at de besitter arbeidsoppgaver som har med temaet å gjøre og har nok vært en stor fordel for meg i intervjusituasjonene og for datamaterialet. Det var også derfor disse informantene ble valgt ut av Dahle, fordi de er eksperter på cybersikkerhet. Det har gitt meg bekreftelse på at Dahle har rekruttert gode og relevante informanter til forskingsprosjektet.

4.4 Datainnsamlingsprosessen – Spørreundersøkelsen

En spørreundersøkelse er «en systematisk metode for å samle inn data fra et utvalg personer, som i denne avhandlingen er ansatte i Wintershall Dea, for å gi en statistisk beskrivelse av den populasjonen utvalget er trukket fra» (Groves et al., 2004 i Ringdal, 2013: 190).

4.4.1 Undersøkelsens populasjon og utvalg

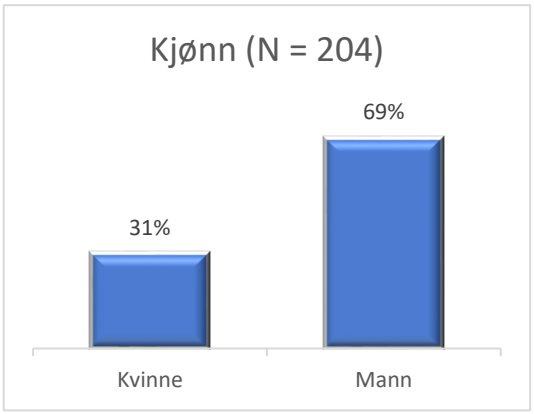
Hvert år har Wintershall Dea en «Safety Day» hvor alle ansatte skal delta. Målet med dagen er at ansatte skal få informasjon og kunnskap om ulike tema på ulike stands. Opprinnelig var planen at jeg skulle delta på «Safety Day» i oktober 2020, og dele ut spørreskjemaet ved IT-teamet sin stand. På grunn av korona hadde ikke IT-teamet stand likevel. Derfor falt valget på et elektronisk spørreskjema, og slik startet prosessen med å lage dette.

Populasjonen for avhandlingens spørreundersøkelse er alle ansatte (og innleide) i Wintershall Dea Norge, i perioden 17. november 2020 til 15. desember 2020. På daværende tidspunkt hadde selskapet ca. 540 ansatte. Undersøkelsen mottok 204 svar, noe som utgjør en svarprosent på 38%. Å vurdere frafall er viktig når en skal vurdere hvor god en undersøkelse er (Ringdal, 2013: 261). Generelt kan vi si at vi opererer med to ulike typer frafall: 1) frafall av respondenter, som vil si personer som ikke svarer på undersøkelsen i sin helhet, og 2) frafall på enkeltspørsmål, som vil si de som deltar på undersøkelsen, men som ikke har svart på alle spørsmålene

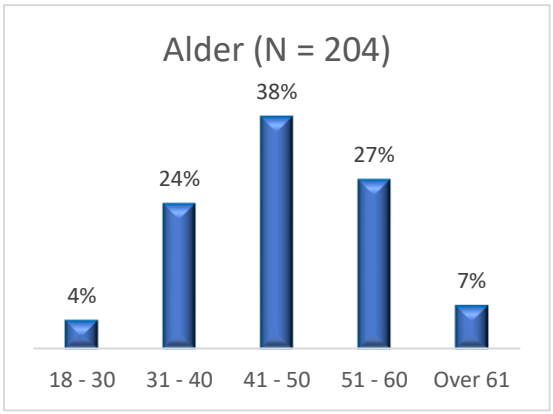
(Jacobsen, 2015: 306). Forskning viser en trend med fallende svarprosenter når det kommer til spørreskjemaer, og for spørreskjemaer som er sendt ut til organisasjoner viser forskning at gjennomsnittlig svarprosent ligger på 37, 2 prosent (Baruch og Holtom, 2008). Slik sett er svarprosenten for avhandlingens spørreundersøkelse det man kan forvente, eller til og med over hva en normalt kan forvente. Når det kommer til frafall på enkeltspørsmål vil dette poengteres i analysen der frafallsprosenten er høy eller skiller seg ut fra de andre spørsmålene. Videre i avsnittet vil demografisk informasjon om spørreskjemaets utvalg presenteres.

Kjønn og alder

Figur 4-1 viser at 69% av respondentene er menn og 31% er kvinner. Menn er altså klart overrepresentert i denne undersøkelsen. Dette samsvarer med kjønnsfordelingen i Wintershall Dea som helhet og det kan dermed antas at spørreundersøkelsen har et representativt utvalg når det kommer til kjønn. Figur 4-2 viser at aldersspennet er fra 18 år til 65 år og flertallet av informanter er mellom 41-50 år.



Figur 4-1: Kjønnsfordeling.

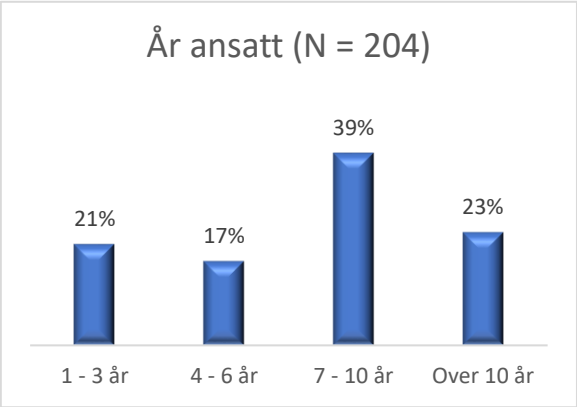


Figur 4-2: Aldersfordeling.

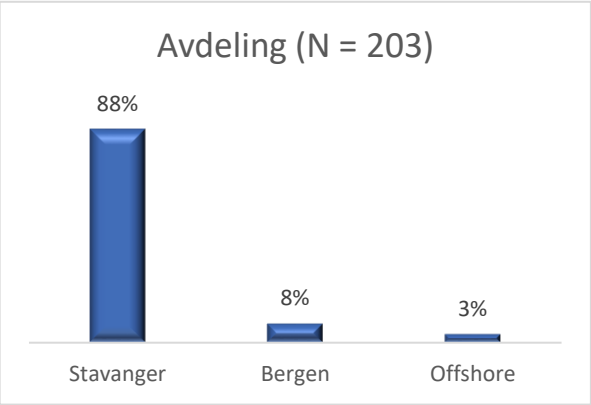
År ansatt og tilhørighet

Figur 4-3 viser at flertallet av de som har svart på undersøkelsen har vært ansatt mellom 7-10 år. Figur 4-4 viser at 88% av respondentene hører til kontoret i Stavanger, 8% jobber i Bergen og 3% jobber offshore (1% har ikke svart). Stavanger kontoret har betydelig flere ansatte enn Bergen kontoret og dermed kan det synes som spørreundersøkelsen har en relativt god representasjon når det kommer til disse lokasjonene. Når det kommer til svarprosenten fra offshore synes det derimot å være et lavt antall respondenter i forhold til antall ansatte på denne lokasjonen som på dette tidspunktet var 110 personer (utgjør ca. 20% av alle ansatte i selskapet). I tillegg er det flere ansatte offshore enn i Bergen, likevel ser man at svarprosenten er lavere for

offshore enn Bergen. Dermed kan det tenkes at resultatet fra spørreundersøkelsen ikke vil være representativt for ansatte som jobber offshore. Den lave svarprosenten fra denne gruppen kan forklares med at arbeidssituasjonen til offshore-arbeidere er annerledes enn de som jobber onshore. For det første tilbringer de ikke arbeidsdagen foran en pc. For det andre jobber de turnus. Undersøkelsesperioden dekker kun to offshore skift (2 x 2 uker) slik at et skift har hatt friperiode når undersøkelsen har vært i sirkulasjon. Dermed er det primært de som har vært fysisk på jobb som har lest mail og eventuelt valgt å delta. På tross av en tilsynelatende skjevhet har jeg ikke valgt å inkludere noe vekting i de deskriptive analysene mine.



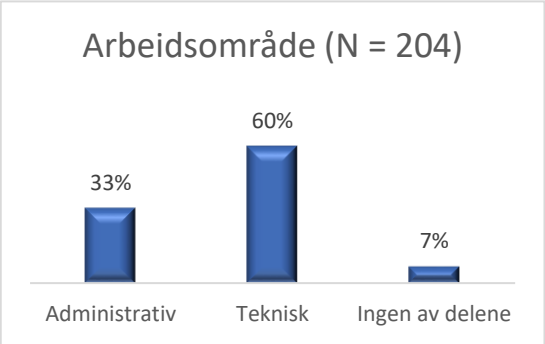
Figur 4-3: År ansatt i selskapet.



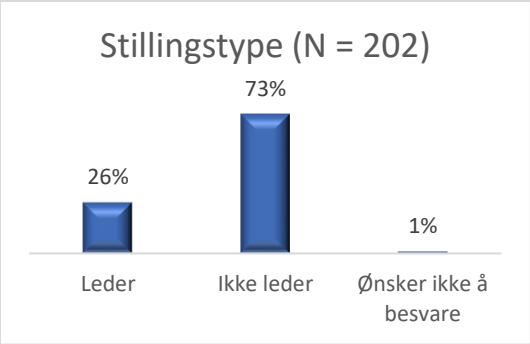
Figur 4-4: Lokasjonstilhørighet.

Arbeidsområde og stillingstype

Figur 4-5 viser at flertallet av respondentene jobber med teknisk arbeid, 33% jobber administrativt og 7% oppgir at de verken jobber teknisk eller administrativt. Det utgjør 15 ansatte av 204. Det kan diskuteres om dette spørsmålet burde hatt flere kategorier å velge mellom når det kommer til arbeidsområde. Samtidig ble kategoriene *administrativt* og *teknisk* foreslått av kontaktpersonen min som har god kunnskap og oversikt over hva ansatte i selskapet jobber med. Figur 4-6 viser at flertallet av respondentene har ikke ledende roller og at 26% av respondentene er ledere.



Figur 4-5: Arbeidsområde



Figur 4-6: Stillingstype

4.5 Planlegging og utforming av spørreundersøkelsen

Intervjuene med ekspertene ble gjennomført før spørreundersøkelsen ble laget og sendt ut. Slik fikk jeg innsikt i temaet og videre kunnskap om hvilke spørsmål undersøkelsen kunne inneholde (Ringdal, 2013). Grunnet oppgavens tidsbegrensning var det mest hensiktsmessig å velge et selvutfyllingsskjema hvor respondentene kan lese spørsmål og svaralternativer samtidig (Ringdal, 2013: 198). På denne måten kunne jeg nå ut til alle ansatte i Wintershall Dea samtidig. Det ble laget en norsk og en engelsk versjon av undersøkelsen ettersom det er et flerspråklig selskap. I oversettelsesarbeidet fra den norske til den engelske versjonen var det viktig å få ord og setninger til å samsvare med den norske, samtidig som det måtte gi mening på engelsk. Hvert spørsmål ble systematisk oversatt etter tur ved hjelp av elektronisk oversettelsesverktøy. Likevel var min egen engelskkunnskap dominerende i dette arbeidet. For å sikre at undersøkelsene samsvarte ble versjonene korrekturlest av en bekjent som mestrer det engelske språket enda bedre enn meg. I tillegg ble begge versjonene lest og godkjent av veileder før utsendelse.

4.5.1 Nettskjema

Spørreundersøkelsen ble laget ved bruk av Universitetet i Oslo sitt *Nettskjema*, som er "et verktøy for utforming og gjennomføring av spørreundersøkelser på nett" (UiO, 2020). Universitetets senter for informasjonsteknologi har utviklet og drifter nettskjema, og systemet har kapasitet til store undersøkelser med mange samtidige leveringer. Nettskjema fokuserer blant annet på brukervennlighet samt sikkerhet og personvern, og er spesielt tilrettelagt for å tilfredsstille norske krav om personvern (UiO, 2020). Informasjonen som hentes inn blir lagret i en database og resultatene kan hentes ut i for eksempel Excel. Nettskjemaet er enkelt å sette seg inn i og utforme. En av de største fordelene er at nettskjemaet kan besvares anonymt. På

denne måten kan deltakernes personvern sikres. Samtidig kan det øke både svarprosenten og kvaliteten på svarene som blir gitt da respondentene kan være helt ærlige uten å gjenkjennes i datamaterialet. Av grunnene nevnt over falt valget på å benytte denne nettbaserte løsningen for spørreundersøkelsen.

4.5.2 Spørreskjemaets oppbygging

Spørreundersøkelsen inneholdt 49 spørsmål, og var delt inn i åtte temaer for å gjøre den mer oversiktlig (Vedlegg D og Vedlegg E). Skjemaet inneholdt instruksjoner mellom temaene og en overskrift med tema for påstandene. Dette var også for å gjøre undersøkelsen oversiktlig samt for å informere deltakeren hva spørsmålene ville handle om. Undersøkelsen var frivillig å delta på, og det er derfor tilfeldig hvem som har deltatt. De ansatte har selv valgt om de vil delta, det betyr selvutvelgelse (Jacobsen, 2015).

Undersøkelsen startet med en introduksjon om cybersikkerhet for å vekke deltakernes interesse for temaet samt for å motivere til deltakelse (Ringdal, 2013). Dette var også et forsøk på å unngå frafall. Videre fulgte informasjon om prosjektets formål, hvorfor deltakerne fikk spørsmål om å delta, hva det innebar å delta, at det var frivillig å delta, informasjon om deltakernes personvern samt kontaktopplysninger til student, veileder og NSD for mer informasjon eller spørsmål knyttet til oppgaven.

Etter informasjonsdelen startet undersøkelsen med demografiske spørsmål fordi slike spørsmål er relativt enkle å besvare (Haraldsen, 1999). Deretter fulgte en rekke spørsmål under de resterende kategoriene. De første kategoriene inneholdt enkle spørsmål å svare på. Videre ble spørsmålene mer avanserte. Samtidig forsøkte jeg å lage enkle spørsmål å svare på i hele undersøkelsen. På den avsluttende siden i spørreundersøkelsen fikk deltakerne mulighet til å svare i en tekstboks dersom de hadde kommentarer eller innspill vedrørende cybersikkerhet. Deretter kom jeg med en påminnelse om å klikke på *send* for å fullføre undersøkelsen før jeg avsluttet med å takke for deltakelsen.

4.5.3 Utforming av spørsmål og svaralternativer

Spørsmålene ble stilt som påstander, som er vanlig å benytte når ønsket er å måle holdninger, som er tilfellet i denne avhandlingen (Jacobsen, 2015). Spørsmål formulert som påstander er ladet. Det vil si at påstandene tar utgangspunkt i noe bra eller dårlig (Jacobsen, 2015). I

avhandlingens undersøkelse ble det benyttet flest positive påstander for å motivere til deltakelse. For eksempel ble følgende påstand stilt: *Jeg vet hva cybersikkerhet er*, i stedet for *Jeg vet ikke hva cybersikkerhet er*.

Spørsmålsformuleringene ble tilpasset målgruppen etter beste evne (Ringdal, 2013). Da det i intervjuene med ekspertene kom frem at selskapet jobber mye med cybersikkerhet og forebygging gjorde dette at jeg kunne være sikrere på at deltakerne ville forstå spørsmålene de ble stilt. Samtidig ble det i minst mulig grad benyttet vanskelige ord og uttrykk. Der det ble anvendt ord som kunne være ukjente for deltakerne la jeg ved en forklaring. For eksempel ble deltakerne spurt om *champion-program* som er et tiltak som kan iverksettes i arbeidet med cybersikkerhet. Her la jeg ved en forklaring av hva som menes med dette før påstanden ble stilt. Spørsmålene ble samtidig forsøkt formulert på en enkel måte ved bruk av korte setninger og enkelt språk (Jacobsen, 2015). Spørsmålene var standardisert som betyr at alle deltakere fikk like spørsmål stilt på samme måte (Ringdal, 2013: 190). Det er vanlig at de fleste spørsmålene i en spørreundersøkelse er lukkede. Med det menes at spørsmålene har faste svaralternativer. Når det er snakk om åpne spørsmål betyr det at respondentene kan formulere svarene fritt (Ringdal, 2013: 200). Avhandlingens spørreskjema inneholdt 46 lukkede spørsmål og tre åpne. Åpne spørsmål ble anvendt for å gi respondentene mulighet til å uttrykke seg i sine egne ord samt for å gi deltakerne et pusterom. Likevel er det kun stilt tre åpne spørsmål på grunn av oppgavens tidsbegrensning, da informasjonen som kommer inn fra disse kan være vanskelig å behandle i ettertid hvis respondentene gir svært ulike svar (Jacobsen, 2015).

Det er vanlig at spørsmål som er formulert som påstander inneholder flere spørsmål der svaralternativene er de samme. Slike svaralternativer kalles ofte for en *Likert-skala* (Jacobsen, 2015). I oppgavens spørreundersøkelse ble de fleste påstandene satt opp i «spørsmålsbatterier» med tanke på plasseffektivitet samt for å slippe å gjenta svaralternativene for hvert spørsmål. Her ble det benyttet Likert-skala med følgende svaralternativer: *Helt uenig, Delvis uenig, Delvis enig, Helt enig, Ønsker ikke å besvare.* Det ble brukt fem punkter på likert-skalaen da «forskning antyder at det å anvende mellom fem og ni alternativer gir de mest stabile svarene, og som respondentene selv synes er enklest å forstå (Preston & Coleman, 2000 i Jacobsen, 2015: 273). Av de 46 lukkede spørsmålene inneholdt 36 av dem denne likert-skalaen. Fire spørsmål inneholdt svaralternativene *Ja, nei, ønsker ikke å besvare*. Resterende spørsmål var under kategorien *Bakgrunnsinformasjon* og hadde derfor svaralternativer som samsvarte med det aktuelle spørsmålet. Hvert enkelt svaralternativ i likert-skalaen ble gitt en tallmessig verdi

for å kunne behandles statistisk (Jacobsen, 2015). *Helt uenig* ble kodet til 1, *Delvis uenig* ble kodet til 2, *Delvis enig* ble kodet til 3, Helt enig ble kodet til 4 og *Ønsker ikke å besvare* ble kodet til 5.

4.6 Gjennomføring av spørreundersøkelsen

Når det kommer til utsendelse av undersøkelsen var det viktig at personvernet til deltakerne ble bevart. Selvutfyllingsskjemaet gir best muligheter til å beskytte svarsituasjonen fordi skjemaet kan fylles ut når ingen andre er til stede og deltakerne kan garanteres absolutt anonymitet (Ringdal, 2013: 198). For at jeg ikke skulle få innsikt i respondentenes email adresser ble undersøkelsen sendt ut av min kontaktperson fra selskapet. Dahle sendte linkene til begge versjonene av nettskjemaet videre på mail til alle ansatte i selskapet med en kort introduksjon. Dette var også den beste løsningen i og med at ansatte i selskapet, i tråd med arbeidet med cybersikkerhet, ikke skal trykke på linker fra fremmede, og/eller som de ikke har fått beskjed om eller venter på.

4.6.1 Informasjon om studien

Det var viktig at deltakerne fikk tilstrekkelig informasjon om undersøkelsen. Før Dahle sendte ut undersøkelsen, sendte jeg ham lenkene til begge versjonene med en introduksjon til spørreskjemaet. I introduksjonen fokuserte jeg på undersøkelsens formål og at undersøkelsen var frivillig samt anonym. Det ble også informert om at prosjektet var et samarbeid mellom selskapet og meg, og at Instituttet for kriminologi og rettssosiologi ved Universitetet i Oslo var ansvarlig for prosjektet. Dahle oversatte så denne informasjonen til engelsk i tillegg til å presisere at det ikke var en phishing test og at det var trygt å delta.

4.6.2 Påminnelse

Det ble sendt en påminnelse to uker etter utsendelse. Denne ble sendt av Dahle da jeg som tidligere nevnt ikke skulle ha tilgang til mailadresser. En ulempe ved å sende ut purring er at den må sendes til alle deltakerne da det ikke er mulig å vite hvem som har svart (Ringdal, 2013: 198). Det kan oppleves som «masete» eller «irriterende» å få slike påminnelser, særlig hvis man allerede har svart på undersøkelsen. Derfor ble det ikke sendt ut mer enn en påminnelse. Likevel skal det nevnes at påminnelsen som ble sendt ut hadde stor påvirkning ved at jeg fikk flere svar. Første gang undersøkelsen ble sendt ut fikk jeg raskt over 100 svar. Så ble det stille en periode, og jeg lå på ca. 130 svar. Etter første påminnelse var jeg oppe i 196 svar allerede etter to dager.

Da undersøkelsen var ferdig satt jeg igjen med 204 svar. Det viser at den ene påminnelsen som ble sendt har hatt stor betydning for svarprosenten. Dersom Dahle hadde sendt ut flere påminnelser er sjansen stor for at jeg hadde fått enda flere svar. Det ble diskutert med selskapet om det skulle sendes ut en påminnelse til, men ettersom de da var i en travel periode rett før jul med mye massekommunikasjon til de ansatte måtte andre temaer prioriteres enn en purring til.

4.7 Analytisk fremgangsmåte

Den analytiske fremgangsmåten vil belyse forholdet mellom avhandlingens problemstilling, teori og empiri. Denne oppgaven søker å skape forståelse rundt fenomenet cyberkriminalitet og hvordan det kan forebygges gjennom cybersikkerhet. For å gjøre dette har jeg i hovedsak benyttet meg av en induktiv forskningsprosess som «betyr at forskeren, med utgangspunkt i empirien som er hentet inn, velger og utvikler teori» (Album, 1966 i Skilbrei, 2019: 53). Data fra intervjuene og spørreundersøkelsen har lagt føringer for hvilke teorier og litteratur som er brukt. For eksempel er teoriene om governmentality og ansvarliggjøring hentet inn for å belyse eller utfordre funn og temaer fra intervjuene og spørreundersøkelsen. Samtidig bærer forskningsstrategien til oppgaven også preg av en deduktiv metode som betyr «at man tar utgangspunkt i allerede eksisterende forskning» (Skilbrei, 2019: 51). Oppgaven er teoridrevet i den grad at allerede eksisterende forskning, som for eksempel litteratur om forebygging av cyberkriminalitet, har lagt føringer for hvilke spørsmål som er stilt i både intervjuguiden og spørreundersøkelsen. Samtidig har kunnskap og teori lagt føringer for hvordan jeg har sett på empirien samt strukturert den. Det kan dermed argumenteres for at oppgaven bærer preg av en abduktiv forskningsstrategi fordi den er både empiri- og teoridrevet. Det betyr at «tilnærmingen startet med empiri, men at jeg aksepterer betydningen av teorier og perspektiver i forkant og/eller i løpet av forskningsprosessen» (Tjora, 2017: 255).

4.7.1 Analyse av kvalitativt intervju

Da alle intervjuene var ferdig systematiserte jeg materialet for å gjøre det klart til tolkning og analyse. I de to følgende avsnittene vil jeg forklare hvordan dette ble gjort. Deretter vil jeg presentere hvordan det kvalitative materialet er tolket og analysert.

Etterarbeid av del en av intervjuene: lydopptak

Jeg startet å transkribere del en av intervjuene etter at alle var gjennomført, og brukte dataprogrammet F4. Ved hjelp av tekstbehandlingsprogrammet gikk denne prosessen raskere. Det er en fordel å transkribere fortløpende ettersom forskeren da kan lære av feil og slik forbedre de neste intervjuene (Skilbrei, 2019: 173). Begrunnelsen for at jeg ikke transkriberte underveis var at jeg heller valgte å bruke tid på del to: de håndskrevne notatene av intervjuene. Hvorfor og hvordan dette skjedde forklares nærmere i avsnittet med etterarbeid av del to av intervjuene. Transkriberingsprosessen var verdifull for å bli bedre kjent med datamaterialet fra intervjuene. For å sikre kvaliteten hørte jeg gjennom hvert intervju da de var ferdig transkribert. Slik fikk jeg også sjekket at teksten stemte med talen på lydopptakeren og rettet opp i eventuelle feil.

Når forskeren transkriberer må det tas stilling til om alt som blir sagt skal skrives ut, eller om muntlige preg skal fjernes (Skilbrei, 2019: 173). Ifølge Marshall og Rossmann (1995, i Tjora, 2017: 174-175) er det slik at «Vi snakker ikke i avsnitt, og vi signaliserer heller ikke tegnsetting mens vi snakker». Jeg valgte derfor å fjerne muntlige preg som for eksempel «ehm», og «eeh» da jeg ikke anså disse lydene som betydelige for å forstå innholdet i den sammenhengen det ble sagt. I tillegg ble pauser markert med tre prikker, og uklarheter ble markert med klamme på følgende måte: (uklart). Følgende markering: [...] ble satt inn der hvor jeg trengte å legge inn egne notater for å forklare hva som menes. Dersom informanten sa noe som kunne gjøre transkripsjonen identifiserende ble det markert med bokstaven X. Jeg valgte å transkribere fra dialekter til bokmål av hensyn til personvern, og for enkelthetens skyld (Tjora, 2017: 174).

Etterarbeid av del to av intervjuene: håndskrevne notater

Forskeren må kunne bruke det som blir sagt i intervjuer for at de skal ha verdi (Skilbrei, 2019). Ettersom jeg kun brukte lydopptaker i første del av intervjuet ble andre del notert for hånd. Siden jeg hadde en detaljert intervjuguide å følge var det ikke nødvendig å notere planlagte spørsmål, og det lot seg gjøre å notere svarene på disse spørsmålene for hånd underveis. En av fordelene ved å ikke bruke lydopptaker er at utskrivningen av intervjuene kan skje raskt samt at irrelevant informasjon kan fjernes med en gang (Ringdal, 2013: 244). Det er likevel vanskelig å få med alt som blir sagt av begge parter i en slik situasjon (Skilbrei, 2019). Forskeren kan for eksempel bli for opptatt av å skrive ned svarene til informanten, og relevant informasjon kan utebli (Ringdal, 2013: 233). Naturlig nok har ikke transkriberingen fra mine håndskrevne

intervjuer blitt like nøyaktige som del en av intervjuene. Det ble blant annet vanskelig for meg å notere ned oppfølgingsspørsmål jeg kom på underveis. Da jeg så over notatene mine fra det første intervjuet, ble det tydelig at jeg måtte finne en bedre måte å notere på for å kunne tyde materialet i ettertid. Jeg fant ut at den beste løsningen for de neste intervjuene var å notere i stikkordsform, og renskrive notatene fra intervjuene inn i Word så fort de var ferdig, da detaljer ved det som ble sagt var friskt i minne (Skilbrei, 2019). At del to ble notert for hånd har videre hatt betydning for hvordan dette materialet er brukt i analysen. For det første brukes det som tidligere nevnt ingen direkte sitater fra denne delen. For det andre er det viktig å påpeke at denne delen er basert på mine egne tolkninger av det som er fortalt av informantene. Jeg opplever likevel at dette datamaterialet presenterer informantenes forståelser og tanker rundt cybersikkerhet og at strategien om å renskrive notatene rett etter intervjuene bidro til dette.

Koding og kategorisering

For å analysere empirien fra intervjuene har jeg tatt inspirasjon fra Skilbrei (2019: 192) sine tre forslag til strategier som kan løse den praktiske oppgaven: tekstreduksjon, koding av materialet og utvikling av typologier og kategorier.

Jeg startet med tekstreduksjon ved å skrive sammendrag fra hvert av intervjuene i Word på en måte som gjorde dem sammenlignbare. Slik ble materialet mer håndterbart samtidig som det ble lettere å studere det viktigste i materialet i lys av formålet med studien (Skilbrei, 2019: 183). Ettersom det kvalitative datamaterialet består av to deler som anvendes ulikt i analysen var det viktig å skille mellom de direkte sitatene fra informantene og mine egne tolkninger fra del to når jeg skrev sammendrag. Som nevnt over brukte jeg transkriberingsprogram til del en som innebærer at hvert avsnitt som transkriberes avsluttes med en visning av tidspunktet for det som blir sagt. Disse tidspunktene ble tatt med i sammendraget. Del to ble skrevet inn med annen skrifttype samt med en linjeavstand på 1,5. Slik ble det enkelt å holde oversikt over hva som hørte til hvilken del av intervjuene. Selv om et analyseprogram kunne strukturert dataen og systematisert funnene på en god måte, anså jeg det ikke nødvendig å bruke et slikt program da den kvalitative dataen ikke var et så stort materiale.

Deretter fulgte jeg neste strategi om å kode materialet for å systematisere det samt for å se etter mønstre og sammenhenger på tvers av intervjuene. Intervjuene ble først kodet på papir før de ble lagt inn i en enkel tabell i Word. Jeg valgte å starte med å kode temaene som ble tatt opp i

intervjuguiden da dette reflekterte innholdet i intervjuguiden (Skilbrei, 2019). Både del en og del to av intervjuene ble inkludert i kodingen. Jeg anvendte i første omgang en deduktiv tilnærming i analysearbeidet siden temaene i intervjuguiden ble valgt etter å ha lest litteratur om fenomenet som undersøkes. Jeg startet dermed med følgende temaer: forebygging, svindel, sikkerhet og koronapandemien. Etter et par gjennomlesinger forandret jeg navn på noen av temaene og la til underkoder under hvert tema. For eksempel ble sikkerhet til sikkerhetskultur og forebygging fikk følgende underkoder: tekniske barrierer, menneskelige barrierer samt opplæring i cybersikkerhet. I tillegg la jeg til koden risiko. Disse temaene gikk igjen i empirien og slik anvendte jeg også en induktiv tilnærming i analysearbeidet.

Videre ble alle intervjuene limt inn i en PDF fil som gjorde det lett å søke etter tema og kodeord. Deretter markerte jeg tekst med ulike farger basert på ulike temaer: rød signaliserte risiko og trusler (som for eksempel svindel), blå signaliserte forebygging samt opplæring, grønn signaliserte kultur og gul signaliserte koronapandemien. Etter ytterligere gjennomlesinger endte jeg opp med følgende hovedtemaer: risiko, sikkerhetskultur, forebygging og koronapandemien, som alle igjen hadde flere underkoder. Utviklingen av kodelisten for analysen har dermed, i tråd med en abduktiv strategi, vært en vekselvirkning mellom teoretiske perspektiver og empirinære tanker. For eksempel ble underkodene tekniske- og menneskelige barrierer utviklet fra empirien mens hovedkoden sikkerhetskultur kom til etter å ha deltatt på ISF sitt virtuelle høstmøte og litteraturlesing.

Neste steg i analyseprosessen var å utvikle kategorier og typologier. For å gjøre dette identifiserte jeg likheter og forskjeller på tvers av materialet (Skilbrei, 2019: 187). For eksempel snakket alle informantene om at cyberkriminalitet var en stor trussel for selskapet. En annen likhet jeg fant var at samtlige av ekspertene trakk frem sikkerhetskultur og opplæring som viktige faktorer for cybersikkerhet. Materialet ble i tillegg knyttet til ulike teorier. For eksempel knyttet jeg teoriene governmentality og ansvarliggjøring til hvordan selskapets arbeid med cybersikkerhet kan forstås.

4.7.2 Analyse av spørreundersøkelse

Deskriptiv statistikk

Resultatene fra spørreundersøkelsen er analysert ved hjelp av deskriptiv statistikk som ofte brukes til å identifisere, beskrive og karakterisere mønstre i datamaterialet (Grønmo, 2016:

434). Som tidligere nevnt vil det kvantitative materialet fungerer som et supplement til det kvalitative, og det er derfor ikke gjennomført en avansert statistisk analyse av det kvantitative datamaterialet. Siktepunktet for den kvantitative analysen er å etablere en representativ oversikt over hvordan respondentene i spørreundersøkelsen forholder seg til cybersikkerhet i Wintershall Dea.

For å tolke og fremstille resultatene statistisk ble dataen fra spørreundersøkelsen først eksportert i Excel-filer. Resultatene fra den engelske versjonen ble så limt inn i Excel med resultatene fra den norske versjonen. Deretter ble det laget pivot tabeller for hvert spørsmål med unntak av de åpne spørsmålene. Pivot-tabellene ble satt opp for å undersøke hvor mange som hadde svart på de ulike påstandene og hvilke svaralternativer som ble valgt. Deretter ble antall svar beregnet i prosent. Videre ble det laget et søylediagram til hver av disse pivot-tabellene for å presentere resultatene på en mer visuell måte. Grafene er konstruert og satt sammen på den måten jeg har ansett som mest hensiktsmessig med sikte på å kommentere og framheve generelle tendenser, mønstre og sammenhenger som har størst relevans for oppgavens problemstilling (Grønmo, 2016: 360). Jeg valgte å bruke prosent i grafene da dette ga best visuelt inntrykk av svaralternativene. Noen påstander presenteres alene. De påstandene som henger sammen eller er naturlig å se på samlet har jeg kombinert i samme graf for å tydeligere vise likheter og forskjeller. Søylediagrammene viser de ulike påstandene i forenklet tekst. Videre er antall respondenter som har svart på påstanden presentert med N=, samt antall prosent som har svart på de ulike svaralternativene. Jeg har stort sett valgt å ikke vise svaralternativer med særlig lav svarprosent i grafene, da dette ikke ga noe betydning for videre diskusjon. Som tidligere nevnt inneholdt undersøkelsen 49 spørsmål. 46 av disse er anvendt i analysen. De resterende tre ble ikke ansett som hensiktsmessige for analysen.

4.8 Datakvalitet

Det er vanlig å benytte begrepene reliabilitet (pålitelighet), validitet (gyldighet) og generaliserbarhet som indikatorer på forskningens kvalitet i forskningsprosjekt (Tjora, 2012: 202). For å sikre reliabilitet har jeg gjort rede for fremgangsmåtene jeg har ansett som mest hensiktsmessige for å undersøke fenomenet som er studert, deriblant metodiske avgjørelser, forskningsstrategier og analysemetoder. Dette har samtidig vært et forsøk på å opprettholde transparens som også anses som et middel til pålitelighet (Tjora, 2012: 202). Reliabilitet handler i tillegg om forskerens forforståelse og diskuteres under etiske refleksjoner.

Validitet knyttes til gyldigheten av de resultatene forskeren kommer frem til, og hvordan disse tolkes (Thaagard, 2018: 19). Innenfor kvalitativ forskning er det utfordrende å kvantifisere validitet, og jeg vil med dette som utgangspunkt ikke fastslå studiens validitet. Jeg oppfatter likevel at validiteten er hevet ettersom jeg har benyttet meg av metodetriangulering. Med hevet validering mener jeg ikke at spørreundersøkelsen er brukt for å sjekke at det ekspertene har sagt er sant, men i stedet at spørreundersøkelsen har gjort dataene mine tykkere og slik bidratt til en kvalitativt bedre analyse (Skilbrei, 2019). For å øke oppgavens gyldighet gjennomførte jeg også intervjuene med ekspertene før spørreundersøkelsen ble sendt ut for å være sikrere på at spørsmålene som ble stilt var relevante for å undersøke oppgavens fenomen (Jacobsen, 2015: 139).

Når det kommer til generaliserbarhet, som er knyttet til forskningens relevans utover de enheter som faktisk er undersøkt (Tjora, 2012), er det vanskelig å generalisere min studie til en populasjon. Dette skyldes at jeg har undersøkt hvordan cybersikkerhet jobbes med og forstås innenfor et spesifikt selskap, og slik knyttes mine resultater til dette selskapet. Det vil for eksempel være vanskelig å si at cybersikkerhet forstås og kan forebygges på samme måte som Wintershall Dea gjør for mennesker som ikke er en del av arbeidslivet. Dette fordi mennesker utenfor arbeidslivet har andre forutsetninger og sannsynligvis ikke har samme opplæring og oppfølging i cybersikkerhet. Det kan derimot tenkes at tilnærmingen kan skape en konseptuell generalisering heller enn en generell generalisering. Konseptuell generalisering handler om å utforske konsepter, typologier eller teorier som vil ha relevans for andre tilfeller enn dem som er studert (Tjora, 2012: 209). Det er mulig at oppgavens funn kan overføres til andre gass- og oljeselskaper som har omtrent lik størrelse som det Wintershall Dea har. Med tanke på at cyberkriminalitet og cyberangrep er en stor utfordring og trussel innen denne sektoren, er det sannsynlig at andre selskaper på samme størrelse også har egne IT-avdelinger med egne «eksperter» som jobber med cybersikkerhet. Det er derfor mulig at de funn og utfordringer som er kartlagt i denne oppgaven også kan være gyldig i slike andre selskaper og at resultatene slik kan være overførbare.

4.9 Etiske refleksjoner

Å drive empirisk forskning reiser mange forskningsetiske spørsmål. Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora (NESH, 2016: 5) definerer i sine retningslinjer forskningsetikk som: *«et mangfold av verdier, normer og institusjonelle*

ordninger som bidrar til å konstituere og regulere vitenskapelig virksomhet». Forskningsetikk handler om refleksjoner om egen forskerpraksis og skal sørge for at forskningen gjennomføres «på en måte som ikke krenker sentrale samfunnsverdier, og sikrer tillit til forskning» (Skilbrei, 2019: 25). Fra start til slutt av dette prosjektet har jeg derfor tatt stilling til ulike etiske utfordringer ved gjennomføringen av studien.

4.9.1 Anonymitet og personvern

Både ekspertene og respondentene ble forsikret om at den innsamlede informasjonen ville behandles konfidensielt og i samsvar med personvernregelverket. For å bevare anonymiteten til informantene som ble intervjuet er de referert til som eksperter og informanter både i det transkriberte materialet og i analysen. I tillegg er kjønn anonymisert. Som tidligere nevnt jobber noen av ekspertene direkte med cybersikkerhet mens andre jobber mer perifert med det. Jeg har ikke valgt å skille mellom disse to gruppene i analysematerialet for å bevare ekspertenes anonymitet. Dette skyldes at informantene ble rekruttert gjennom et mellomledd som kanskje kunne klart å gjenkjenne hvem som har sagt hva hvis jeg hadde skilt mellom gruppene. Jeg anså heller ikke dette som nødvendig for forståelsen av materialet. For å gjøre det lettere å skille mellom ekspertene i datamaterialet og analysen ble alle tildelt en bokstav, eksempelvis «Informant A» eller «Ekspert A». Disse ble gitt tilfeldig og ikke i den rekkefølgen intervjuene fant sted. I det første møte jeg hadde med Wintershall Dea ble det avklart at det ikke var nødvendig å anonymisere selskapet jeg har samarbeidet med og heller ikke min kontaktperson, Ole Martin Dahle. Når det kommer til deltakerne i spørreundersøkelsen er alle respondentene anonymisert da skjemaet ble besvart anonymt.

4.9.2 Informasjonsskriv og samtykkeskjema

I forkant av intervjuene fikk ekspertene tilsendt et informasjonsskriv og samtykkeskjema (vedlegg A) over e-post for at de skulle få tilstrekkelig informasjon om studien og deres rettigheter. Ettersom alle ekspertene ble rekruttert via et mellomledd, som i tillegg besitter en overordnet stilling i selskapet, kan det diskuteres om dette har lagt noen form for begrensning for informantenes handlingsfrihet. Jeg anså det derfor som ekstra viktig å presisere at det var frivillig å delta og mulig å trekke seg når som helst. Før intervjuene startet og opptakeren ble skrudd på gikk jeg igjen igjennom skjemaene for å sikre at deltakernes rettigheter var forstått samt at jeg fikk en ny godkjenning på bruk av lydopptaker. I intervjuet som foregikk på Wintershall Dea sitt kontor ble informasjonsskrivet og samtykkeskjemaet medbrakt og gått

igjennom før start. Samtykkeskjemaet ble også signert av informantene før intervjuet fant sted og sendt til meg i forkant, slik at jeg visste at denne informasjonen ble gått igjennom mer enn en gang. Ingen av informantene benyttet seg av rettigheten til å trekke seg, og det var heller ingen som ga uttrykk for at de hadde opplevd et press for å delta verken før intervjuet eller i etterkant. I tillegg ga flere informanter uttrykk for at samtalen var fruktbar også for dem, da det fikk dem til å tenke over hvor viktig det de jobber med er. Samtidig ga samtlige av informantene meg beskjed om å ta kontakt i ettertid hvis det skulle dukke opp noen spørsmål. På bakgrunn av de ovennevnte faktorene opplever jeg som forsker at informantene ikke har følt press på å delta.

Når det kommer til spørreundersøkelsen (vedlegg D) mottok ansatte i første omgang en e-post fra Dahle om at han, i forbindelse med et masterprosjekt, snart ville sende ut en undersøkelse som handlet om cybersikkerhet og at det var trygt å delta på denne. I starten av spørreundersøkelsen ble deltakerne informert om prosjektets formål, at det var frivillig å delta samt om personvern og oppbevaring av data. Jeg kontaktet NSD for å høre om det var nødvendig med samtykkeerklæring for spørreundersøkelsen, noe det viste seg å ikke være. Jeg forsikret både ekspertene og respondentene i spørreundersøkelsen om at den innsamlede dataen ville behandles fortrolig, noe som er et viktig krav innenfor forskning (Thaagard, 2018). Samtykkeerklæringene og lydopptakene er oppbevart på sikker server etter Universitet i Oslo sin standard. Samtykkeerklæringene er oppbevart i sikkert skap på UiO med kodelås. Lydopptakene er lagret sikkert og kryptert i Nettskjema.

4.9.3 Forforståelse

Forskere tolker materialet sitt i lys av hvem de er og hva de kan (Skilbrei, 2019) og innenfor all type samfunnsforskning vil forskeren ha en form for engasjement i temaet som forskes på (Tjora, 2012: 203). Dette kan fremstå som støy i prosjektet da engasjementet kan påvirke resultatene (Tjora, 2012: 203) og kan samtidige påvirke prosjektets reliabilitet. Min forforståelse knytter seg for eksempel til studiet kriminologi og fører til et kriminologisk blikk på forskningen. Likevel er cyberkriminalitet og cybersikkerhet et relativt nytt fenomen og forskningsområde innenfor kriminologien, selv om det har fått et større fokus i dag i takt med digitalisering og teknologisk utvikling. Det er derimot ikke et tema som har vært sentralt i kriminologistudiet. Dermed kan det tenkes at min forforståelse ikke har lagt så store føringer for resultatene. Det skal likevel nevnes at jeg i forkant av intervjuene hadde visse forventninger om hva ekspertene ville fortelle meg. Dette skyldtes at jeg hadde lest en del litteratur og

rapporter om cyberkriminalitet og cybersikkerhet i virksomheter, og det er dermed sannsynlig å anta at dette kan ha formet min oppfattelse av informasjonen fra informantene. Jeg har likevel etter beste evne forsøkt å se dataene så objektivt som mulig.

4.9.4 Avtale med selskapet

Som tidligere nevnt ble det inngått en veiledningsavtale mellom Wintershall Dea og meg (Vedlegg F). Avtalen innebærer blant annet at selskapet har fått innsyn i oppgaven før innlevering for å sjekke at dokumentet ikke inneholder konfidensiell informasjon som ikke kan publiseres. Med tanke på temaet for oppgaven anså jeg denne avtalen som svært rimelig, spesielt ettersom ekspertene besitter sensitiv informasjon om hvordan selskapet jobber for å beskytte seg mot cyberangrep. Jeg er klar over at dersom jeg hadde skrevet og publisert sensitiv informasjon kunne dette fått konsekvenser for selskapets cybersikkerhet. Jeg har heller ikke opplevd det som problematisk at selskapet har fått innsyn i oppgaven før innlevering.

5 Analyse og diskusjon

I analysen vil funn fra intervjuene med ekspertene og spørreundersøkelsen med de ansatte gjennomgås. Analysen er delt i to kapitler. Første del ser på hvilket trusselbilde Wintershall Dea må forholde seg til samt hvordan ekspertene og ansatte forstår risiko og trusler i forhold til cyberkriminalitet. Del to går dypere inn på hvordan ekspertene jobber med å forebygge cyberkriminalitet og ansattes opplevelse av dette arbeidet. Underveis i begge kapitlene vil ekspertenes mentaliteter og logikker for forebygging diskuteres opp mot det teoretiske rammeverket for avhandlingen.

5.1 Del en: Risiko og trusler

5.1.1 Trusselbildet i Wintershall Dea

Wintershall Dea har til nå ikke vært utsatt for noen vellykkede dataangrep av typen vi har sett andre selskap har vært offer for, som for eksempel Hydro og Mærsk. Ekspertene er likevel klar over at lignende angrep kan skje i deres virksomhet og at de har vært utsatt for svindelforsøk som kunne fått større konsekvenser enn det fikk. I tillegg er ekspertene klar over at selskapet kan ha vært utsatt for angrep som ikke er oppdaget. For eksempel sier informant D at:

> *«Vi har ikke hatt mange reelle hendelser som har gått dypt inn i infrastrukturen. Og da sitter du gjerne med det spørsmålet, okei, er det fordi vi ikke klarer å se det? Og det kan det være. For gjennomsnittlig tid et selskap bruker på å finne ut om det er tatt [utsatt for angrep] er nesten et år, godt over 2-300 dager».*

Næringslivets sikkerhetsråd mener også at det er stor sannsynlighet for at det foregår et betydelig antall uoppdagede angrep mot norske virksomheter (NSR, 2020: 47). Mørketallsundersøkelsen deres fra 2018 til 2020 viser at antallet virksomheter som rapporterer om hendelser knyttet til malware (skadevare) og/eller virus har gått ned fra 21% til 11%. Dette mener NSR kan bety at det har vært færre nye virus og/eller malware, eller at beskyttelsen mot slike angrep har forbedret seg. Samtidig påpeker de at tilsvarende undersøkelser i utlandet viser at kun 9% av angrepene gir alarmer og at 68% av ransomware (løsepengevirus) forblir uoppdaget (NSR, 2020: 47). I nasjonal trusselvurdering for 2021 antas det også at mange angrep ikke er og heller aldri vil oppdages (PST, 2021: 8).

Ekspertene forteller at det aldri før har vært så stort fokus på cybersikkerhet som i dag. Informant F sier for eksempel at: *«Cybersecurity generelt, det har jo fått en enorm attention da. Heldigvis»*. Vedkommende utdyper dette i større grad senere i intervjuet: *«Fokuset på sikkerhet er større enn noen gang, og vi har pengesummene til å gjøre disse tiltakene som er nødvendige. Vi trenger noe som er sikkert nok»*. Informant B forteller at cybersikkerhet i dag blir løftet opp på styrenivå og tror det skyldes at folk har sett hvor store økonomiske konsekvenser dataangrep kan ha for selskaper. Vedkommende bruker dataangrepene på Hydro og Mærsk som eksempel og tror disse angrepene har vært springbrett for det som foregår nå. Det er ingen tvil om at IKT-kriminalitet gir store økonomiske tap for virksomheter. Selv om det som tidligere nevnt er vanskelig å få tak i nøyaktig statistikk over dette, gir Center for Strategic and International Studies (CSIS) en pekepinn på omfanget. CSIS har anslått at årlige globale tap er på mellom 375 til 575 milliarder dollar per år på verdensbasis. For Norge anslår CSIS-estimatet et tap på cirka 20 milliarder kroner (NOU 2015: 13: 57).

Informant B forteller også at hen har sett en endring i IT bransjen. Da vedkommende startet var ikke IT-sikkerhet noe som ble prioritert og det ble brukt lite penger til sikring. Ekspert G er også enig i at fokuset på cybersikkerhet har økt de siste årene og sier samtidig at: *«Og det er jo helt nødvendig, sant. Det går vel bare opp for oss mer og mer hvor uendelig mange måter denne trusselen kan dukke opp på»*. Informant C legger til følgende om dagens fokus på cybersikkerhet: *«Så, vi har aller mest å vinne i forhold til å unngå at vi får en konsekvens av et angrep»*. På spørsmål om hvorfor vedkommende tror det har blitt slik, forteller hen:

> *«Det henger nok mye sammen med på en måte omfanget av trusler og type trusler og altså, hvor teknisk avanserte angrepene er. Det har utviklet seg og utvikler seg i, ja, rasende fart. Og bransjen på sikringssiden er nødt til å henge med på samme måte som bransjen på trusselsiden også gjør det de kan for å finne nye måter å ramme oss på. Så det spillet de spiller er jo i kontinuerlig utvikling»*.

Digitale trusler og konsekvensene av disse har fått stor oppmerksomhet i dagens samfunn og det er grunn til å tro at omfanget av slike trusler og utfordringer vil øke (Mark mfl., 2019: 173). Ulike cyberhendelser har videre ført til at cybersikkerhet er blitt en av topp-prioritetene på sikkerhetspolitiske agendaer over hele verden (Balzacq og Cavelty, 2016: 176). Det er med andre ord snakk om at fenomenet er i endring, noe vi ser at ekspertene også gir uttrykk for.

Ekspert C forteller at bransjen deres i stor grad er tuftet på en risikovurdering av alt de gjør, og at de tar det med seg i måten de driver på. Videre sier vedkommende at det handler om å redusere risikoen så langt det er mulig. Informant F forteller at ønske er å ikke ha noen svekkelser og at de må finne barrierer for å sikre eventuelle svekkelser. Vedkommende sier også at de ikke tar noen risikoer og heller ingen sjanser. Samtidig forteller informant D at man alltid lever med noe risiko og noe sårbarhet. Lysneutvalget (2015: 1) skriver i sin rapport *Digitale Sårbarheter Olje & Gass* at «enhver aktivitet i olje- og gassektoren er forbundet med risiko forårsaket av trusler og sårbarheter». Videre står det i rapporten at dette i økende grad også gjelder risiko grunnet digitale sårbarheter og at petroleumssektoren er blant de mest utsatte. At petroleumssektoren er av spesiell interesse for trusselaktører støttes også av Nasjonal sikkerhetsmyndighet (NSM, 2020: 25) samt i den nasjonale trusselvurderingen til politiets sikkerhetstjeneste (PST, 2021: 8).

Ut ifra det ekspertene forteller ser det ut som det er det tidligere omtalte konstruktivistiske perspektivet på risiko som beskriver deres tilnærming til cyberkriminalitet. Dette fordi ekspertene jobber med risikoanalyser og barrierer for å sikre svekkelser og dermed arbeider fremtidsrettet for å forhindre cyberangrep. Det konstruktivistiske perspektivet er også fremtidsrettet og tar utgangspunkt i hvordan individer og kollektiv forstår, tolker og forteller om framtiden (Engen mfl., 2016). Videre handler dette perspektivet om hvordan risiko oppleves og forstås samt hvordan det konstrueres i samspill mellom individer og organisasjoner (Engen mfl., 2016). I lys av det ekspertene forteller synes også deres måte å forstå risiko å samsvare med Ericson og Haggertys (1997) definisjon som nettopp handler om ulike teknologier og kommunikasjonsregler som brukes for å håndtere farer.

At Wintershall Dea har stort fokus på risikoer knyttet til digitale angrep samt å redusere disse er forståelig med tanke på trusselen det utgjør. Samtidig er det forventet av myndighetene at virksomheter tar del i arbeidet med sikring av digitale sårbarheter. I januar 2019 lanserte regjeringen *Nasjonal strategi for digital sikkerhet* (Departementene, 2019: 6). Rapporten skriver at det finnes flere sentrale myndighetsaktører med ansvar for digital sikkerhet i Norge. Samtidig presiseres det at myndighetene ikke kan løse utfordringene i det digitale rom alene, men at det må gjøres i fellesskap. Rapporten forklarer hva som menes med dette:

> «God digital sikkerhet er imidlertid ikke en målsetting myndighetene kan nå alene. Næringslivet har kompetansen og ressursene, og er en driver for digitalisering og

> innovasjon. Næringslivet er derfor en sentral del av løsningen. For å beskytte det digitale samfunnet må privatpersoner, virksomheter, sektorer og nasjoner se utover seg selv. Alle virksomheter har et ansvar for å ivareta sin egen digitale sikkerhet...» (Departementene, 2019: 9)».

Et av delmålene i strategien er at virksomheter skal ha en risikobasert tilnærming mot uønskede digitale hendelser samt bruke anerkjente rammeverk, standarder og styringssystemer for digital sikkerhet. I lys av dette kan Norges strategi for å styre cyberkriminalitet knyttes til Foucault (1991) sitt begrep governmentality, som handler om hvordan staten styrer befolkningen. Foucault mente blant annet at staten i dag styrer på avstand ved bruk av ulike teknikker, og at denne mentaliteten hadde blitt det vanlige grunnlaget for alle moderne former for politisk tanke og handling. Neumann (2003) mener at denne styringsformen har fokus på forebygging heller enn direkte styring, og at denne typen makt stadig blir mer utbredt i Norge. I den nasjonale strategien for digital sikkerhet ser vi en tydelig politisk tankegang og mentalitet som samsvarer med Foucault sitt begrep. Staten ansvarliggjør virksomheter i kampen mot cyberangrep, legger vekt på implementering av forebyggende tiltak, og prøver slik å styre cyberkriminalitet på avstand.

I 2015 kom Lysneutvalget med rapporten *Digitale sårbarheter i Olje & Gass*. I rapporten står det blant annet at: «Det norske tilsynsregime i olje- og gassektoren er basert på prinsippet om egenregulering eller internkontroll» (Lysneutvalget, 2015: 20). Den norske modellen er blant annet basert på en ansvarliggjøring av hver enkelt bedrift, kombinert med sanksjonsmidler fra myndighetenes side. Dette begrunner Lysneutvalget (2015) med at selskapene har detaljert kunnskap om virksomhetene sine, noe sikkerhetsmyndighetene ikke har. På grunn av dette kan ikke bedre digital sikkerhet forenkles til et krav om mer myndighetskontroll. I stedet mener Lysneutvalget (2015: 21) at myndighetene må påvirke næringen gjennom for eksempel bevisthetskampanjer og informasjon om trusselsituasjonen. Når det kommer til fenomenet cybersikkerhet og digitale sårbarheter fremkommer det i begge nevnte rapporter at staten gir selskaper og virksomheter i Norge ansvaret for sin egen sikkerhet. Staten bidrar med ulike myndighetsaktører som blant annet gir ut informasjon om fenomenet, men selskapene må selv bidra i dette arbeidet. Med andre ord ser vi en mentalitet hvor staten fortsatt er aktiv samtidig som ansvaret fordeles til virksomheter og borgere i samfunnet, som nettopp er poenget med Foucaults governmentality- begrep.

5.1.2 Hvordan ekspertene holder seg oppdatert på trusselbildet

Virksomheter bør holde seg oppdatert på trusselbilde for å skape forståelse av situasjonsbilde. Dette er viktig i forhold til arbeidet med forebygging av cyberkriminalitet. Et trusselbilde forstås som «en vurdering av de farene og truslene samfunnet står overfor samt hvilke metoder og hendelser som anses sannsynlige» (NOU 2015: 13: 253). Et situasjonsbilde forstås som «et kontinuerlig oppdatert øyeblikksbilde om pågående hendelser og aktiviteter» (NOU 2015: 13: 253).

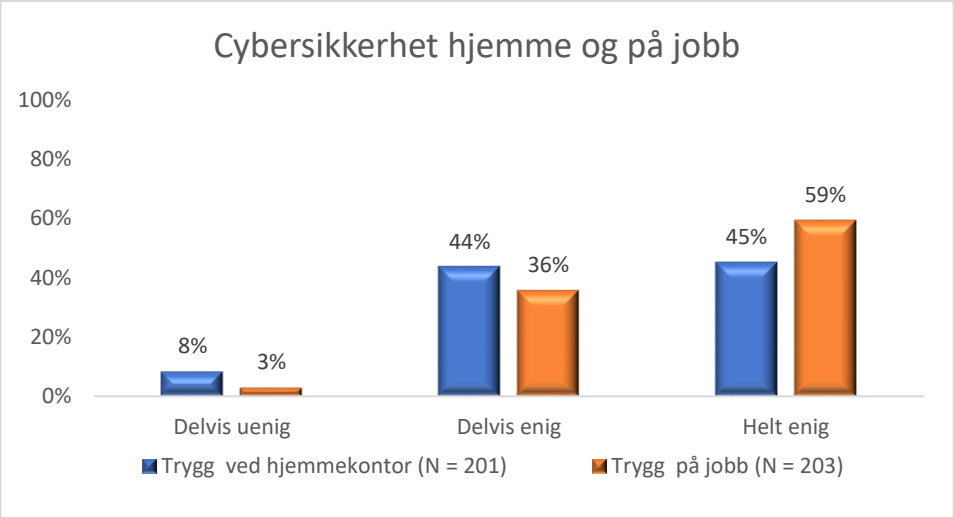
For å holde seg oppdatert på trusselbildet leser ekspertene i Wintershall Dea artikler og forskjellige sider som publiserer informasjon jevnlig. I tillegg henter de informasjon fra ulike sosiale medier som for eksempel Twitter. Ellers deltar de blant annet på seminarer, samlinger og konferanser. På grunn av korona har det meste av dette blitt avlyst det siste året, men de som jobber fast med cybersikkerhet gjør en del kursing hele tiden. Selskapet er også medlem av Nasjonal sikkerhetsmyndighet og får mye informasjon om trusselbildet derfra. Ellers er det en del andre statlige organer som gir ut mye nyttig informasjon. Flere av informantene forteller at det er viktig å alltid holde seg oppdatert når en jobber med IT og cybersikkerhet. Informant B uttrykker blant annet at: *«Jeg følger med hver dag, det blir en livsstil. Det er liksom det siste du gjør før du legger deg og det første du gjør når du står opp. Det er ikke bare en åtte til fire jobb»*. Dette synet støttes av informant D som forteller at:

> *«Når du jobber med IT må du alltid holde deg oppdatert. For det er en ferskvare. Hvis du ikke oppdaterer deg på fem år med IT så er du egentlig å regne som pensjonist vet du. Mens når det gjelder cybersikkerhet, det er jo en ting å kunne mekanismer for å beskytte seg, men for å kunne vite hvordan folk jobber og hvordan nye angrepsflater er så må en til enhver tid holde seg oppdatert og følge med. Det er nok nesten en livsstil å være oppdatert».*

Ekspertene snakker her indirekte om læring og kunnskapsutvikling – og dette synes å være en del av deres logikker og mentaliteter i arbeidet med forebygging av cyberkriminalitet. Det snakkes om at det er en «livsstil» å arbeide med cybersikkerhet, og i det at man alltid må være oppdatert og i konstant utvikling. Dette kan knyttes opp mot sikkerhetsperspektivet (Zedner, 2009) hvor både den objektive og subjektive dimensjonen understreker betydningen av «jakten på sikkerhet», hvor en konstant må være på utkikk etter (ukjente) trusler. Det synes å være et iboende fokus på dette for de som jobber med cybersikkerhet.

Det kan derimot være vanskelig for virksomheter å ha en forståelse av situasjonsbildet når trusselbildet stadig hurtigere endres (NOU 2015: 13: 262). Det siste året har Covid-19 ført til at situasjonsbildet og trusselbildet har endret seg. Ansatte har sittet mer på hjemmekontor enn de har vært på selskapets lokaler. I NSM sin risikovurdering for 2020 uttrykkes det at økt bruk av hjemmekontor fører med seg ulike digitale trusler og sårbarheter (NSM, 2020). Politiets trusselvurdering (2021: 24) viser at økt bruk av hjemmekontor har ført til at bedrifter er særlig utsatt for faktura- og direktørsvindel. Dette er en faktor ekspertene ikke har måtte ta like stort hensyn til tidligere med tanke på det forebyggende arbeidet. Det er usikkert hvilke konsekvenser dette har og kan få for cybersikkerheten til Wintershall Dea og andre organisasjoner. Når ekspertene blir spurt om selskapet har opplevd en økning i svindelforsøk på grunn av korona viruset har de delte meninger. En av informantene sier at de så en stor økning i phishing mail som omhandlet korona. Tre av ekspertene mener derimot at selskapet ikke har mottatt flere svindelforsøk som følge av viruset. Ekspertene forteller at de ikke har hatt mulighet til å drive opplæring og forebygging av cybersikkerhet på samme måte som før. Det kan dermed tenkes at ansatte ikke har hatt samme fokus på temaet den siste tiden som tidligere. I tillegg mister de daglige påminnelser som for eksempel folderne med speileffekt på forsiden som selskapet har plassert rundt i lokalene sine. På disse står det: «Du ser nå på den viktigste personen for å ivareta Wintershall Dea».

Ekspertene ble i tillegg spurt hvor de tror ansatte er mest utsatt for svindelforsøk, om det er på kontoret eller når de har hjemmekontor. Her er det også litt delte meninger. To av ekspertene forteller at selskapet har så gode systemer at de ikke er utsatt uansett hvor de sitter. En annen informant sier at de jobber fra samme arbeidsflate og må bruke VPN (virtuelt privat nettverk) for å logge inn på systemene. Samtidig tenker vedkommende at ansatte kan være litt mer utsatt når de sitter hjemme fordi det blir vanskeligere å diskutere og høre hva andre tenker om for eksempel en mail som mottas. De mister denne kommunikasjonen og ansvaret ligger derfor litt mer hos den ansatte. Informant C tror ansatte er mer utsatt når de jobber hjemmefra fordi IT-teamet har mindre kontroll på hva de gjør og hvilket wifi som brukes.



Figur 5-1: Jeg føler meg trygg med tanke på cybersikkerhet når jeg har hjemmekontor. Jeg føler meg trygg med tanke på cybersikkerhet når jeg er på jobb.

I spørreundersøkelsen ble ansatte spurt om de føler seg trygg med tanke på cybersikkerhet når de er på jobb. Figur 5-1 viser at 59% er helt enige i denne påstanden og 36% er delvis enige. På spørsmål om ansatte føler seg trygg med tanke på cybersikkerhet når de har hjemmekontor er 45% helt enige og 44% delvis enige. Resultatene tyder på at ansatte føler seg tryggere når de jobber på kontoret enn når de har hjemmekontor. Hvilken effekt økt bruk av hjemmekontor vil få for selskapets cybersikkerhet er et interessant spørsmål å jobbe med videre for selskapet.

5.1.3 Trusselaktørene og deres mål

Den norske olje- og gassvirksomheten driver med oppstrøms-aktiviteter og nedstrøms-aktiviteter (Lysneutvalget, 2015: 7). Den førstnevnte aktiviteten er det virksomhetene gjør for å bringe borestrøm opp fra grunnen og videre prosessere denne. Den andre nevnte aktiviteten er det virksomhetene gjør for å bringe olje- og gass produkter ut til forbrukere. For alle operasjoner som utføres i disse aktivitetene er virksomhetene avhengig av informasjonssystemer. Dermed er olje- og gassektoren digitalt sårbar i alle ledd i verdikjeden og slik et stort mål for ulike trusselaktører (Lysneutvalget, 2015: 7). Trusselaktører som blant annet driver med digitale angrep og IKT-kriminalitet kan ha «ulik motivasjon, ulik tilgang på ressurser og ulike grad av kunnskap og organisering» (NOU 2015: 13: 54).

Sosiale hackere og «script kiddies» anses som de minst teknisk avanserte truslene (NOU 2015: 13: 54). Ekspertene i Wintershall Dea ser også på disse aktørene som mindre farlige. På spørsmål om hvem trusselaktørene er sier ekspertene at det kan være ensomme amatørhackere, og at det er de profesjonelle hackerne de bekymrer seg for. Informant B forteller for eksempel

at *«Før var det mange små som holdt på med dette, 14-åringer liksom, som ikke visste hva de drev med. I dag er det organisert. Det er mye mer profesjonelt i dag»*. Kriminelle grupperinger i utlandet nevnes også som potensielle trusselaktører. En av ekspertene sier at enkelte land driver virksomheter med egne kundeservicer, og at de ofte opererer med en organisasjonsstruktur som legale selskaper. NorSIS (2020: 10) skriver også at mange av de kriminelle som opererer på nett stadig blir mer profesjonelle og at de nærmest driver som multinasjonale selskap. En annen informant forteller at uansett om det er små grupper som angriper, er de godt organiserte og har bygget opp selskaper hvor folk går til dette som en dagligdags jobb. Informasjonen fra ekspertene samsvarer med NorSIS sin rapport om trusler og trender, som skriver at cyberkriminaliteten profesjonaliseres og at mange av de kriminelle som opererer på nett stadig blir mer profesjonelle samt opererer som multinasjonale selskap (NorSIS, 2020: 10).

Aktivistgrupper blir også nevnt av ekspertene som en trussel for selskapet. En av informantene forteller at olje-og gass bransjen er populær i Norge for ulike trusselaktører, og sier at selskapet har fått informasjon om at de står på rød-lister hos aktivistgrupper som gjerne er inspirert av klima og annet. Dette kan for eksempel skyldes at selskapet ønsker å bore i områder som aktivistgrupper mener bør fredes. Selskapet har ikke opplevd angrep fra aktivistgrupper, men er klar over at det er en reell trussel. Politisk motiverte grupper og enkeltpersoner kalles ofte for *hacktivister* og bruker digitale verktøy for å både true og påvirke (NOU 2015: 13: 54).

Den største bekymringen for selskapet er statlige aktører og myndigheter. Politiets sikkerhetstjeneste (PST) sin trusselvurdering fra 2021 skriver også at statlig styrt spionasje er en alvorlig trussel i det digitale rom, og at norske virksomheter det neste året vil oppdage eller bli informert om at etterretningstjenester har forsøkt å få tilgang til informasjon i deres digitale nettverk (PST, 2021: 7). Flere av ekspertene mener at det ofte er penger som styrer hvem som begår dataangrep. En informant forteller blant annet at de «med stor lommebok» står bak mye. Vedkommende forteller videre at det finnes mennesker som går på jobb hver dag med mål om å svindle andre land på oppdrag fra myndighetene sine, og at disse menneskene sitter i store grupperinger, som for eksempel store IT-avdelinger, når de opererer. En annen informant er inne på det samme, og forteller at det handler om kost-nytte. Ifølge eksperten er det ofte statlige aktører som ønsker å angripe. Vedkommende forteller at russiske myndigheter plutselig kan ønske å gå etter selskapet. Informanten mener også at angrep fra statlige aktører kan bli et enda større problem i fremtiden. Dette støttes av PST (2021: 7) som skriver at Russland og Kina vil

utgjøre en stor risiko mot Norge fremover når det gjelder nettverksoperasjoner. Statlige trusselaktører har store ressurser, mye kunnskap og er samtidig godt organisert. Disse omtales ofte som *sofistikerte angripere* (NOU 2015: 13: 50). En av ekspertene forteller om en hendelse hvor en ansatt hadde med jobb-pc-en sin til et land hvor den ble hacket. Heldigvis oppdaget de det med en gang den ansatte kom hjem fordi de fikk varsel om det. Informanten presiserer at det viser hvor viktig det er å ha systemer som kan overvåke og varsle.

Ifølge NSM (2020: 15) er det viktig å forstå hva trusselaktørene er ute etter for å kunne sikre verdiene våre. Ekspertene i Wintershall Dea sier at trusselaktørene som regel er ute etter økonomisk vinning, informasjon eller spionasje. Det blir blant annet uttalt fra informant A:

> *«Formålet er å skaffe verdi og penger. Uansett hvordan de gjør det er målet å få penger. De gjør ikke dette for gøy. Informasjon kan selges for å få penger. Vi ser et vanvittig stort trykk og avanserte metoder for å skaffe penger».*

Ifølge Politiets trusselvurdering (2021: 22) begås datakriminalitet først og fremst for økonomisk vinning. Dette støttes av Nasjonal sikkerhetsmyndighet (NSM, 2020: 7) og Næringslivets sikkerhetsråd (NorSIS, 2020: 32) som i tillegg sier at aktørene også er ute etter sensitiv informasjon. Det kan for eksempel dreie seg om forretningshemmeligheter og teknologi (NSM, 2020: 7). Uttalelsene fra ekspertene og sikkerhetsorganene underbygger altså påstanden om at cyberkriminalitet blir begått med økonomiske motiver som eksempelvis Bernaards mfl. (2012) viser til. Denne oppfatningen av motiver står derimot i kontrast til den tidligere nevnte studien til Kranenbarg (2021) hvor svært få cyberkriminelle oppgir at lovbruddet ble utført for økonomisk vinning, men at det heller ble motivert av kjedsomhet, spenning eller andre indre motiver.

5.1.4 Svindel

Ifølge ekspertene blir Wintershall Dea forsøkt svindlet hver dag: *«Vi ser jo tusenvis av angrep»*, sier informant A. Informantene er også klare på at alvorlighetsgraden til angrepene varierer. For en del år siden opplevde selskapet en teknisk svindel. Angrepet varte i seks timer på selskapets telefoni. På denne tiden hadde virksomheten videosystemet sammen med telefonsystemet, og det utsatte dem for en sårbarhet. Trusselaktørene fant ut at med en viss kode gjennom et visst program kunne de hacke seg inn og ringe ut fra selskapets system. Angrepet ble oppdaget og stanset av Telenor som så at det var noe rart siden «selskapet» hadde ringt til

flere land som de ikke pleier å ringe til på rare tidspunkter. Informant A tror angrepet førte til at selskapet begynte å se seg selv fra utsiden, og at det var en «*trigger*» til at de startet alt arbeidet med å beskytte seg.

Direktørsvindel (CFO) og phishing mail er de vanligste svindelmetodene Wintershall Dea utsettes for i dag. Løsepengevirus var mer vanlig før, men selskapet har i dag systemer på plass for å sikre seg mot dette. Dette står i kontrast til informasjonen fra Politiets trusselvurdering (2021: 22) som skriver at løsepengevirus er den største nåværende trusselen på datakriminalitetsfeltet. I tillegg opplever selskapet hacking av Office 365 kontoer, men dette er de også sikret for gjennom tofaktorautentisering. Selskapet har «four eyes principle», signering og regler når det gjelder innkjøp og betalinger. Regninger må godkjennes gjennom en totrinnsfase som skal fange opp hvis det er noe som ikke stemmer. I tillegg skal det ikke være mulig å sende en regning uten at det finnes en ordre på den, og alt må gjennom to godkjennere og en utbetaler. Informant A forteller at prosessen slik skal være «*vanntett*». At prosesser er *vanntette* forstås i denne kontekst som en ambisjon heller enn en realitet. Vi har tidligere sett at ekspertene ikke ønsker å ta noen risikoer og heller ingen sjanser, men at de samtidig er klar over at man alltid lever med noe risiko og noe sårbarhet. Det blir også uttalt fra ekspertene at man aldri kan stole fullt og helt ut på de tekniske barrierene.

Alle ekspertene uttrykker at svindelforsøk har blitt mer målrettet og avansert, og at trusselaktørene har blitt flinkere. Dette synet støttes av Balzacq og Cavelty (2016: 176) som sier at cyberangrep alt i alt har blitt farligere ettersom de er bedre organisert og sofistikerte samt vanligere og kostbare. En av ekspertene mener at teknologien kan forklare dette og sier blant annet at «når teknologien blir bedre blir svindelen bedre». Informanten bruker google translate som eksempel og forklarer at det i dag er vanskeligere å se på språket at det er et svindelforsøk fordi denne tjenesten har blitt bedre. En annen ekspert forteller at trusselaktørene bruker personlig informasjon, gjerne fornavn og etternavn, og utgir seg for å være en fra selskapet. En ekspert sier også at direktørsvindel har blitt mer avansert da det ikke lenger kun kommer en mail fra «direktøren» i selskapet, men at det i tillegg ringes fra «gyldige» telefonnumre. Ekspert C forteller også at enkelte trusselaktører leier inn skuespillere som en del av apparatet sitt for å manipulere og svindle.

5.1.5 Utsatthet for svindelforsøk

De som jobber med finans samt ansatte som er publisert på nettsider er ifølge ekspertene mest utsatt for å bli offer og misbrukt i svindelforsøk. Dette støttes av Nasjonal sikkerhetsmyndighet som i sin risikoanalyse for 2020 skriver at personer med beslutningsmyndighet og personer som har tilgang til spesielt sensitiv informasjon er av spesiell interesse for trusselaktører (NSM, 2020: 22). Samtidig forteller informant B at alle ansatte er potensielle ofre for trusselaktører, blant annet fordi mailadresser til ansatte kan kjøpes på darknet og misbrukes. At alle er potensielle ofre for cyberkriminalitet støttes av Van't Hoff-de Goede mfl. (2021: 22). På spørsmål om selskapet har restriksjoner på hva ansatte kan legge ut på nett sier ekspertene at de har en intern policy, for eksempel hvis noen skal representere selskapet. De har regler knyttet til hvem som kan uttale seg, for eksempel til media, på vegne av selskapet og disse ansatte har mottatt trening og opplæring i dette. Ellers har selskapet ingen klare regler for hva ansatte legger ut på nett i privat regi, men flere av informantene mener at ansatte selv må ta ansvar. Informant A sier blant annet at:

> *«Vi har ingen [regler]. Men ansatte må forstå at de selv er en verdifull person. Kanskje tenker de selv at de ikke er det. Men alle har en verdi. En Office 365 konto har en enorm verdi, også en G-mail og en Facebook konto kan gi mye informasjon. Linkedin og. Folk må forstå at de må hindre at denne informasjonen ikke skal misbrukes. Men sånn ellers, alle vet jo at jobber du i regnskap med å betale ut penger så skal du ikke skrive på Linkedin eller Facebook at dette er en arbeidsoppgave du har. Vi har jobbet mye med å lage en god grunnmur når det gjelder IT-sikkerhet og hva de ansatte kan».*

Informant E støtter utsagnet og opplever samtidig at selskapet ikke har hatt noe problem med dette:

> *«Jeg tenker at vi som ansatte må være bevisst på at vi er ansatt der vi er ansatt. Skal vi ut og ha en presentasjon for eksempel, skal den gjennom kommunikasjonsavdelingen først. Men jeg har ikke opplevd det som et problem at folk legger ut ting på for eksempel Facebook».*

Ekspert D forteller om en mindre alvorlig hendelse som skjedde for ikke så lenge siden. Da var det en person som hadde laget en Linkedin-profil og sendt ut venneforespørsler til ansatte i selskapet. Vedkommende hevdet å jobbe i Wintershall Dea, og skulle selge en bil som en ansatt. Senere fikk selskapet en telefon fra personen som kjøpte bilen fordi han ønsket kontakt med

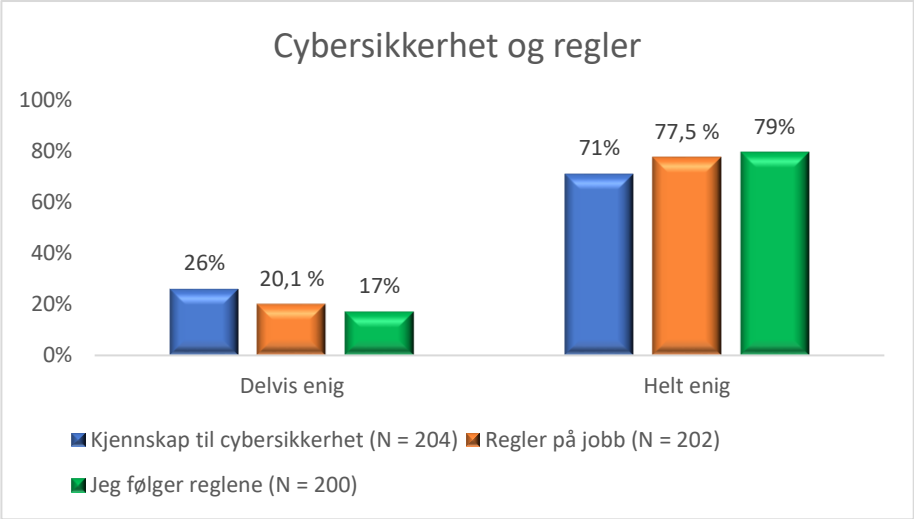
han som «jobbet» hos dem. Selskapet kunne ikke gjøre noe med dette, men informanten presiserer at dette er et godt eksempel på at man må være forsiktig med å godta ukjente «venne» forespørsler, og hvilken informasjon man deler på sosiale medier da det lett kan misbrukes.

Dette synet støttes av Nasjonal sikkerhetsmyndighet som sier at det er viktig å være bevisst over hvilken informasjon man deler om seg selv og om virksomheten man jobber i på sosiale medier og ulike digitale plattformer. Dette fordi trusselaktører kan bruke slik informasjon som en inngangsportal. NSM mener at virksomheter bør gi klare retningslinjer og anbefalinger til ansatte om hvordan de bør oppføre seg i det digitale rom (NSM, 2020: 33).

5.1.6 Ansattes syn på cybersikkerhet

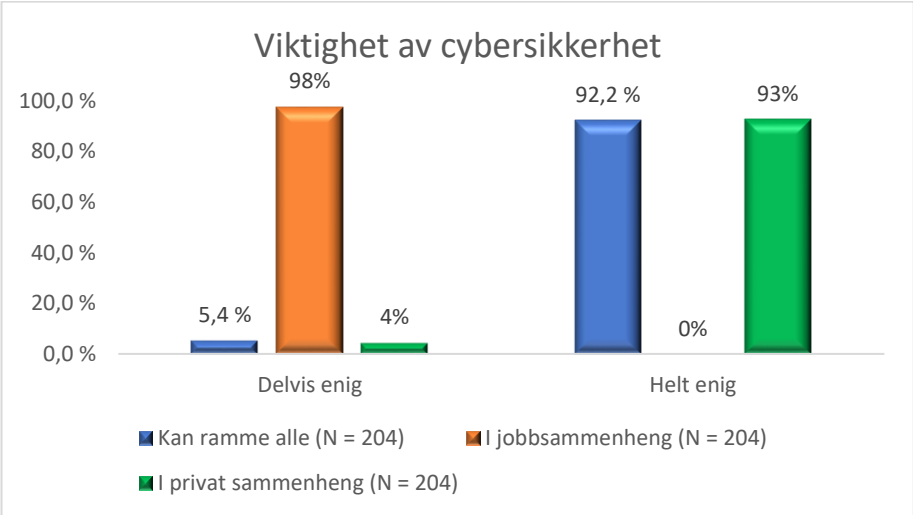
Det ser ut som ekspertene i Wintershall Dea, i likhet med Zedner (2009), har erkjent at en absolutt tilstand av sikkerhet ikke er mulig når det kommer til cyberangrep. Dette fordi ekspertene gir uttrykk for at man alltid vil leve med noe risiko og noe usikkerhet og forsøker å beskytte seg mot cyberangrep med forebyggende tiltak. Når det kommer til den subjektive tilstanden av sikkerhet som handler om individers egen følelse av trygghet (Zedner, 2009), kan man kanskje i en organisasjon si at ansattes forståelse av trusler vil representere selskapets subjektive tilstand av sikkerhet. Forskning viser at menneskelig svikt i dag er den største årsaken til sikkerhetsbrister (Da Veiga, 2020). Flere studier viser også at det er en sammenheng mellom opplevd alvorlighetsgrad og atferd på internett (Crossler mfl., 2017; Jansen, 2018). Dersom ansatte ikke anser risikoen for å bli utsatt for cyberangrep som like stor som ekspertene kan dette få konsekvenser for det forebyggende arbeidet i selskapet. Sett slik vil ansattes forståelse av cybersikkerhet ha stor betydning for Wintershall Dea sitt forebyggende arbeid.

I lys av dette vil det være hensiktsmessig å undersøke de ansatte i Wintershall Dea sitt syn på cybersikkerhet. Figur 5-2 viser at 71% av respondentene er helt enige i påstanden om at de vet hva cybersikkerhet er og 26% er delvis enige. Resultatene viser også at 77% av de ansatte er helt enige i påstanden om at Wintershall Dea har regler for cybersikkerhet, og 79% er helt enige i at de følger disse reglene. Likevel ser man at det er 20% som er delvis enige i at det er regler på arbeidsplassen og 17% som er delvis enige i at de følger regler. Selv om de fleste har svart helt enige på disse påstandene er det interessant å se at såpass mange har svart delvis enige. Med tanke på den store risikoen dataangrep utgjør for enkeltindivider og organisasjoner og det store fokuset det har i selskapet, ville det vært bedre for det forebyggende arbeidet til ekspertene at flere ansatte var helt enige i disse påstandene.



Figur 5-2: Jeg vet hva cybersikkerhet er. Arbeidsplassen min har regler for cybersikkerhet. Jeg følger de regler og prosesser arbeidsplassen anbefaler når det gjelder cybersikkerhet.

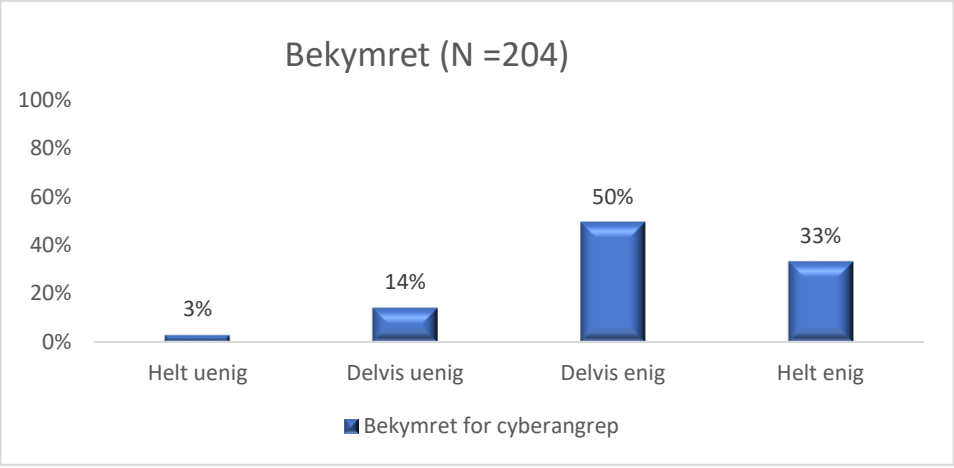
Figur 5-3 tyder på at de ansatte er enige i at dataangrep og andre sikkerhetshendelser kan ramme alle da hele 92% oppgir at de er helt enige i denne påstanden. Samtidig er 98% av respondentene helt enige i at cybersikkerhet er viktig i jobbsammenheng og 93% er helt enige i at det er viktig i privat sammenheng. Dette tyder altså likevel på at de ansatte i Wintershall Dea er klar over at cyberkriminalitet og cybersikkerhet er en stor trussel i dagens samfunn. Ifølge Malmedal og Røislien (2019: 100), som kartla den digitale sikkerhetskulturen i Norge, er risikooppfattelsen til individer en viktig faktor som påvirker hvordan vi tenker og handler når det kommer til digitale trusler. Hvilken effekt det har for ekspertenes forebyggende arbeid at ansatte synes å være klar over risikoen for digitale trusler, er interessant og vil ses nærmere på i del to av analysen.



Figur 5-3: Dataangrep og andre sikkerhetshendelser kan ramme alle. Cybersikkerhet er viktig i jobbsammenheng. Cybersikkerhet er viktig i privat sammenheng.

Det er viktig å poengtere at selv om de ansatte synes å være enige i påstandene som er listet opp til nå, er det ikke nødvendigvis slik at de handler deretter. Malmedal og Røislien (2016: 77) sier at det synes å være et gap mellom det man forventer at mennesker gjør for å beskytte seg selv på nettet, og det de faktisk gjør. Hvor godt internettbrukere beskytter seg mot cyberkriminalitet er ukjent (Van't Hoff-de Goede mfl., 2021: 21) og Crossler mfl. (2013) mener dette delvis skyldes at det er forskjell på hvordan folk sier eller tror de oppfører seg på internett og hvordan de faktisk oppfører seg. Tidligere studier viser at flere kun oppfører seg trygt på internett i begrenset grad, og at utrygg atferd på internett er vanlig (Van't Hoff-de Goede mfl., 2021: 23).

I spørreundersøkelsen ble ansatte også spurt om de bekymrer seg for cyberangrep.
Figur 5-4 viser at 33% av de ansatte er helt enige i at de bekymrer seg og at 50% av respondentene er delvis enige i denne påstanden. Som ekspertene forteller og litteraturen viser, er cyberangrep noe som kan ramme alle og utviklingen i antall angrep er bekymringsverdig. NSM sier blant annet at «Nettverksoperasjoner utgjør en alvorlig risiko for norske virksomheter og samfunnsfunksjoner, og NSM ser et jevnt trykk av slike operasjoner mot mål i Norge. I tillegg blir de vanskeligere å oppdage, og metodene sammensatte» (NSM, 2020: 25). Dersom ansatte er bekymret for cyberangrep kan det tenkes at de utfører sikker atferd på nett. Forskning viser derimot at det ikke synes å være en sammenheng mellom opplevd sårbarhet og trygg atferd på internett (van't de-Goede mfl., 2021). I del to av analysen vil det undersøkes hvordan ulikhet i syn på cybersikkerhet samt bekymringer slår ut i forebyggingsstrategiene.



Figur 5-4: Jeg bekymrer meg for cyberangrep.

5.1.7 Oppsummerende drøfting av del en

Del en av analysen har sett på hvilket trusselbilde Wintershall Dea må forholde seg til samt hvordan ekspertene og ansatte forstår risiko og trusler i forhold til cyberkriminalitet. Ut ifra det ekspertene forteller er det tydelig at fokuset på cybersikkerhet er større enn noen gang. Olje- og gassektoren er digital sårbar i alle ledd i verdikjeden og derfor et stort mål for ulike trusselaktører. Omfanget av trusler og mulighetene for nye type trusler gjør at det er viktig for ekspertene å til enhver tid holde seg oppdatert på trusselbildet. Det uttrykkes i den sammenheng at det er en livsstil å arbeide med cybersikkerhet. Selskapet blir forsøkt svindlet hver dag og svindelforsøkene blir stadig mer målrettet og avanserte på grunn av teknologiens hurtige utvikling. Samtidig er alle ansatte potensielle ofre for denne typen kriminalitet. Det ser dermed ut til at fenomenene cyberkriminalitet og cybersikkerhet har endret seg i løpet av de siste årene og at de stadig er i endring. Det fører videre til at ekspertene aldri vet hvilken trussel de står ovenfor og kan utsettes for. Cybersikkerhet ser dermed ut til å være et spill i kontinuerlig utvikling og et kappløp mellom de som jobber med cybersikkerhet og potensielle trusselaktører. Ekspertene forsøker å holde seg oppdatert til enhver tid samtidig som potensielle lovbrytere stadig finner nye måter å utføre angrep på.

Selv om ekspertene uttrykker at de alltid må holde seg oppdatert på trusselbildet er dette vanskelig fordi trusselbildet er i stadig utvikling. Koronapandemien er et godt eksempel på dette. Om pandemien har hatt påvirkning for cybersikkerheten til selskapet er det derimot delte meninger om. Noen av ekspertene mener at ansatte er sikre uansett om de jobber hjemmefra eller på kontoret. Andre mener derimot at ansatte er mer utsatt på hjemmekontor ettersom de mister kommunikasjon med kolleger og ikke får dagligdagse påminnelser som for eksempel folderne som er satt opp i lokalene med budskapet om at ansatte er den viktigste personen for å ivareta selskapets sikkerhet. De ansatte gir utrykk for at de føler seg tryggere når de jobber på kontoret enn ved hjemmekontor. Det er likevel en høy andel i begge påstandene som oppgir at de kun er delvis enige i at de føler seg trygge når det kommer til cybersikkerhet på kontoret og ved hjemmekontor. Dette er et interessant funn med tanke på alt arbeidet ekspertene legger ned i cybersikkerhet og funnet står i kontrast til noen av ekspertenes opplevelse av at ansatte er trygge uansett hvor de jobber fra.

Som en konsekvens av den store trusselen cyberangrep utgjør er petroleumssektoren tuftet på en risikovurdering av alt som gjøres med et mål om å redusere risikoene. Det utvikles barrierer og risikoanalyser for å sikre svekkelser. Ekspertene jobber i den sammenheng fremtidsrettet for å forhindre cyberkriminalitet. Samtidig som det er tydelig at ekspertene har et stort fokus på cybersikkerhet er det forventet av myndighetene at virksomheter har et slikt fokus og en risikobasert tilnærming mot uønskede digitale hendelser. Det forventes at virksomheter skal anvende rammeverk, standarder og styringssystemer for digital sikkerhet. I lys av dette kan regjeringens strategi for å styre cyberkriminalitet kobles til Foucault sitt governmentality-begrep. Den er tydelig rettet mot at staten fordeler ansvaret for digital sikkerhet til private selskaper. På den måten blir staten fortsatt aktiv i kampen mot cyberkriminalitet, samtidig som den styrer på avstand ved å ansvarliggjøre virksomheter og individer. Dermed kan regjeringens strategi for digital sikkerhet også kobles til Garlands ansvarliggjøringsstrategi.

Det er rimelig å anta at ansattes forståelse av cybersikkerhet har stor betydning for hvordan de etterfølger ekspertenes arbeid med forebygging. Det ble derfor undersøkt hvordan ansatte ser på cybersikkerhet. Resultatene viser at flesteparten av respondentene vet hva cybersikkerhet, er enige i at selskapet har regler for cybersikkerhet og at de følger disse reglene. Resultatene indikerer også flere ansatte bekymrer seg for cyberangrep. I tillegg viser resultatene at flesteparten av respondentene mener cyberangrep kan ramme alle, og at cybersikkerhet er viktig på jobb og i privat sammenheng. Slik ser det ut til at det er likheter mellom ekspertenes og ansattes syn på cybersikkerhet. Ettersom flesteparten av de ansatte bekymrer seg for cyberangrep og anser cybersikkerhet som viktig er det rimelig å anta at de oppfører seg trygt på internett for å unngå å bli utsatt. Likevel er det en god del ansatte som oppgir at de kun er delvis enige i at det er regler på arbeidsplassen og at de følger disse reglene.

I det følgende vil del to av analysen presenteres. Her vil det undersøkes hvilke konsekvenser ansattes syn på cybersikkerhet har for det forebyggende arbeidet til ekspertene. I tillegg vil del to gå nærmere inn på hvordan ekspertene jobber med å forebygge cyberkriminalitet samt deres og ansattes opplevelse av arbeidet.

5.2 Del to: Forebygging

Når ekspertene blir spurt hva de gjør for å sikre seg mot dataangrep er barrierer et ord som går igjen. Ifølge Lysneutvalget (2015) er denne barrieretankegangen viktig, og det er vanlig at virksomheter implementerer barrierer for å redusere risiko. Dette gjøres både for å hindre at uønskede hendelser skjer og for å redusere konsekvensene av uønskede hendelser som har inntruffet (NOU: 2015: 13: 157). Ut fra empirien er det tydelig at ekspertene skiller mellom tekniske barrierer og menneskelige barrierer når de snakker om cybersikkerhet. I denne avhandlingen handler tekniske barrierer om de ulike rammeverkene og verktøyene selskapet bruker for å beskytte seg mot dataangrep. Menneskelige barrierer handler om det forebyggende arbeidet selskapet driver med rettet mot de ansatte, og hvilke logikker og mentaliteter de anvender i dette arbeidet.

5.2.1 Tekniske barrierer

Når det kommer til den tekniske siden av cybersikkerhet, altså de tekniske barrierene, er dette noe selskapet har jobbet med i mange år. Ekspertene støtter seg på ulike rammeverk og verktøy for å beskytte seg mot dataangrep. Selskapet har klassiske antivirusprogrammer, og det gjøres i tillegg mye testing. En gang i måneden scannes hele infrastrukturen for sårbarheter, og dersom det kommer et funn på scannen, jobbes det aktivt med å lukke dette. IT-teamet var også tidlig ute med å bestille penetrasjonstesting fra eksterne selskap hvor det kjøres en full scann av hele angrepsflaten og systemene de har. Ut ifra rapporter fra slike tester har ekspertene jobbet målrettet med å sikre de tekniske sidene av IT. Slike tester fra eksterne selskap trekkes frem som sentrale forebyggende verktøy (NOU 2015: 13: 257). I tillegg har Wintershall Dea en programvare som kan hjelpe å identifisere om selskapet utsettes for løsepengevirus. Ekspert D forteller at tankegangen til de som jobber i IT er at «jo flere lag jo bedre. Jo flere elementer du kan legge til jo bedre». IT-teamet er stort og består av folk som jobber med forskjellige fagfelt som for eksempel nettverk, sikkerhet og overvåking. Det er alltid en på vakt som har overordnet ansvar både offshore og onshore. Den som er på vakt har døgnvakt på telefon. Alt som skjer logges gjennom brannmur og selskapet har blokkert trafikk mot alle land som er på «svarte lister» fra offisielle DNS tjenester. Ekspertene er samtidig klar over at det ikke er mulig å beskytte seg helt mot dataangrep, og de stoler heller ikke fullt ut på at de ulike programmene fungerer. Når informant D forteller om programvaren som skal si ifra om selskapet utsettes for løsepengevirus sier hen at: *«Vi følger selvfølgelig med»*. Informanten nevner også at man alltid lever med noe risiko og noe sårbarhet.

De tekniske barrierene Wintershall Dea setter inn for å beskytte seg mot dataangrep kan knyttes til det tidligere omtalte perspektivet situasjonell kriminalitetsforebygging som handler om å endre utformingen av produkter, systemer og miljøer for å redusere kriminalitet (Farrell, 2010). Ved å sette inn antivirusprogrammer, programvare som skal identifisere løsepengevirus samt bestille penetrasjonstesting og blokkere trafikk fra enkelte land er det tydelig at selskapet endrer både produkter og systemer for å forhindre cyberangrep. Slike tiltak er, som tidligere nevnt, vanlig å sette inn for å forebygge slik kriminalitet (Brewer, 2019; Leukfeldt, 2017).

For tiden står leverandørsiden i fokus for ekspertene. Selskapet kjøper tjenester fra tjenestetilbud og bygger i utgangspunktet ikke så mye selv. Likevel er de sterkt involvert på arkitektsiden og forteller hvordan ting skal bygges opp samt stiller krav til hvordan det bygges. Informant D mener at dette er litt av suksessoppskriften til selskapet og forteller:

> *«Hvis vi bare hadde gått inn og kjøpt så har vi egentlig merket at mange av de som tilbyr tjenester i dag gjerne ikke har samme krav som selskapet når det gjelder sikkerhet. Så til og med selskaper som selger tjenester til gass- og olje har gjerne ikke tenkt så mye gjennom sikringen av tjenester, som de har tenkt på funksjonaliteten. Men det er ofte en funksjonalitet som er hovedfokus, at ting virker. Og at det er brukervennlig, men så har de ikke tenkt så mye på alt rundt».*

Vedkommende utdyper videre:

> *«Og det er egentlig veldig spesielt. For ganske etablerte aktører på markedet som du skulle forvente at hadde klare interne krav til hvordan de bygde ting har veldig dårlige rutiner for å ivareta sikringen av kritiske systemer. Systemer som de forventer at vi legger veldig sensitiv informasjon i har vi måttet være med i og stilt krav som... der vi sier at vi ikke vil bruke tjenesten før de fikser en del ting».*

At leverandører må tenke på sikkerhet i produktene sine er også noe NSM trekker frem som viktig. I sin risikorapport fra 2020 skriver de blant annet at «Trusselaktører kan få tilgang til store mengder data dersom sikkerheten i leverandørens løsning eller i datasenteret der slik informasjon lagres, ikke er tilstrekkelig god» (NSM, 2020: 29). Litt av problemstillingen til IT-

avdelingen i Wintershall Dea når det gjelder dette, er at etterhvert som det blir lettere og lettere å kjøpe tjenester så blir IT mindre og mindre involvert. Veldig ofte opplever ekspertene at de involveres sent i denne prosessen og informant D mener at IT derfor lider litt av det som ofte kalles *«skygge-IT»*, som vil si at selskapet selv går ut og kjøper tjenester. IT blir ofte ikke involvert i denne prosessen før det eventuelt viser seg at tjenesten ikke virker som forventet.

Dataangrep kan skje på grunn av teknisk svikt som gjør at tekniske barrierer er svært viktig når det gjelder forebygging av cybersikkerhet. Van't Hoff-de Goede mfl. (2021) trekker frem faktoren *mulighet* som et viktig element for at mennesker skal oppføre seg trygt på internett. Mulighet handler om det materielle miljøet og blant annet tilgjengeligheten av verktøy som støtter sikker praksis. Slik kan det materielle miljøet og faktoren mulighet knyttes til de tekniske tiltakene selskapet setter inn. Van´t Hoff-de Goede mfl. (2021) mener at slike verktøy kan bidra til å styrke ansattes selvtillit til sikker atferd på nett. Samtidig poengterer Lysneutvalget (2015: 3) at selv om implementering av tekniske barrierer er viktig og har fått økende oppmerksomhet, er kvaliteten på disse i liten grad testet og verifisert. Slike barrierer kan på den ene siden gjøre det vanskeligere for potensielle lovbrytere å komme til i systemene. På den andre siden fører det til at potensielle lovbrytere heller forsøker å nå systemene ved å gå via mennesker i organisasjoner (NOU 2015: 13). Tekniske tiltak har ofte kun en begrenset effekt og å bli offer for cyberkriminalitet spores stadig tilbake til menneskelig atferd (Leukfeldt, 2017). Dette kan forklare at det i senere tid har vært en dreining fra angrep på datamaskiner og nettverk til angrep rettet mot enkeltpersoner (NSR, 2020). Når cyberkriminelle retter søkelyset mot mennesker istedenfor maskiner, betyr det at menneskelige barrierer også er svært viktig i arbeidet med cybersikkerhet i virksomheter.

5.2.2 Menneskelige barrierer

Ekspertene har jobbet lenge med den menneskelige faktoren, altså brukersiden, når det kommer til cybersikkerhet. Det uttrykkes at menneskelige barrierer er svært viktig, og at ansatte ses på som selskapets første barriere. I lokalene til Wintershall Dea er det for eksempel plassert foldere med speileffekt på forsiden hvor det står: «Du ser nå på den viktigste personen for å ivareta Wintershall Dea». Igjen kan perspektivet om situasjonell kriminalitetsforebygging trekkes inn. Vi ser her et eksempel på at selskapet endrer miljøet ved å sette inn «speil» som skal virke forebyggende. Informant F uttrykker synet på de ansatte ved å si at «mennesker er det svake punktet». Denne uttalelsen støttes av informant B:

> *«Vi har veldig fokus på at første barriere er våre ansatte, så vi bruker mye penger på at de og skal bli gode. Det er jo da blant annet opplæring... vi er opptatt av opplæring. De ansatte er vårt første sted for beskyttelse. De ansatte er vårt første skjold og det prøver vi å formidle. De sparer oss for mye arbeid hvis de klarer å være dette skjoldet».*

Informant C forteller at det er viktig å *«sette ansatte i stand til å bidra til å ivareta sikkerheten mot trusler fra internettet»*. Informant E setter også ansatte i fokus og mener at *«det viktigste er en bevisstgjøring hos alle ansatte»*. Det er forståelig at ekspertene har dette synet på ansatte i selskapet når det er snakk om cybersikkerhet, og det er heller ikke uvanlig at sikkerhetsbrister forklares med menneskelige faktorer. NorSIS (2020: 10) skriver at den menneskelige faktor er en større sårbarhet enn noensinne, og mørketallsundersøkelsen til NSR (2020: 24) viser at 50% av respondentene mener at sikkerhetsbrudd skyldes menneskelige feil. Malmedal og Røislien (2016: 53) sier at mennesker ofte får skylden for å ta feil valg fordi de ikke forstår hvilken risiko som er knyttet til handlingene deres.

I lys av det ekspertene forteller synes det å handle om å skape en bevissthet blant de ansatte, og videre en ansvarliggjøring av dem i arbeidet med forebygging. Ekspertene ønsker å få ansatte til å forstå at de må være med på å ta ansvar for den digitale sikkerheten til selskapet, og ved å anvende ulike teknikker og metoder kan det se ut som ansatte søkes å gjøres til selvregulerende individer. Dette samsvarer med Garland (1996) sin ansvarliggjøringsstrategi som handler om at staten prøver å styre kriminalitet ved å fordele ansvaret utover i samfunnet, blant annet til organisasjoner som videre skal aktivere handlinger for å forebygge kriminalitet. Det kan også se ut som ekspertene har akseptert at selskapet selv er ansvarlige for sikkerheten når det kommer til digitale sårbarheter, som er en del av strategien til Norge når det kommer til digitale sårbarheter (Departementene, 2019). Hvilke handlinger, teknikker, logikker og metoder Wintershall Dea bruker for å få til dette vil diskuteres videre i oppgaven.

5.2.2.1 Sikkerhetskultur

For å forebygge dataangrep trekker flere av informantene frem viktigheten av å skape en god sikkerhetskultur, og for å skape en slik kultur synes de å legge spesiell vekt på faktorene *tillit, dialog, ledelse* og *opplæring*. Det kan dermed se ut til at en av teknikkene selskapet anvender for å forebygge cyberangrep handler om å skape en god sikkerhetskultur. Jeg vil videre i

oppgaven presentere hva informantene forteller om disse fire faktorene de trekker frem som viktige samtidig som de diskuteres opp mot resultatene fra spørreundersøkelsen samt litteratur og teori.

Informant D forteller at mye av cybersikkerheten til selskapet handler om kultur og læring. Denne uttalelsen støttes av ekspert F som sier at det er viktig med en god kultur hvor ansatte har tillit til hverandre når det er snakk om svindel og cybersikkerhet. Informant B forteller at IT-teamet driver mye opplæring og at de er opptatt av en god dialog mellom dem og ansatte. Videre sier vedkommende at IT-teamet er veldig åpne for at ansatte kan komme til dem hvis de lurer på noe eller ønsker å snakke om for eksempel en mail de har mottatt. Lysneutvalget (2015) trekker også frem kultur som en viktig faktor i det forebyggende arbeidet og kobler videre kultur til sikkerhetskultur. At kultur og sikkerhetskultur er viktig for å forhindre cyberangrep i organisasjoner støttes også i litteraturen (NOU 2015: 13) og av flere sikkerhetsforskere, blant annet Alshaikh (2020) og Da Veiga (2020).

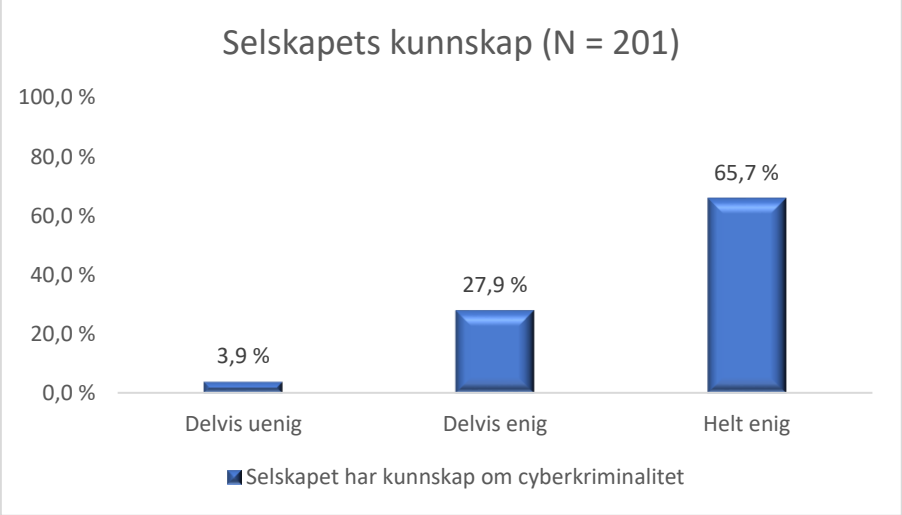
Ekspertene synes å ha en tilnærming til cyberkriminalitet som noe som kan forebygges ved å styre ansattes atferd ved hjelp av ulike teknikker som for eksempel en sterk sikkerhetskultur. Det kan dermed argumenteres for at ekspertene har samme forståelse av kultur som den som anvendes innenfor retningen *bedriftskultur* (Eriksson-Zetterquist mfl., 2015). Det kan også se ut til at ekspertene prøver å skape en sikkerhetskultur som styrer den kollektive oppmerksomheten og atferden i møte med cyberkriminalitet (Engen mfl., 2016). Her ser vi også en styringslogikk hos ekspertene som igjen kan knyttes til governmentality og responsibilization begrepene. I tillegg er det tydelig at Wintershall Dea sitt arbeid med å forebygge cyberkriminalitet er sterkt koblet til risikomentaliteten innenfor nodal governance perspektivet. Dette fordi vi ser at ekspertene har et proaktivt syn og en fremtidsrettet tankegang når det kommer til arbeidet med og forebygging av fenomenet.

Det kan se ut til at ekspertenes arbeid for å forebygge cyberkriminalitet samsvarer med SETA-tilnærmingen for en god cybersikkerhetskultur. Tilnærmingen går ut på å implementere regelmessige initiativer for kommunikasjon og sikkerhetsopplæring samt trening og bevissthet (Alshaikh, 2020). Initiativene sikkerhetsopplæring og trening kan knyttes til opp*læring*. Initiativene kommunikasjon og bevissthet kan knyttes til *dialog*. *Tillit* kan knyttes til SETA-tilnærmingen. Det er rimelig å anta at ingen av disse faktorene for å bygge en god sikkerhetskultur, samt for å forebygge cyberkriminalitet vil være mulig uten en tillitsrelasjon

mellom ekspertene og ansatte i organisasjonen. I spørreundersøkelsen ble de ansatte i Wintershall Dea presentert for flere påstander som kan knyttes til SETA – initiativene. Resultatene fra spørsmålene kan være en indikator på hvordan ansatte opplever forebyggingsarbeidet og sikkerhetskulturen til selskapet.

Tillit

Samarbeid basert på tillit er nødvendig for en funksjonell sikkerhetskultur. Gjensidig tillit mellom arbeidsgiver og ansatt samt mellom ansatte i organisasjoner kan føre til harmonisering av verdier, kunnskap og atferd hos partene og dermed bidra til en formålstjenlig sikkerhetskultur (Da Veiga, 2020). Figur 5-5 viser at 66% av respondentene er helt enige i at Wintershall Dea har kunnskap om cyberkriminalitet og de trusler det medfører, og 28% er delvis enige i denne påstanden. Resultatene tyder dermed på at flesteparten av respondentene har tillit til selskapets kunnskap om cyberkriminalitet. Videre kan det argumenteres for at en slik tillit er viktig for ansattes etterfølgelse av regler og rutiner i sikkerhetsarbeid.

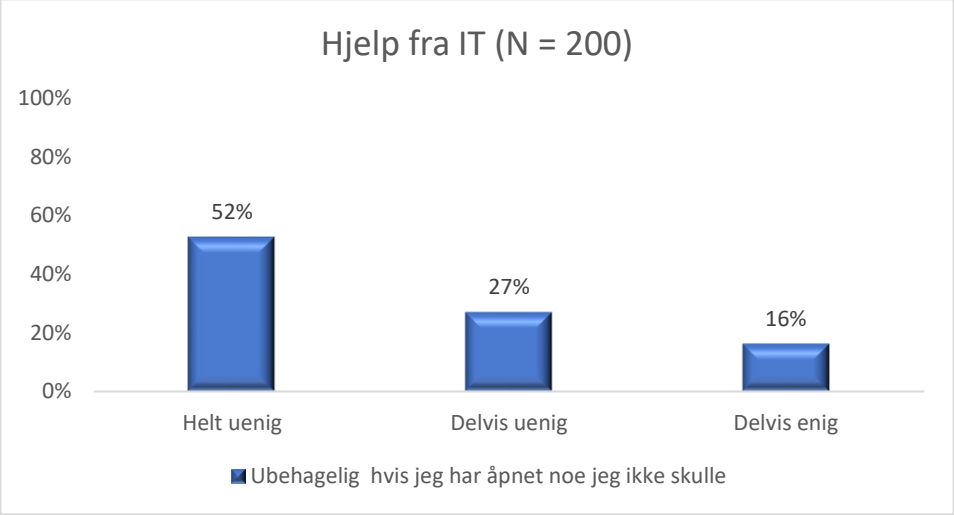


Figur 5-5: Jeg opplever at selskapet har kunnskap om cyberkriminalitet og de trusler det medføre.

Dialog

De ansatte ble også spurt om de synes det er ubehagelig å søke hjelp fra IT-teamet hvis de har åpnet noe de ikke skulle. Figur 5-6 viser at 52% av respondentene er helt uenige i denne påstanden, mens 27% er delvis uenige. At 79% av respondentene har valgt et alternativ med begrepet uenig i seg kan tyde på at flesteparten opplever at det er god kommunikasjon mellom dem og ekspertene. Slik kan det argumenteres for at ekspertene har oppnådd ønsket om en god dialog. Samtidig, i og med at 16% har svart delvis enig i påstanden, betyr det at noen opplever

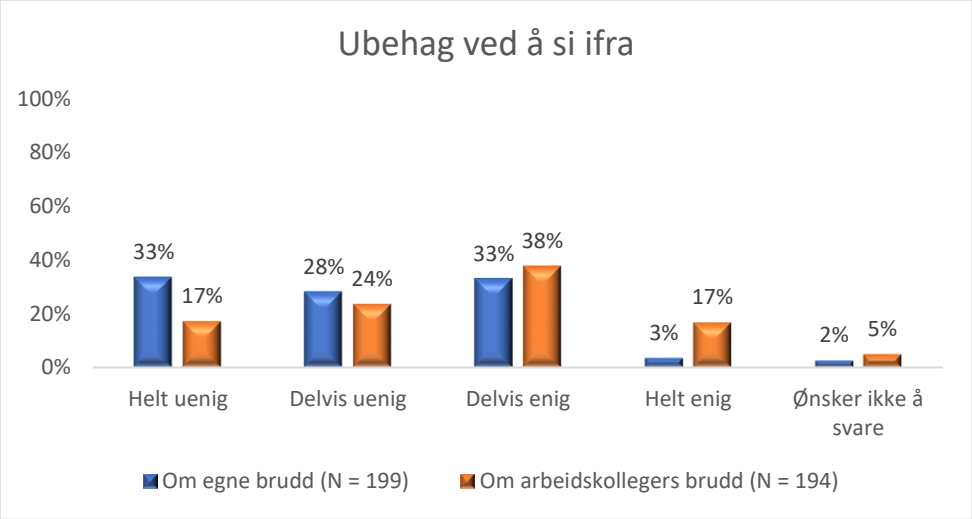
dette som ubehagelig. Som tidligere nevnt slo Wintershall og Dea seg sammen til selskapet Wintershall Dea for et par år siden. Sammenslåingen kan være en mulig forklaring på dette, for eksempel at ikke alle ansatte kjenner ekspertene like godt og at det derfor er ubehagelig å oppsøke hjelp. I tillegg nevnte noen av ekspertene i intervjuene at de to selskapene har hatt ulikt fokus på cybersikkerhet før sammenslåingen. Ekspertene gjennomfører av og til tester for å blant annet undersøke ansattes villighet til å trykke på linker. Dette fører de statistikk på, og denne statistikken har endret seg etter sammenslåingen. Det tar naturligvis tid å bli kjent med hvilke sikkerhetsrutiner som gjelder i et selskap og å motta opplæring, og dette kan videre gjenspeiles både i tester og kampanjer som utføres av ekspertene samt i resultatene i avhandlingens spørreundersøkelse.



Figur 5-6: Jeg synes det er ubehagelig å søke hjelp fra IT-teamet hvis jeg har åpnet noe jeg ikke skulle ha åpnet.

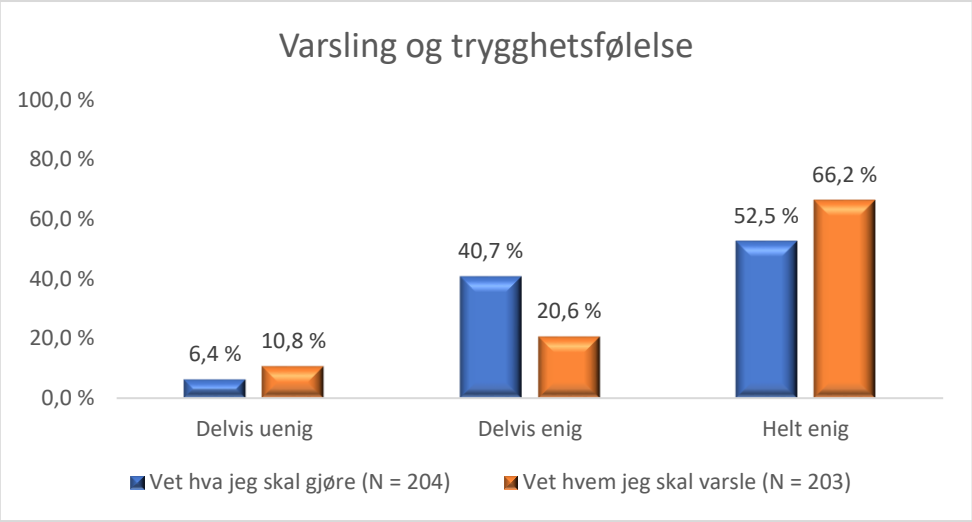
Dersom ansatte opplever ubehag ved å søke hjelp fra IT-teamet er det rimelig å anta at det kan føre til at de ikke sier fra ved brudd på selskapets IKT-regler. For at svindel og dataangrep skal oppdages er det viktig at ansatte rapporterer om sikkerhetsbrister. Derfor ble ansatte spurt om de synes det er ubehagelig å si fra om egne brudd på IKT-regler. Figur 5-7 viser at kun 3% er helt enige i denne påstanden mens 33% er delvis enige. Det tyder dermed på at det også i denne påstanden er ansatte som opplever ubehag ved å kontakte IT-teamet. En mulig forklaring kan knyttes til selskapets store fokus på opplæring i cybersikkerhet, og at ansatte derfor synes det er flaut å si fra om noe de har fått opplæring i og trent på at de ikke skal gjøre.

I tillegg ble ansatte spurt om de synes det er ubehagelig å si fra om arbeidskollegers brudd på IKT-regler, som også er viktig for å avdekke sikkerhetsbrister. Figur 5-7 viser at 17% av respondentene er helt enige i denne påstanden og at 38% er delvis enige. 5% har ikke ønsket å svare hvilket utgjør 10 av 204 respondenter. I lys av dette kan det se ut til at ansatte opplever det som mer ubehagelig å si fra om kollegers brudd på IKT-regler enn egne brudd. Det er rimelig å anta at tillit mellom ansatte og ekspertene spiller en rolle for om ansatte gir beskjed om IKT-brudd.



Figur 5-7: Jeg synes det er ubehagelig å si fra om egne brudd på IKT-regler. Jeg synes det er ubehagelig å si fra om arbeidskollegers brudd på IKT-regler.

En mulig forklaring på at noen av respondentene ikke gir beskjed om egne eller kollegers brudd på IKT-regler kan være at de ikke vet hva de skal gjøre eller hvem de skal kontakte om noe som avviker fra normalen skjer. Figur 5-8 viser derimot at 93% av respondentene er enige i at de vet hva de skal gjøre og 87% oppgir at de vet hvem de skal varsle. Likevel kan det tenkes at respondentene som har valgt svaralternativet delvis enig på disse påstandene ikke er helt sikre på hva de skal gjøre eller hvem de skal varsle når noe som avviker fra normalen skjer. Dette kan være en grunn til at de lar være å kontakte IT-teamet.



Figur 5-8: Jeg vet hva jeg skal gjøre om noe som avviker fra normalen skjer. Jeg vet hvem jeg skal varsle om noe som avviker fra normalen skjer.

Ledelse

Ekspertene trekker også frem ledelsen i selskapet som en viktig faktor for å skape en god sikkerhetskultur. Informant D forteller blant annet at *«ledere setter kulturen i selskapet, og hvis ikke lederen leder an, og på en måte jobber på riktig måte, er gode forbilder, så sliter du med å få med deg resten»*. Ekspertene utrykker samtidig at de får god støtte fra både ansatte og ledelsen. Informant A hadde følgende å si om dette: *«Det er og veldig høy forståelse for arbeidet som må gjøres i ledelsen. Sånn at vi har på en måte ganske frie tøyler i forhold til å få sikret alt»*. At ledere er viktig for å skape en god kultur støttes også i litteraturen. Schein (2010, i Whelan, 2017) mener at ledere setter standarden for hvordan man tenker og handler, og at denne væremåten videre aksepteres og følges av de ansatte. NSM (2020: 41) setter også fokus på ledere, og mener at sikkerhetsengasjerte ledere er viktig for sikkerhetstilstanden i virksomheter. Dersom virksomheter har en fraværende ledelse i sikkerhetsspørsmål kan det gjøre at avstanden til sikkerhetsarbeidet blir for stort. I tillegg mener de det kan føre til at det blir vanskeligere å beslutte, gjennomføre og evaluere tiltak som er relevante. Eriksson-Zetterquist (2015) knytter også god kultur til en tilstedeværende ledelse. Van't Hoff-de Goede mfl. (2021) trekker frem faktoren *mulighet* som et viktig element for at mennesker skal oppføre seg trygt på internett. Som tidligere nevnt handler mulighet om det materielle miljøet men også det sosiale miljøet og hvordan menneskene rundt oss påvirker atferden vår. Herath og Rao (2009) fant i sin studie at sosial innflytelse fra ledere kan ha stor påvirkning for sikker atferd på internett i organisasjoner.

Det kommer tydelig frem fra intervjuene med ekspertene at *tillit*, *dialog* og *ledelse* ses som viktige for å skape en god sikkerhetskultur for å forebygge cyberangrep. Det synes videre å virke som at tillit må ligge i bunn for at opplæringsarbeidet skal fungere ideelt. Når det kommer til opplæring er dette den faktoren ekspertene trekker frem mest når de forteller om forebygging av cyberkriminalitet. Videre vil jeg derfor først presentere hva ekspertene forteller at de gjør for å lære opp ansatte i cybersikkerhet. Deretter vil ekspertenes arbeid med opplæring i svindelforsøk og opplæring i passordbruk beskrives samtidig som funn fra det kvantitative materialet trekkes frem. Deretter vil jeg presentere resultater fra spørreundersøkelsen som belyser hvordan ansatte opplever opplæringen. Til slutt vil jeg presentere tiltaket champion-program som kan settes inn i forebyggingsarbeid av cyberkriminalitet.

Opplæring

Ekspertene gjør mye forskjellig for å lære opp ansatte i cybersikkerhet. Blant annet gjennomføres det hvert år en «security awareness» kampanje som alle ansatte må delta på. Ekspertene lager da en presentasjon som vises avdelingsvis. Noen ganger holder IT-manager presentasjonen for å forsterke alvoret. Her går de igjennom fokusområdet sitt og hva ansatte må bli flinkere til. I presentasjonen viser de hva som er trendene i media, hva myndighetene snakker om og hva det er viktig å være obs på. En av informantene forteller at ekspertene prøver å tilrettelegge presentasjonen til det de ser er aktuelt å presentere, samtidig som de får med det de selv synes er viktig. Ekspert B sier at de prøver å knytte informasjonen opp til hendelser som er skrevet om i media. Dette forklares med at det da er ferskt i minne til ansatte som sannsynligvis har lest i media at det faktisk er noe som kan skje og som kan få store konsekvenser. Informant A har følgende å si om denne presentasjonen:

> *«Vi viser en del funn og ting som har skjedd. Vi prøver å gjøre det så real som mulig, og dra opp aktuelle saker fra vårt selskap, og sammenligner litt med hva som skjer ellers i verden... og nye trender og ting som skjer». Presentasjonene skaper mye engasjement, dialog og spørsmål».*

I forkant av presentasjonen er det vanlig at ekspertene har kjørt en form for test slik at de har noe spennende og aktuelt å fortelle om og samtidig vise hvorfor de fokuserer på det de gjør. De forsøker å lære ansatte ting de mener de kan forvente av dem som sluttbrukere. Selskapet har også e-learnings portaler hvor ansatte kan gå inn og klikke seg igjennom. I 2021 har det også blitt startet et nytt globalt cybersecurity læringsopplegg for alle ansatte, basert på en rekke korte

filmer som tar for seg ulike aspekter ved cybersikkerhet. I tillegg arrangerer HSEQ- avdelingen hvert år en «Safety Day» hvor alle ansatte kan delta. Her settes det opp ulike stands og IT-avdelingen har sin egen. Målet med denne dagen er at ansatte skal få informasjon og kunnskap om ulike tema på ulike stands. Alle nyansatte skal igjennom en e-learning om cybersikkerhet. Informant A forteller at ekspertene gir ut informasjon til de ansatte om IT-sikkerhet generelt, og at de ønsker de ansatte skal ha en generell forståelse av at alt kan forfalskes. Samtidig sier hen at vi i dag lever i en digital verden hvor alle vet at de ikke skal trykke på usikre linker. Vedkommende mener at man må kunne heve seg over dette, i hvert fall når det gjelder de yngre generasjonene. Informanten sier også at den eldre generasjonen er mer sårbar når det kommer til dette. Det er tydelig at opplæring av ansatte er et viktig fokus for ekspertene. Kunnskap eller bevissthet om sikker atferd trekkes også frem av van´t Hoff-de Goede mfl. (2021) som en nødvendighet for at mennesker skal oppføre seg trygt på internett. Dette synet støttes også av Michie mfl. (2011). Studier som har undersøkt kunnskap knyttet til sikker atferd på nett viser derimot ulike resultater (van´t Hoff-de Goede mfl., 2021). På den ene siden fant Downs mfl. (2007) i sin studie at mennesker som for eksempel kan identifisere usikre nettsteder er mindre sårbare for phishingangrep. På den andre siden fant Cain mfl. (2018) ingen forskjell mellom mennesker som hadde fått opplæring i cybersikkerhet og de som ikke hadde det når det kommer til sikker atferd på nett.

Ekspertene i Wintershall Dea kjører i tillegg ulike tester og kampanjer på ansatte. Dette kan for eksempel være phishing og smishing- kampanjer hvor ansattes villighet til å klikke på usikre linker testes. Informant D forteller om en SMS-lotto som ble utført der IT-teamet sendte ut en melding til ansatte hvor mottakerne kunne lese at de hadde vunnet fem tusen. For å hente premien måtte det bare klikkes på linken som lå vedlagt i meldingen. De ansatte som trykket på linken fikk opp en siden hvor de ble informert om at de hadde blitt lurt. Når informant D forteller om denne testen er hen klar på at det er forståelig at flere går på disse kampanjene. Samtidig mener hen det er lurt å få ansatte til å tenke over at de gjorde noe de ikke skulle gjort, og presiserer at de ønsker en åpen dialog mellom IT-teamet og de ansatte hvis det skjer noe. Hen forteller blant annet at:

> *«Du prøver hele tiden å finne nye vinklinger, og få det litt faktisk så folk får oppleve det. Og få litt den der... shit, jeg dreit meg faktisk litt ut. For det er jo en annen ting. Vi har jo lyst til at folk sier fra når de gjør feil. Det er ikke sånn at du får kjempe kjeft. Det er veldig lett å gå på disse kampanjene etter hvert. Det begynner å bli bra språk. Det*

begynner å bli relevante ting. De identifiserer jo folk i selskapet og de har riktig telefonnummer og signaturer og titler og... de er ekstremt profesjonelle. Så det viktige er jo at folk, når de får den mageføIelsen, sier ifra. Både hvis de har gjort noe feil, eller hvis de har mottatt noe sånt, til oss. Og den kulturen prøver vi å få».

Informant A er enig i at det er viktig å lage presentasjoner og tester som får ansatte til å forstå hvor lett det er å gå på svindelforsøk. Vedkommende forteller om en gang da ekspertene sendte ut en SMS til flere ansatte hvor det stod at de hadde besøk som ventet på dem i resepsjonen. I SMS-en kunne de trykke på en link for å se bilde av den besøkende. SMS-en kom i samme logg som tidligere meldinger fra resepsjonen, og det var en del som gikk på. Det var også noen som dro ned til resepsjonen for å se hvem som var på besøk. Ekspert B sier at teamet lærer de ansatte til å tenke annerledes når det er jobb og at de ønsker å gi dem et rammeverk og kunnskap til å ta de rette valgene. Informanten forteller at hen en gang sendte ut en smishing fra «lederen» i avdelingen samtidig som hen holdt et foredrag. Dette var for å vise hvor enkelt det er å sende ut en smishing og utgi seg for å være noen andre. Vedkommende snakker også om samme SMS-kampanje som informant A, og bruker det som et eksempel for å illustrere at ekspertene fokuserer på å bruke eksempler istedenfor å kun fortelle om cybersikkerhet til de ansatte. Hen legger til at:

«50% trykket på linken og flere gikk ned i resepsjonen for å se hvem som hadde kommet på besøk. Jeg lagde en nettside som kom opp når de trykket på linken hvor det stod at de ble lurt og at det var en test. Vi ønsker at folk ikke skal trykke ukritisk på meldinger».

Ekspertene forteller at de opplever at ansatte tar godt imot opplæringen de får. Informant A belyser dette og sier at de stort sett får gode tilbakemeldinger, spesielt når IT-teamet har stand og viser reelle ting fordi det skaper engasjement hos de ansatte. Informant B forteller at de fleste ansatte er positive til og interesserte i arbeidet IT-teamet gjør. På spørsmål om hvilken nytte ekspertene tror opplæringen har er flertallet enige i at den har god effekt. Det ekspertene viser frem på «Safety Day» trekkes frem som noe av det mest effektive de gjør. Der viser de for eksempel frem hvor lett det er å hacke seg inn på telefoner eller å få alle skjermer til å gå i svart. De opplever at dette skaper stort engasjement blant de ansatte. Informant B sier følgende når hen snakker om dette arrangementet:

> *«Ja, så da pleier vi å stå der. Men da pleier vi å lage litt mer kule ting. Da kjører vi ofte demo. Da viser vi frem via eksempler der vi enten står og hacker telefoner eller ja... viser ekte ransomware, hvordan det faktisk skjer. Vi har laget masse forskjellige demoer opp igjennom. Og det synes jo folk er veldig spennende. Vi har jo fått mye skryt etter disse safety-dayene fordi de synes at IT alltid liksom skiller seg ut. Og det har vi jo prøvd å gjøre for å få folk til å få opp øynene da».*

Informant C forteller at det IT-teamet har vist frem på Safety-Day har blitt snakket om i lang tid etterpå. Vedkommende har blant annet hørt snakk om det i kaffekroken og mener det fører til at ansatte som har gått glipp av denne dagen også får høre om det. Samtidig sier ekspertene at ikke alt av opplæringsarbeidet fungerer like bra. Informant C mener det henger sammen med hvor ofte ansatte blir presentert for det, og at det ikke fungerer hvis ansatte skal høre om cybersikkerhet hele tiden. Utsagnet støttes av ekspert B som har drevet med dette i en del år. Vedkommende forteller at ansatte ikke orker for mye informasjon om cybersikkerhet og at ekspertene derfor tar mye av opplæringen muntlig. Informant A forteller at de har prøvd å vise ting på nett, men at det ikke tjener til sin hensikt. For eksempel har ekspertene sendt ut presentasjoner som ansatte skal gå igjennom selv, men det har vist seg å være nytteløst. Selskapet har derfor valgt å heller fokusere på andre måter å drive opplæringen på. Informant A forteller samtidig at disse metodene kanskje ikke er helt tradisjonelle, men at de opplever dem som gode måter.

Opplæring i svindelforsøk

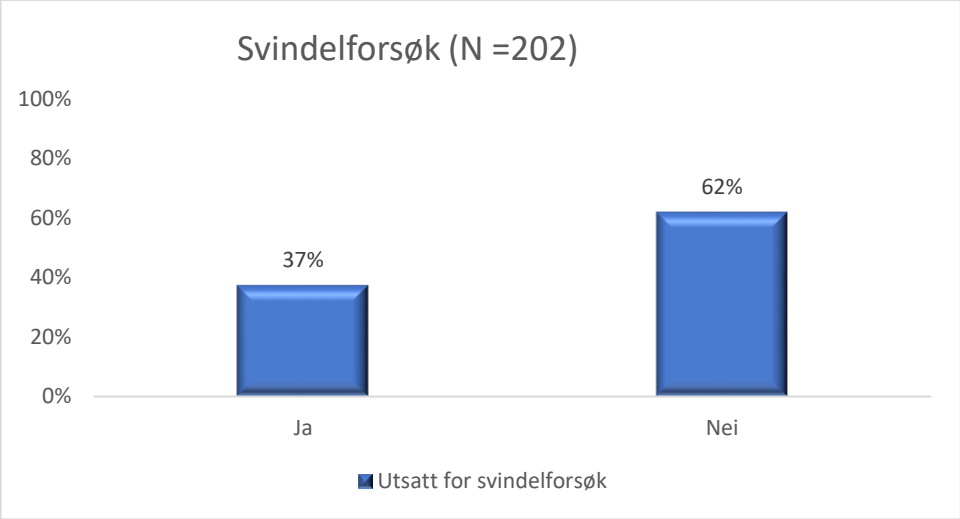
Dersom ansatte mottar noe de mistenker kan være et svindelforsøk forteller ekspertene at de sender det videre til IT-teamet, gjerne via servicedesken. Det finnes også informasjon på nett om hva de skal gjøre hvis dette skjer, og IT teamet oppfordrer ansatte til å tenke kritisk. For eksempel forteller informant A følgende: *«Vi kan ikke si noe mer til de ansatte enn: Forventer du denne mailen? Er det noe som skurrer? Ta en ekstra sjekk, send et ekstra spørsmål eller en ekstra mail»*. Ekspertene sier også at de ønsker informasjon om hva ansatte får samtidig som ansatte oppfordres til å slette slike mailer. De fleste ansatte sender kun mail videre til IT-teamet hvis det er noe eksepsjonelt ved den. Altså hvis ansatte ser at det er et godt utført svindelforsøk og en mail mange kan lures av. Tidligere har selskapet hatt et system i Outlook med en knapp hvor ansatte kan melde fra om slike mailer. Denne knappen mangler de for tiden da selskapet er på vei vekk fra IT-teknologien som ble brukt før fusjonen. I spørreundersøkelsen rapporterer flere ansatte at de savner denne knappen.

Ellers sier ekspertene at ansatte vet at de ikke skal åpne vedlegg ukritisk. Informant A forteller blant annet at: «Ellers, når det gjelder phishing mail.. det er bare å delete. De vet det nå, vi har lært dem det.» Senere i intervjuet sier samme informant at:

> *«Hos oss er det ikke sånn at du skal være forsiktig når du trykker på noe, du har faktisk ikke lov å trykke på noe som du ikke har eksplisitt spurt etter. Du skal hverken åpne vedlegg eller linker som du ikke har spurt etter eller forventer å få».*

Informant B legger til følgende om temaet: *«I teorien skal ingen åpne et vedlegg uten videre».* Ekspert C mener at folk i deres bransje er utdannet og informert om temaet og at risikoen derfor er mindre for at folk skal gå på forsøkene.

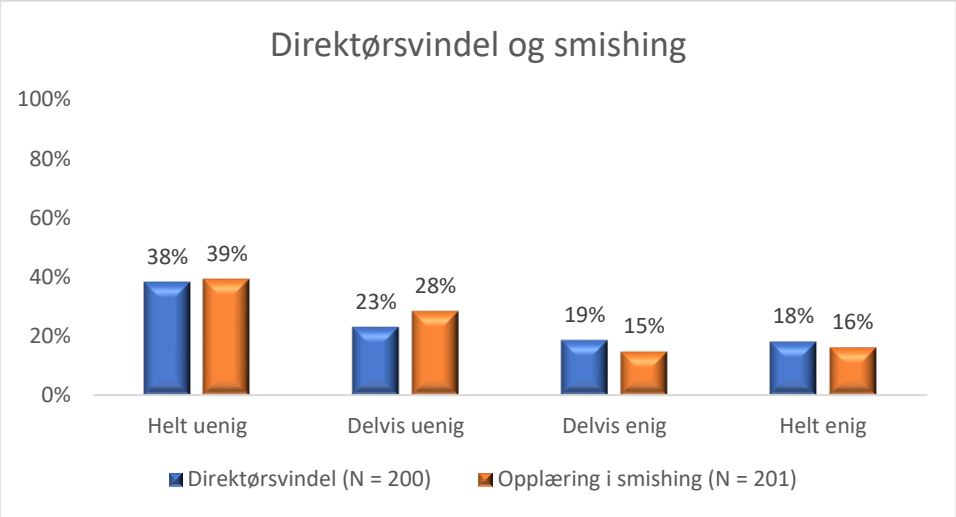
I spørreundersøkelsen ble de ansatte spurt om de har blitt utsatt for svindelforsøk i jobbsammenheng de siste 12 månedene. Figur 5-9 viser at 37% av respondentene svarte ja og 62% svarte nei. I og med at ekspertene forteller at selskapet blir forsøkt svindlet hver dag er det overraskende at såpass mange av de ansatte har svart nei på denne påstanden.



Figur 5-9: Jeg har blitt utsatt for svindelforsøk de siste 12 månedene i jobbsammenheng (ikke som en test/prøve fra IT).

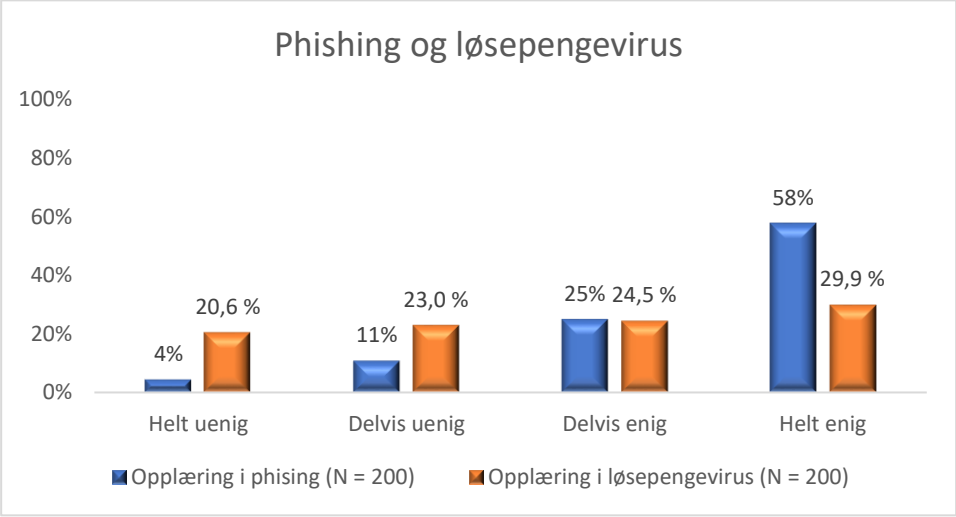
Samtidig viser Figur 5-10 at 38% er helt uenige i at de har lært hva direktørsvindel er og 23% er delvis uenige i denne påstanden. Når det kommer til smishing er 39% helt uenige og 28% er delvis uenige i at de har mottatt opplæring i det. Resultatene fra undersøkelsen tyder på at ansatte ikke er sikre på disse to svindelmetodene. Med tanke på at direktørsvindel er en av de

vanligste svindelmetodene selskapet utsettes for er det et interessant gap at så mange ansatte mener de ikke har mottatt opplæring i denne typen svindel.



Figur 5-10: Jeg har fått opplæring i hva direktørsvindel er. Jeg har fått opplæring i hva smishing er.

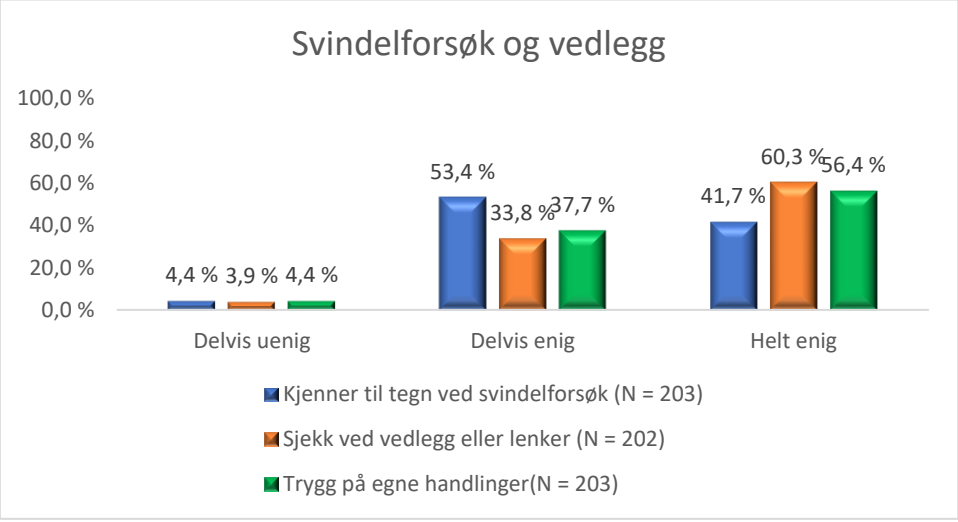
Figur 5-11 viser at 30% er helt enige i at de har fått opplæring i løsepengevirus og 25% er delvis enige. Samtidig har 43% valgt et alternativ hvor de er uenige i at de har mottatt opplæring i denne svindeltypen. Ekspertene forteller at løsepengevirus ikke er så vanlig lenger og dette kan være en forklaring på at få ansatte mener de har mottatt opplæring i det. Phishing er den svindelmetoden de ansatte er mest enige i å ha fått opplæring i da 58% er helt enige i denne påstanden og 25% er delvis enige.



Figur 5-11: Jeg har fått opplæring i hva phishing er. Jeg har fått opplæring i hva løsepengevirus er.

En mulig forklaring på at flere av respondentene oppgir at de ikke har fått opplæring i de ulike svindelformene kan skyldes at det ikke ble gitt noen introduksjon over hva svindelformene går ut på i spørreundersøkelsen. Dette kan ses som en kritikk til min analyse og samtidig ha slått ut på resultatene av disse påstandene. Likevel var dette en bevisst handling da inntrykket fra intervjuene med ekspertene var at de ansatte hadde fått god opplæring i ulike svindeltyper. Dersom de har fått så god opplæring som inntrykket gir burde de ansatte være klar over hva de ulike svindeltypene betyr. Det skal likevel nevnes at det kan være vanskelig å huske på disse forskjellene.

Figur 5-12 viser at 56% er helt enige i at de føler seg trygge på hva de skal gjøre hvis de mottar noe som ligner et svindelforsøk. Samtidig oppgir 38% av respondentene at de er delvis enige i denne påstanden. Figuren viser også at 60% er helt enige i at de undersøker et vedlegg eller en link før det åpnes. Når de ansatte blir spurt om de vet hvilke tegn de skal se etter for å sjekke om noe de har mottatt kan være et svindelforsøk, er det derimot kun 42% som er helt enige i denne påstanden. Det er altså flere ansatte som oppgir at de er trygge på hva de skal gjøre, og som oppgir at de faktisk gjør dette. Men det vil ha liten effekt for selskapets cybersikkerhet hvis flere ansatte ikke vet hvilke tegn de skal se etter i dette arbeidet. Dette kan være en forklaring på hvorfor flere ansatte blir lurt av testene ekspertene gjennomfører. Det kan samtidig være en forklaring på hvorfor det kun er 31% som oppgir at de har vært utsatt for svindelforsøk de siste 12 månedene (Figur 5-9).



Figur 5-12: Jeg vet hvilke tegn jeg skal se etter for å sjekke om noe jeg mottar kan være et svindelforsøk. Jeg undersøker om et vedlegg eller en lenke er trygg før jeg åpner den. Jeg er trygg på hva jeg skal gjøre hvis jeg mottar noe som ligner et svindelforsøk.

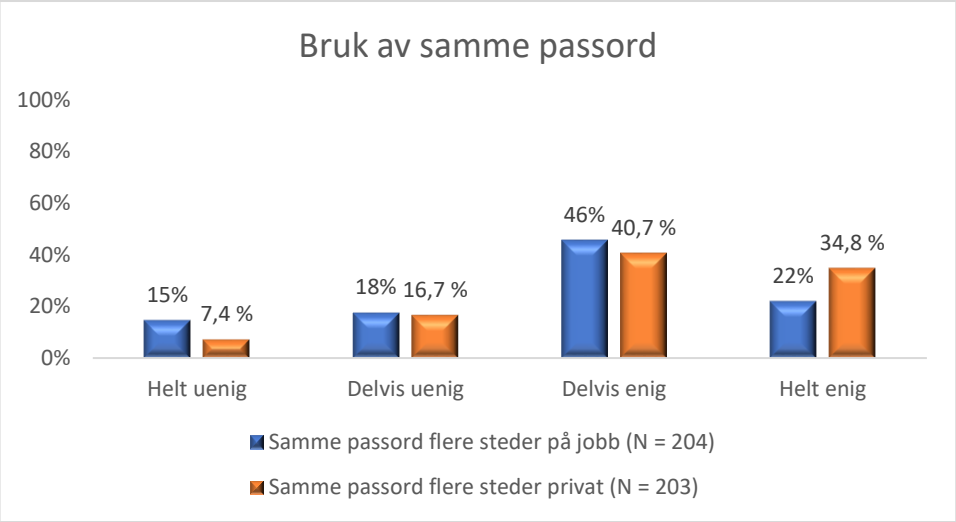
Opplæring i passordbruk

I Wintershall Dea er det vanlig at ekspertene gjennomfører tester og kampanjer rettet mot de ansatte en gang i året. Ved å kjøre slike tester kan de finne ut hva de må fokusere på i opplæringsarbeidet. Informant D forteller om en undersøkelse som ble sendt ut:

> *«Den undersøkelsen avdekket jo at folk blander litt jobb og hjemme, ikke sant. De kan finne på å ha samme passord forskjellige steder, de kan finne på å lagre film og data på onedriven sin privat. De kan gjerne bruke sånn dropbox og verktøy som de ikke har fått fra selskapet. Og de kan gjerne bruke pc-en steder de ikke burde bruke den. Så vi prøver å lære de hvordan».*

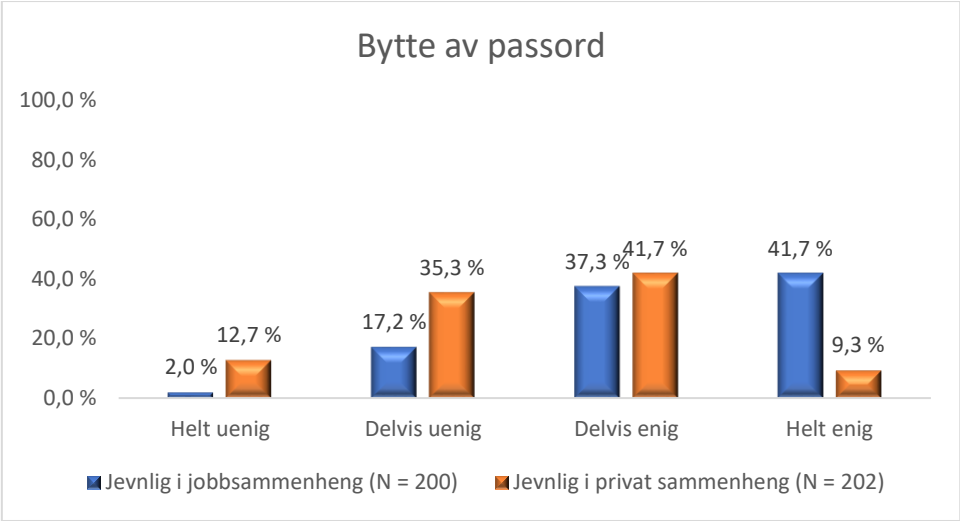
Å lære ansatte til å tenke over passordbruk er viktig for ekspertene. Rapporten *Trusler og trender* fra 2020 viser at kun halvparten av alle nordmenn bruker forskjellige passord for de fleste tjenester på nett, og sier samtidig at det er viktig å bytte på hvilke passord man bruker samt endre passord med jevne mellomrom for å beskytte seg mot cyberangrep (NorSIS, 2020). Det er dermed interessant å undersøke hvordan ansatte i Wintershall Dea ser på bruk av passord. Er det for eksempel slik at ansatte ikke tar med seg cybersikkerhets-tankegangen hjem? I spørreundersøkelsen ble ansatte spurt om de bruker samme passord flere steder i jobbsammenheng.

Figur 5-13 viser at 22% er helt enige i denne påstanden og 46% er delvis enige. På spørsmål om de bruker samme passord flere steder i privat sammenheng er 35% helt enige og 41% er delvis enige.



Figur 5-13: Jeg bruker samme passord flere steder i jobbsammenheng. Jeg bruker samme passord flere steder i privat sammenheng.

De ansatte ble også spurt om de bytter passord med jevne mellomrom i jobbsammenheng. Figur 5-14 viser at 42% er helt enige i denne påstanden og 37% er delvis enige. Kun 9% er helt enige i at de bytter passord med jevne mellomrom i privat sammenheng og 42% er delvis enige.



Figur 5-14: Jeg bytter passord med jevne mellomrom i jobbsammenheng. Jeg bytter passord med jevne mellomrom i privat sammenheng.

Resultatene fra disse fire siste påstandene tyder på at ekspert D har rett i at de ansatte har mer fokus på cybersikkerhet i jobbsammenheng enn de har privat. I tillegg oppgir flere ansatte at de bruker samme passord flere steder både i jobbsammenheng og i privat sammenheng. Dette samsvarer ikke helt med kunnskapen ansatte selv uttrykker at de har om cybersikkerhet. Hva forteller dette? Betyr det at de ikke er klar over hvilken risiko cyberkriminalitet er, selv om de gir uttrykk for at de gjør det? Dette kan knyttes til ansattes subjektive tilstand av sikkerhet i forhold til deres faktiske objektive tilstand av sikkerhet. Den subjektive tilstanden av sikkerhet handler om individers egen følelse av sikkerhet og kan samsvare med objektiv sikkerhet. Men som Zedner (2009) sier, kan den subjektive tilstanden av sikkerhet også være lite relatert til nivået av den objektive sikkerhet. I lys av det de ansatte oppgir i de fire siste påstandene kan det se ut til at deres subjektive følelse av sikkerhet ikke samsvarer med den objektive tilstanden av sikkerhet som handler om det faktiske trusselbildet. Dette fordi forskning (Da Veiga, 2020) viser at ansatte i organisasjoner er den største årsaken til sikkerhetsbrister og samtidig veldig utsatt for å bli offer. Hadde de ansatte vært klar over dette ville kanskje resultatene vist noe annet.

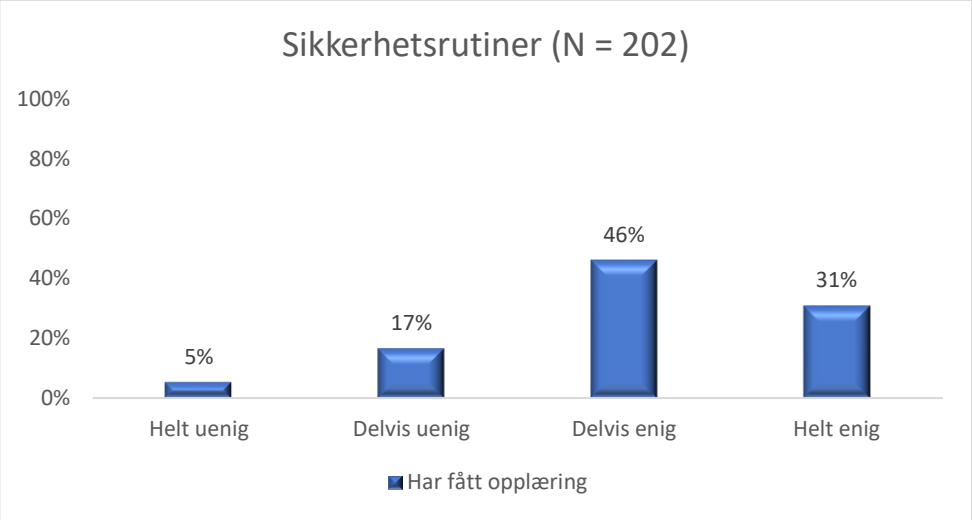
Governmentality- begrepet til Foucault (1991) kan også sies å være relevant med tanke på at en stor del av Wintershall Dea sitt arbeid med cybersikkerhet innebærer å inkludere ansatte til å ta ansvar for sin egen cybersikkerhet. Dette vitner om en tankegang som er lik Garlands (1996) responsibilization strategy som går ut på at staten søker å styre blant annet gjennom å aktivere handlinger fra ikke-statlige byråer og organisasjoner. Med andre ord forsøker staten å overføre ansvaret for forebygging av kriminalitet til organisasjoner og enkeltpersoner, og på denne måten gjøre individer til selv-regulerende individer. Ekspertene i Wintershall Dea forteller at ansatte har et viktig ansvar når det kommer til cybersikkerhet, og at dette er noe de må være med å ta ansvar for. Slik kan det argumenteres for at selskapet ansvarliggjør ansatte i kampen mot digitale sårbarheter. En del av ansvarliggjøringsstrategien innebærer en rekke nye teknikker og metoder hvor staten «søker å få til handling fra private byråer og enkeltpersoner – enten ved å stimulere til nye former for atferd, eller ved å stoppe etablerte vaner» (Riley og Mayhew, 1980: 15 i Garland, 1996). Det kan se ut til at det er dette ekspertene forsøker å gjøre i arbeidet med å lære opp ansatte i cybersikkerhet. Med andre ord kan det se ut til at selskapet driver en ansvarliggjøringsstrategi hvor de ansatte involveres og ror, mens det er selskapet som styrer ved å drive opplæring, sette rutiner og regler samt gjennomføre tester. Denne måten å styre på krever at ansatte tar et aktivt ansvar for egen sikkerhet (Franko, 2020: 171). Å ansvarliggjøre samfunnsborgere er også en del av strategien til myndighetene i kampen mot digitale

sårbarheter. Ett av delmålene til regjeringen er blant annet at befolkningen skal ha «en god digital dømmekraft og god sikkerhetskultur» (Departementene, 2019: 13).

Ansattes opplevelse av opplæring

Det er tydelig at ekspertene i Wintershall Dea legger ned mye arbeid og gjør mye forskjellig for å lære opp ansatte til å tenke på cybersikkerhet. Det er derfor interessant å undersøke hvordan ansatte ser på denne opplæringen, for eksempel om ansatte uttrykker at de har fått opplæring i selskapets sikkerhetsrutiner.

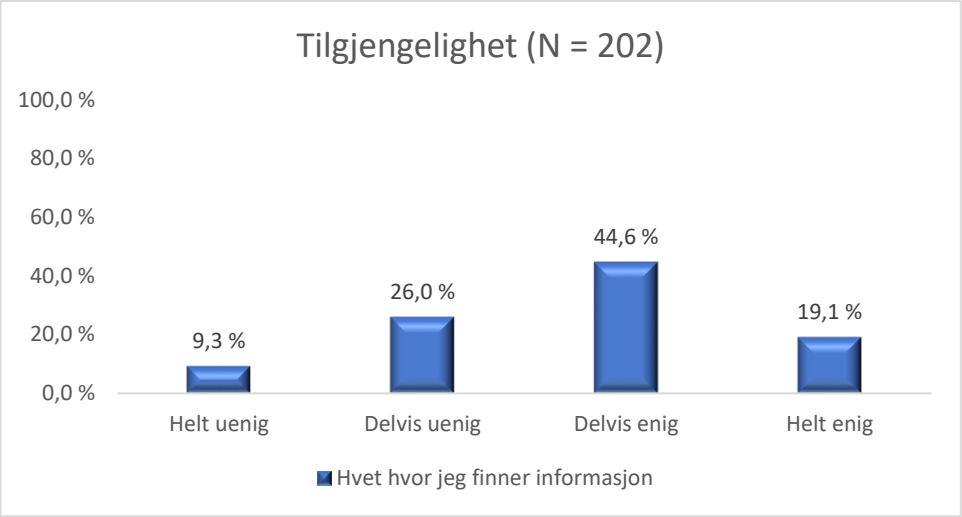
Figur 5-15 viser at kun 31% av respondentene er helt enige i denne påstanden, mens 46% er delvis enige. Resultatene viser dermed at 77% av respondentene har valgt et alternativ hvor de er enige i at de har fått opplæring, og samsvarer slik med det ekspertene uttrykker. Når det gjelder respondentene som har valgt et alternativ for uenig kan en mulig forklaring på dette være at disse er ganske nye i selskapet. Som tidligere vist (Figur 4-3) har 21% av respondentene jobbet i selskapet mellom ett og tre år.



Figur 5-15: Jeg har fått opplæring i selskapets sikkerhetsrutiner når det gjelder cybersikkerhet.

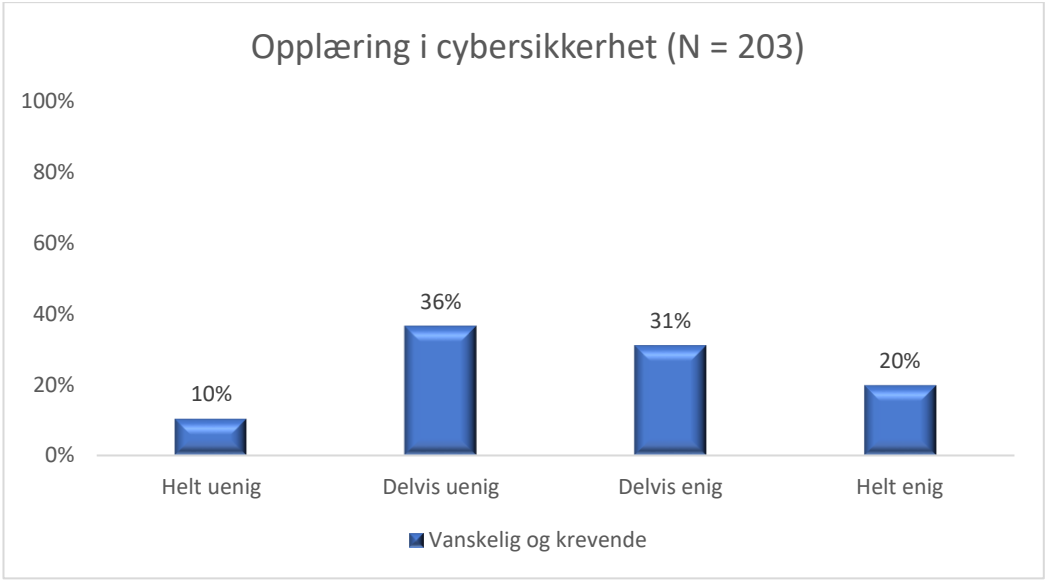
Det er også viktig at ansatte vet hvor informasjon om IT-sikkerhet på jobb er tilgjengelig hvis de ønsker å lære mer eller oppdatere seg. Ekspertene uttrykker at ansatte også må ta ansvar og del i arbeidet med cybersikkerhet, både til seg selv og selskapet. Det er derfor interessant å undersøke om ansatte faktisk vet hvor informasjon og oppdatering er tilgjengelig.

Figur 5-16 viser at kun 19% av respondentene er helt enige i denne påstanden.



Figur 5-16: *Jeg vet hvor informasjon om IT-sikkerhet på jobb er tilgjengelig hvis jeg ønsker å lære mer eller oppdatere meg.*

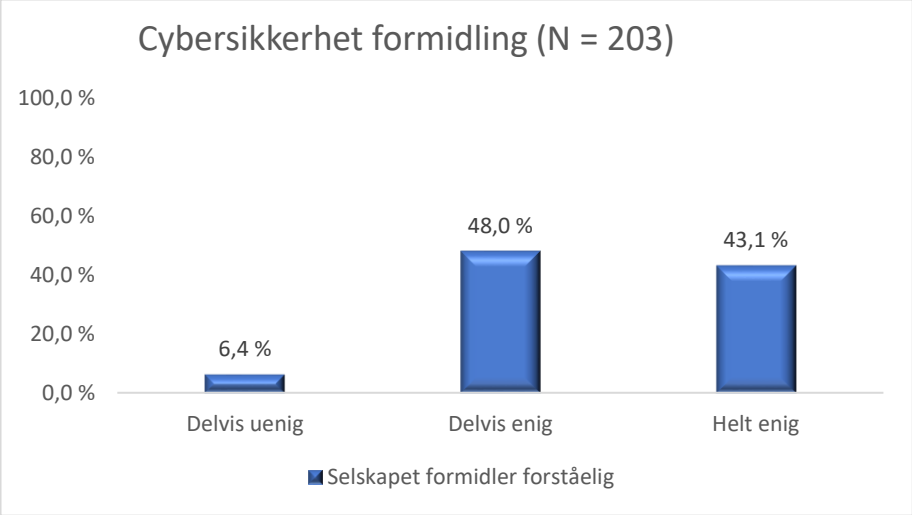
Når det kommer til opplæring i cybersikkerhet er det rimelig å anta at ansatte i organisasjoner må oppleve dette som hensiktsmessig for å handle etter de regler og prosedyrer som selskaper legger opp til. I spørreundersøkelsen ble ansatte derfor spurt om de synes at opplæring i cybersikkerhet er vanskelig og krevende. Figur 5-17 viser at 20% av respondentene er helt enige i denne påstanden og 31% er delvis enige. Dette kan tyde på at selskapet har litt å gå på når det gjelder måten de driver opplæring på.



Figur 5-17: Opplæring i cybersikkerhet er vanskelig og krevende.

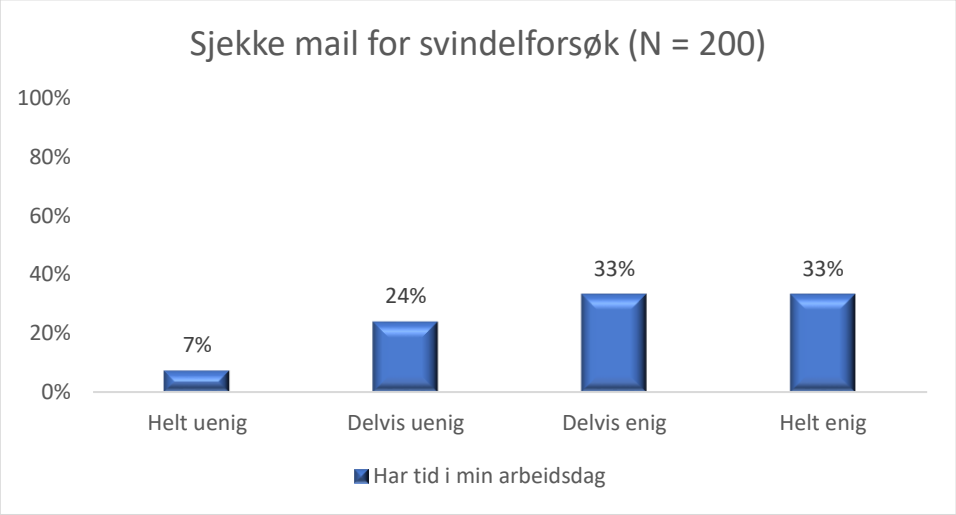
Ekspertene gir inntrykk av at de ansatte vet de ikke skal trykke på usikre linker, og resultatene fra spørreundersøkelsen tyder på at ansatte vet hva de skal gjøre når de får mail de tror kan være svindel, og også hvem de skal kontakte. Likevel forteller ekspert B at 50% trykket på linken i den ene SMS-kampanjen. Det samsvarer ikke helt med informasjonen fra intervjuene og spørreundersøkelsen. En mulig forklaring er at de som har svart på avhandlingens spørreundersøkelse er de som faktisk har kontroll på cybersikkerhet, og at de som ikke har svart er de som kan bli lurt av slike tester. Videre vil andre mulighet forklaringer på dette gapet undersøkes.

Kan det skyldes at opplæringen foregår på et språk som er vanskelig for ansatte å forstå? I spørreundersøkelsen ble ansatte spurt om de synes selskapet formidler kunnskap om cybersikkerhet på en forståelig måte. Figur 5-18 viser at 43% er helt enige i denne påstanden. Det tyder altså på at flere ansatte opplever formidlingen som god. Likevel er 48% delvis enige i påstanden, så kanskje kan det være noe med formidlingen som kan forklare hvorfor flere går på slike tester eller ikke gjør som de skal.



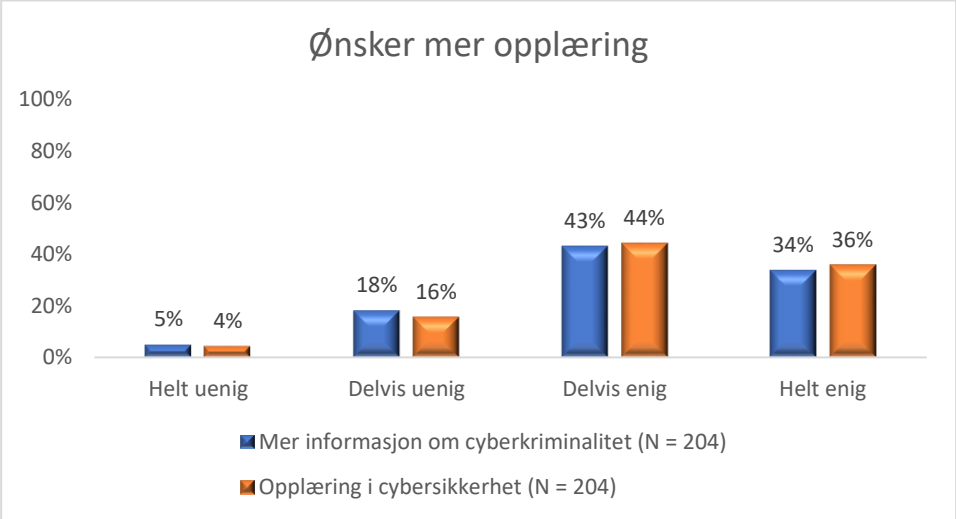
Figur 5-18: Selskapet formidler kunnskap om cybersikkerhet på en forståelig måte.

Ansatte kan ha travle arbeidsdager og en kan derfor også spørre seg om ansatte går på slike tester fordi de ikke har tid i arbeidsdagen til å sjekke ting de mottar grundig nok. I spørreundersøkelsen ble ansatte spurt om de opplever at de har tid til å sjekke mail og lignende for svindelforsøk i løpet av arbeidsdagen. Figur 5-19 viser at 33% er helt enige i denne påstanden og 33% er delvis enige. Som figuren viser er 24% delvis uenige og 7% er helt uenige. Utfordringen med tidspress kan belyse at noe av forklaringen kan ha noe med dette å gjøre.



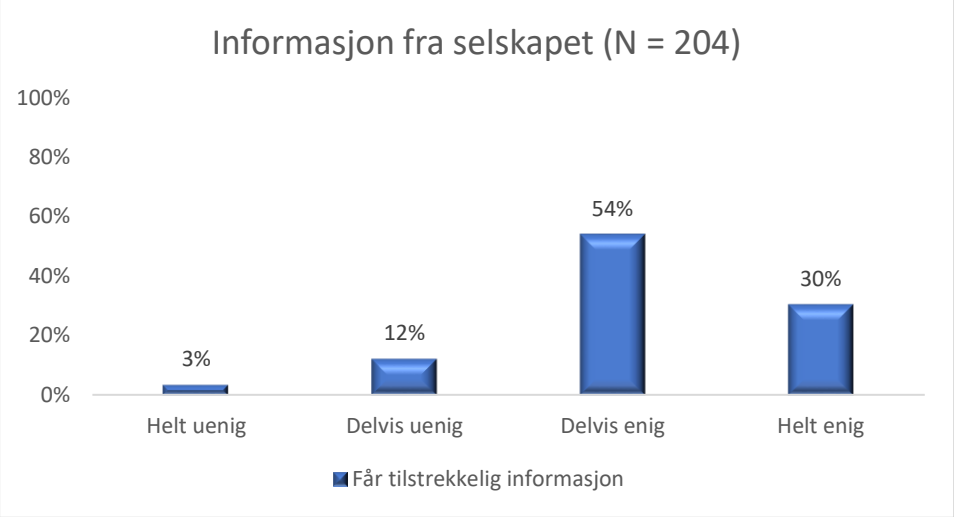
Figur 5-19: Jeg opplever at jeg har tid i min arbeidsdag til å sjekke mail og lignende for svindelforsøk.

Kan noe av forklaringen ligge i metodene for opplæring – at disse ikke oppleves tilstrekkelige for de ansatte? Funnene kan indikere det, men samtidig viser spørreundersøkelsen at 36% er helt enige i at de ønsker mer opplæring i cybersikkerhet, og 44% er delvis enige i denne påstanden (Figur 5-20). I tillegg er 34% av respondentene helt enige i at de ønsker mer informasjon om cyberkriminalitet og de trusler det medfører og 43% er delvis enige i denne påstanden.



Figur 5-20: Jeg ønsker mer informasjon om cyberkriminalitet og de trusler det medfører. Jeg ønsker mer opplæring i cybersikkerhet fra selskapet.

Det kan tyde på at flere ansatte i Wintershall Dea faktisk er åpne for mer opplæring enn det de får i dag. Likevel viser Figur 5-21 at 30% av respondentene er helt enige i at de får tilstrekkelig informasjon fra selskapet om de truslene som finnes på internett, og 54% er delvis enige.



Figur 5-21: Jeg synes jeg får tilstrekkelig informasjon fra selskapet om de truslene som finnes på internett.

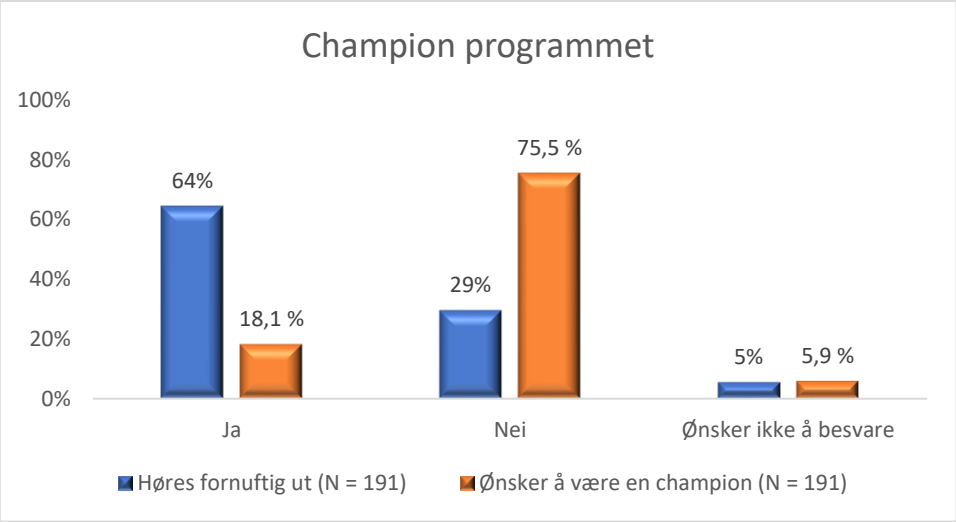
Det er rimelig å anta at ansatte må ha en viss interesse for cybersikkerhet for å ønske mer opplæring. Malmedal og Røislien (2016: 80) finner i sin studie av den norske cybersikkerhetskulturen at det er en sterk sammenheng mellom interesse for teknologi og IKT og god cybersikkerhetspraksis.

5.2.3 Champion program

Forskning viser at en SETA-tilnærming til cybersikkerhetskultur er viktig for å beskytte seg mot dataangrep (Alshaikh, 2020). Samtidig viser forskning at en slik tilnærming nødvendigvis ikke er nok for en god sikkerhetskultur. En SETA- tilnærming bør være på plass, men andre initiativer bør også settes inn. Hvordan organisasjoner kan implementere praksiser for å utvikle en god sikkerhetskultur finnes det derimot lite forskning på (Alshaikh, 2020). For å undersøke dette har Alshaikh identifisert fem viktige initiativer som tre australske organisasjoner har implementert i sine informasjonssikkerhetskulturer for å påvirke og endre ansattes atferd. Disse tiltakene er: 1) å identifisere viktige cybersikkerhetsoppførsler, 2) å etablere et nettverk med «champions», 3) å utvikle et «brand» for cyberteamet, 4) å bygge et cybersikkerhetsnettvek og 5) å tilpasse sikkerhetsbevissthet med interne og eksterne kampanjer. I denne oppgaven har jeg valgt å undersøke tiltaket om å etablere et nettverk med champions. Forskning viser at et slikt

tiltak passer godt til store selskaper som Wintershall Dea, hvor det kan være vanskelig for IT-teamet å alene nå ut til alle ansatte og slik bygge en god sikkerhetskultur (Alsaikh, 2020). Programmet går ut på at enkelte ansatte i virksomheter, såkalte champions, får opplæring og trening i sikkerhet. En champion vil representere sikkerhet i sin avdeling, og vil være tilgjengelig for andre i sin avdeling dersom de har spørsmål om cybersikkerhet. Slik kan de ansatte gå til avdelingens champion i stedet for å kontakte IT-avdelingen. Studien til Alsaikh (2020) konkluderer med at et champion program kan ha svært god effekt for sikkerhetskulturen til et selskap. I de tre organisasjonene som hadde innført et slikt program viste deg seg at etableringen blant annet har spilt en viktig rolle i å støtte cybersikkerhetsteamene i de ulike organisasjonene med å bygge en sikkerhetskultur. I tillegg har championene hjulpet cybersikkerhetsteamene med å identifisere kunnskapsmangel hos ansatte i sine avdelinger, blant annet fordi championene har bedre kunnskap og innsikt i disse. Det viste seg også at championene var enkle å nå hvis en ansatt trengte hjelp til å for eksempel rapportere en phishing mail. Studien til Alshaikh (2020) viser samtidig at det kan være utfordrende å implementere et slikt program med tanke på tilgjengeligheten av ressurser. Det krever blant annet betydelig ekspertise, tid, krefter og finansiering. Det skal også nevnes at undersøkelsen til Alshaikh ble gjort av australske selskaper, og derfor ikke nødvendigvis er overførbart til norske selskaper. Et slikt initiativ kan også ses som en styringslogikk hvor ansatte inkluderes til å ta del i og ansvar for sin egen og selskapets cybersikkerhet og kan slik knyttes til mentaliteten i responsibilization begrepet.

I spørreundersøkelsen ble ansatte informert om et slikt initiativ, og spurt om de synses det høres fornuftig ut. Figur 5-22 viser at 64% av respondentene svarte ja på dette spørsmålet og 29% svarte nei. 5% av respondentene har valgt alternativet *ønsker ikke å svare*, og utgjør 12 av 193 respondenter. I tillegg er det to personer som ikke har svart på spørsmålet. På spørsmål om den ansatte kunne tenke seg å være en champion selv er det derimot 75% som svarer nei. Dette er det spørsmålet i undersøkelsen hvor flest ansatte har valgt alternativet *ønsker ikke å besvare*, med 6%, som utgjør 12 av 192 respondenter. I tillegg er det en person som ikke har svart.



Figur 5-22: Jeg synes champion-programmet høres fornuftig ut. Jeg kunne tenkt meg å være en champion.

Resultatene tyder altså på at flertallet av respondentene synes champion programmet høres ut som en god ide, men svært få ønsker å ha denne rollen selv. Hva kan dette skyldes? I slutten av spørreundersøkelsen ble ansatte spurt om de har noen tanker eller innspill til cybersikkerhet og fikk muligheten til å svare i en tekstboks. Her har flere forklart hvorfor de mener at champion programmet ikke er fornuftig og/eller hvorfor de ikke ønsker å være en champion selv. En del av kommentarene som går igjen er at det er IT-teamet som er ekspertene på dette feltet og derfor dem som burde ta seg av cybersikkerheten til selskapet. Følgende presenteres noen eksempler på utsagn fra ansatte som er beskrivende for flere tekstsvar:

> *«I can't really see the benefit of a champion, what is the problem with contacting IT, the "real" experts?».*
>
> *«Champion-posisjoner fylles ofte av liksom-eksperter. Assistanse for cybersikkerhet bør ivaretas av profesjonelle».*
>
> *"I think we should keep the competence where it belongs".*
>
> *"Jeg tror ikke championer kommer på høyt nok kompetanse nivå i alle avdelinger/lag. Dette må gå gjennom IT kyndig personell".*
>
> *«Let the experts do expert stuff!».*

Det synes å være en oppfatning blant de ansatte om hva som er «ekte» ekspertise. Med andre ord virker det som at ansatte gjør vurderinger av kvaliteten på ekspertisen.

5.2.4 Oppsummerende drøfting av del to

Del to av analysen har sett på hvilke konsekvenser ansattes syn på cybersikkerhet har for det forebyggende arbeidet til ekspertene. I tillegg er det undersøkt hvordan ekspertene jobber med å forebygge cyberkriminalitet samt deres og ansattes opplevelse av arbeidet.

Det er tydelig at ekspertene anvender en barrieretankegang for å sikre seg mot dataangrep. Det forebyggende arbeidet er i tillegg sterkt koblet til risikomentaliteten innenfor nodal governance perspektivet ettersom ekspertene har et proaktivt syn og en fremtidsrettet tankegang til dette arbeidet. Videre er et interessant funn at ekspertene skiller mellom tekniske og menneskelige barrierer. De tekniske barrierene handler om de ulike rammeverkene og verktøyene selskapet anvender for å beskytte seg. For eksempel settes det inn antivirusprogrammer samt programvarer som skal identifisere løsepengevirus. Slike barrierer endrer utformingen av produktene og systemene som brukes og kan slik kobles til perspektivet om situasjonell kriminalitetsforebygging. Ekspertene uttrykker at de tekniske barrierene er viktige for selskapet og disse har vært et fokus i flere år.

Det er derimot tydelig at det største fokuset for ekspertene er de menneskelige barrierene. Dette forstås i sammenheng med at cyberkriminelle de siste årene har rettet søkelyset mot mennesker istedenfor maskiner (NSR, 2020) og det faktum at den menneskelige faktor er en større sårbarhet enn noensinne (NorSIS, 2020). Menneskelige barrierer handler om det forebyggende arbeidet ekspertene driver med rettet mot de ansatte, og hvilke logikker og mentaliteter de anvender i dette arbeidet. Ekspertene uttrykker at ansatte er selskapets første barriere mot cyberangrep og i denne sammenheng ses ansatte som «det svakeste punkt». Det gjør det klart hvorfor ekspertene bruker mye tid på å gjøre ansatte bevisst over hvilken rolle de spiller og hvilket ansvar de har i kampen mot cyberangrep. Denne ansvarliggjøringen av ansatte kan videre knyttes til Garlands (1996) ansvarliggjøringsstrategi som går ut på at staten i første omgang fordeler ansvaret for kriminalitetskontroll utover i samfunnet, for eksempel til virksomheter, som videre aktiverer handlinger for å forebygge kriminalitet.

Ekspertene anvender ulike teknikker og metoder i arbeidet med å ansvarliggjøre de ansatte. Å skape en god sikkerhetskultur forstås som en av teknikkene i dette arbeidet. De uttrykkes at

dette er viktig for å forebygge cyberangrep, og det er spesielt de fire faktorer tillit, dialog, ledelse og opplæring som trekkes frem i en slik kultur. Det ble derfor undersøkt hvordan ansatte opplever disse faktorene som videre kan være en indikator for hvordan de anser sikkerhetskulturen i selskapet. Resultatene fra spørreundersøkelsen indikerer at flesteparten av respondentene har tillit til selskapets kunnskap om cyberkriminalitet. Det er rimelig å anta at en slik tillit er viktig for at ansatte skal etterfølge regler for cybersikkerhet. Resultatene tyder også på at flesteparten av de ansatte opplever at det er god dialog mellom dem og ekspertene. Dette indikerer at ekspertene har oppnådd ønsket om en god tillit og kommunikasjon. Likevel er det flere respondenter som har valgt alternativet delvis enig når det kommer til om det er ubehagelig å oppsøke hjelp fra IT-avdelingen. Dette indikerer at det er noe som oppleves som ubehagelig i dialogen med ekspertene. Ubehag ved å søke hjelp kan videre føre til at ansatte ikke sier fra ved brudd på IKT-regler, noe som er viktig for at angrep skal oppdages. Resultatene indikerer at det også her er ansatte som opplever ubehag. Enda flere oppgir at det er ubehagelig å si fra om kollegers brudd på IKT-regler. En forklaring på at ansatte ikke gir beskjed om IKT-brudd kan være at de ikke vet hvem som skal kontaktes eller hva de skal gjøre om noe som avviker fra normalen skjer. Resultatene tyder derimot på at flertallet både vet hvem som skal varsles og hva som skal gjøres.

Ledelsen i selskapet trekkes også frem av ekspertene som svært viktig for en god sikkerhetskultur. Videre forstår ekspertene ledelsen som sentral for å få ansatte til å forstå at cybersikkerhet er viktig. Det synes som at både ledelse og tillit må ligge i bunn for at opplæringsarbeidet skal fungere ideelt. Ekspertene legger ned mye arbeid i å lære opp ansatte i cybersikkerhet. Blant annet gjennomfører de kampanjer, holder presentasjoner, tester ansattes villighet til å klikke på usikre linker og tilbyr filmer som tar for seg cybersikkerhet. I tillegg gjennomføres det hvert år en Safety-Day hvor IT-teamet viser eksempler, for eksempel hvor lett det er å hacke seg inn på telefoner. Ekspertene opplever at ansatte tar godt i mot denne opplæringen. Det ble derfor undersøkt hva de ansatte uttrykker om opplæring i svindelforsøk, passordbrud og opplæring generelt.

Når det kommer til opplæring i svindelforsøk viser resultatene at flertallet av de ansatte mener de ikke har vært utsatt for svindelforsøk de siste 12 månedene. Dette er et interessant funn med tanke på at ekspertene forteller at selskapet blir forsøkt svindlet hver dag. Det ble videre undersøkt om ansatte opplever å ha mottatt opplæring i noen av de vanligste svindelforsøkene som er direktørsvindel, smishing, løsepengevirus og phishing. Resultatene indikerer at

flesteparten uttrykker å ikke ha mottatt opplæring i direktørsvindel og smishing. Litt over halvparten har valgt et alternativ med enig i når det kommer til å ha mottatt opplæring i løsepengevirus. Phishing er den svindelmetoden flest ansatte oppgir å ha mottatt opplæring i. Når det kommer til opplæring i direktørsvindel, smishing og løsepengevirus er det likevel en ganske lav prosent som oppgir å ha mottatt dette. Dette står i kontrast til det ekspertene har fortalt om at ansatte har fått god opplæring i svindelforsøk. Videre tyder resultatene på at flertallet er trygge på hva de skal gjøre hvis de mottar noe som ligner et svindelforsøk. Enda flere oppgir at de faktisk undersøker om et vedlegg eller en lenke er trygg før den åpnes. Likevel oppgir under halvparten av respondentene at de vet hvilke tegn de skal se etter for å sjekke om noe de mottar kan være et svindelforsøk. Dette er et veldig interessant funn. Det vil ha liten hensikt for selskapets cybersikkerhet hvis flertallet ikke vet hva de skal se etter.

Sikker passordbruk er et viktig sikkerhetstiltak for å forebygge cyberangrep. Resultatene fra spørreundersøkelsen viser at over halvparten av de ansatte har valgt et alternativ med enig i når det kommer til bruk av samme passord flere steder i jobbsammenheng. Enda flere oppgir at de bruker samme passord i privat sammenheng. Kun halvparten oppgir at de bytter passord med jevne mellomrom i privat sammenheng. Det er derimot godt over halvparten som oppgir at de bytter passord med jevne mellomrom i jobbsammenheng. Dette indikerer at ekspertene har rett i at ansatte opplever å ha mer fokus på cybersikkerhet i jobbsammenheng.

Som tidligere nevnt uttrykker ekspertene at ansatte tar godt i mot opplæringen. Det ble derfor undersøkt hva ansatte tenker om dette. Resultatene viser at under halvparten mener de har fått oppæring i selskapets sikkerhetsrutiner når det gjelder cybersikkerhet. Likevel har godt over halvparten valgt et alternativ med enig i og indikerer at flesteparten mener å ha mottatt slik opplæring. Slik samsvarer denne informasjonen med det ekspertene uttrykker. På den andre siden er det få som oppgir at de vet hvor informasjon om IT-sikkerhet er tilgjengelig, og halvparten oppgir at opplæring i cybersikkerhet er vanskelig.

Ekspertene forteller at flere ansatte blir lurt av testene som gjennomføres. I den sammenheng ble det undersøkt om ekspertenes formidling av cybersikkerhet kan være en forklaring på dette. Resultatene indikerer derimot at ansatte er fornøyd med måten kunnskap om cybersikkerhet formidles på. Likevel har nesten halvparten valgt alternativet delvis enig i denne påstanden og indikerer at ikke alle er fornøyd med hvordan selskapet formidler kunnskap om cybersikkerhet.

Resultatene tyder også på at tidspress i arbeidsdagen kan forklare hvorfor ansatte blir lurt av ekspertenes tester.

Påstandene som er gått igjennom kan indikere at ekspertenes metoder for å drive opplæring ikke oppleves som tilstrekkelige for de ansatte og kan videre forklare hvorfor flere blir lurt av tester. Likevel viser resultatene at flesteparten ønsker mer opplæring i samt mer informasjon om cybersikkerhet. På den ene siden tyder dette på at ansatte er mottakelige for mer opplæring. Dette står i kontrast til utsagn fra ekspertene om at de ikke kan drive med for mye opplæring. På den andre siden oppgir godt over halvparten av de ansatte at de får tilstrekkelig informasjon fra selskapet om de trusler som finnes på internett. Til slutt ble det undersøkt hva de ansatte tenker om å innføre et champion program i selskapet. Her viser resultatene at over halvparten synes dette høres fornuftig ut. Likevel oppgir flere at de ikke kunne tenke seg å være en champion. Flere forklarer dette med at det er IT-teamet som er ekspertene på cybersikkerhet og at ansatte ikke vil kunne gjennomføre en slik jobb på en tilstrekkelig måte. Det tyder dermed på at flesteparten av de ansatte har stor tiltro til ekspertene og deres arbeid.

6 Diskusjon og avslutning

Denne oppgaven har sett på hvordan det norske gass-og oljeselskapet Wintershall Dea strategisk arbeider med forebygging av cyberangrep, samt hvilke opplevelser og forståelser ansatte har av arbeidet. Den eksisterende forskningslitteraturen og de empiriske funnene presentert i denne oppgaven illustrerer at cyberkriminalitet er et komplekst fenomen, og en stadig voksende trussel i det moderne samfunnet for både myndigheter, organisasjoner og individer. Samfunnet, økonomien og mye kritisk infrastruktur har i stor grad blitt avhengig av nettverksstrukturer og IKT-løsninger. Internetts utvikling har derimot ført til at cyberangrep har blitt en dagligdags forekomst (Renaud mfl., 2020), som kan føre til store konsekvenser for alle berørte. For å bekjempe cyberkriminalitet har cybersikkerhet vokst frem på sikkerhetsagendaen og fått et stort fokus, både i forskningslitteraturen og i den offentlige debatten.

Basert på oppgavens empiri og teori kan informantenes forståelse av cyberkriminalitet og arbeid med cybersikkerhet forstås som *et spill i kontinuerlig utvikling*. De empiriske funnene illustrerer at arbeid med cybersikkerhet er et komplekst fenomen som aldri tar slutt. Som en konsekvens av risikoene og truslene cyberkriminalitet bringer med seg synes det å ha vokst frem et spenningsforhold mellom sikringssiden på den ene siden og trusselsiden på den andre siden. Aktører som jobber med cybersikkerhet må stadig utvikle seg for å håndtere og bekjempe denne typen kriminalitet, og slik konstant jakte etter sikkerhet (Zedner, 2009). Samtidig er det en eksponentiell vekst i den digitale sfæren, hvor internett utvikler seg dag for dag, og gir potensielle lovbrytere stadig nye muligheter til å begå cyberkriminalitet. Følgelig blir det et form for kappløp mellom de som ønsker å sikre seg og de som ønsker å utføre cyberangrep. Dette spillet synes å være vanskelig med tanke på risikologikken, som i stor grad er fundert på instrumentelle kalkuleringer, og at man alltid skal være i forkant av truslene. I tillegg kompliseres spillet ettersom det er snakk om å være i forkant av ukjente trusler da man på grunn av internettets stadige utvikling aldri kan vite hvilken trussel man står ovenfor.

Denne konstante jakten etter sikkerhet, som følge av et spill i kontinuerlig utvikling, gjør det særlig interessant å undersøke hvordan aktører tenker om og erfarer cyberkriminalitet og cybersikkerhet i deres praksis, og særlig hvordan disse utfordringene kan imøtekommes. Analysen i denne oppgaven viser at regjeringens strategi for digital sikkerhet (Departementene, 2019) synes å trekke på mentalitetene og logikkene slik de er skissert innen teorien til Foucault om governmentality, ansvarliggjøringsstrategien til Garland samt perspektivet om nodal

governance. For å sikre våre digitale verdier og produsere sikkerhet ser myndighetene ut til å styre cyberkriminalitet på avstand. De har fremdeles en viktig rolle i dette arbeidet, blant annet ved å komme med retningslinjer og initiere til opprettholdelse av disse, men gjennomføringen ser derimot ut til å overlates til samfunnsmedlemmer. Flere aktører trekkes inn i dette arbeidet, både organisasjoner og individer, og slik ansvarliggjøres samfunnsmedlemmer i kampen mot cyberkriminalitet.

Wintershall Dea sitt arbeid med forebygging av cyberangrep kan også kobles til governmentality, ansvarliggjøringsstrategien og nodal governance. Selskapet synes å styre direkte gjennom implementering av ulike tiltak, men også indirekte ved å ansvarliggjøre ansatte. På samme måte som myndighetene ansvarliggjør selskapet, ansvarliggjør selskapet sine ansatte. Dette kan blant annet ses ved at selskapet har et stort fokus på forebygging, med både en teknisk og menneskelig barrieretankegang. På den tekniske siden settes det inn ulike barrierer og situasjonelle kriminalitetsforebyggende tiltak som for eksempel brannmurer og antivirusprogrammer. Når det gjelder den menneskelige siden er det et stort fokus på å få ansatte til å forstå viktigheten av cybersikkerhet, og det synes derfor å være avgjørende å skape en bevissthet blant de ansatte. Menneskelige barrierer anses som svært viktige og ansatte ses på som selskapets første barriere mot cyberangrep. Det ser dermed ut til at selskapet er bevisst på at cyberkriminelle de siste årene har rettet angrepene sine mot enkeltpersoner istedenfor datamaskiner og nettverk (NSR, 2020: 78). I den forbindelse oppfattes ansatte som «det svakeste punkt» når det kommer til utsatthet for cyberangrep, og det brukes derfor store ressurser på å skape og forbedre de menneskelige barrierene.

Ekspertene som jobber med cybersikkerhet ønsker å få ansatte til å forstå at de er en viktig ressurs for å forebygge cyberangrep. For ekspertene står sikkerhet i fokus og de har et særlig ansvar for cybersikkerheten til selskapet. Samtidig er det et ønske å spre dette ansvaret ut til flere. Det kan være krevende og det synes å være et spenningsforhold mellom ekspertene og respondentene. Ekspertene ser hver dag hvor alvorlig trusselen om cyberangrep er samtidig som de er klar over at menneskelig svikt er den største årsaken til sikkerhetsbrister (Da Veiga, 2020). For at ansatte skal ta trusselen på alvor er det nødvendig at de også forstår alvoret i den. Ekspertene fokuserer på selskapets sikkerhetskultur for å skape en mentalitet og ansvarliggjøring av ansatte. For å få til dette fokuserer de på å implementere en god sikkerhetskultur gjennom faktorene tillit, dialog, ledelse og opplæring. Funnene fra spørreundersøkelsen indikerer at flesteparten opplever at selskapet har en god sikkerhetskultur.

Gjennom å undersøke ansattes opplevelse av ekspertenes arbeid med forebygging av cyberangrep synes det som ekspertene har fått til dette arbeidet i en viss grad, men at det har vært og er krevende å lære opp ansatte i cybersikkerhet. Spørreundersøkelsens funn tyder på at ansatte forstår at cybersikkerhet er viktig og at cyberkriminalitet kan ramme alle. Dermed ser det ut til ansatte forstår risikoen cyberangrep utgjør. Likevel viser funnene at flere ansatte ikke gjør det de bør for å være sikre på nett blant annet ved at de bruker samme passord flere steder, ikke bytter passord jevnlig, og er usikre på hva de skal se etter for å gjenkjenne svindelforsøk. Til tross for at funnene tyder på at flesteparten av de ansatte opplever en god sikkerhetskultur fremkommer det i studien at flere ansatte vegrer seg for å ta kontakt med IT-teamet. Dette kan videre ha konsekvenser for om de rapporterer egne og kollegers brudd og kan igjen føre til uoppdagede angrep. Resultatene viser at flesteparten av de ansatte ikke er interessert i å ta på seg rollen som en champion. Det forklares med at dette arbeidet best gjøres av ekspertene. Det kan likevel indikere at ansatte ikke har forstått hvor alvorlig cyberangrep er.

Å jobbe med cybersikkerhet synes å være et arbeid som aldri tar slutt. Ekspertene må stadig utvikle seg og være oppdatert på cyberkriminalitet for å klare å bekjempe det. Samtidig må de drive konstant opplæring av ansatte slik at de også er oppdatert på trusselbildet og forstår alvorligheten av trusselen. Det er tydelig at cybersikkerhet er et kontinuerlig spill i utvikling mellom sikringssiden på den ene siden og trusselsiden på den andre.

6.1 Videre forskning

Hva betyr cybersikkerhet og dets kontinuerlige spill i utvikling for fremtiden? Ettersom cyberkriminalitet er i stadig utvikling er det tydelig at det er et stort behov for videre forskning på feltet. Dette gjelder både forskning på flere typer bedrifter samt komparativt globalt. I tillegg er det et behov for forskning som bygger på observasjoner og ikke bare det de som arbeider med cybersikkerhet forteller. Denne oppgaven har belyst hvordan ansatte opplever og forstår arbeid med cybersikkerhet basert på selvrapportert atferd. Det vil være nyttig å undersøke faktisk atferd for å få mer kunnskap om ansattes atferd på internett.

Antall ord: 36 603

7 Litteraturliste

Alleyne, B. (2011) "We are all hackers now": Critical sociological reflections on the hacking phenomenon. *Goldsmiths Research online*. Tilgjengelig fra: http://www.arifyildirim.com/ilt510/ brian.alleyne.pdf.

Alohali, mfl. (2018) Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information and Computer Security*, 26(3), s. 306-326.

Alshaikh, M. (2020) Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98(2), s. 1-10.

Arachchilage, N. A. G., og Love, S. (2014) Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, s. 304–312.

Balzacq, T og Cavelty, D. Myriam (2016) A theory of actor-network for cyber-security. *European journal of international security*, 1(2), s. 176-198.

Baruch, Y. og Holtom, B. C. (2008) *Survey response rate levels and trends in organizational research*. London: Sage Publications.

Beck, U. (1992) *Risk society*. London: Sage Publications.

Bereczkei, T., og Birkas, B. (2014) The insightful manipulator: Machiavellians' interpersonal tac- tics may be linked to their superior information processing skills. *International Journal of Psychological Studies*, 6(4), s. 65–70.

Bernaards, F., Monsma, E., og Zinn, P. (2012) High tech crime. *Criminaliteitsbeeldanalyse, 2012*. Rotterdam: Theme Media Center.

Bourbeau, P. (2015) *Security: Dialouge Across Disciplines*. Cambridge: Cambridge University Press.

Boss, S. mfl. (2015) What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), s. 837-864.

Burris, S. (2004). Governance, microgovernance and health. *Temple Law Review*, 77, s. 335-362.

Brewer, R. m.fl., (2019) *Cybercrime Prevention: Theory and Applications*. Palgrave. https://doi.org/10.1007/978-3-030-31069-1

Brodeur, J-P. (2010) The Policing web. Oxford: Oxford University Press.

Cain, A. A., Edwards, M. E., og Still, J. D. (2018) An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 42, s. 36–45.

Caneppele, S., og Aebi, M. F. (2017) Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice,* 13 (1), s. 66-79.

CBS. (2018) *Cybersecuritymonitor 2018.* Den Haag: CBS.

Crossler, R. E. mfl. (2013) Future directions for behavioral information security research. Computers and Security, 32, s. 90–101.

Crossler, R. E. og Bélanger, F. (2014) An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database*, 45(4), s. 51–71.

Crossler, R. E., Bélanger, F., og Ormond, D. (2017) The quest for complete security: An empiri- cal analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 21(2), s. 343–357.

Da Veiga, A. mfl. (2020) Defining organisational information security culture – Perspectives from academia and industry. *Computers & Security*, 92, s. 1-23 (10171).

Departementene (2019) *Nasjonal strategi for digital sårbarhet*. Oslo: Justis- og Beredskapsdepartementet og Forsvarsdepartementet.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007) Behavioral response to phishing risk. I *Proceedings of the anti-phishing working groups – 2nd annual eCrime researchers summit*. New York: ACM Press, s. 37–44.

Dupont, B. (2017) Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, 67, s. 97–116.

Dupont, B., og Whelan, C. (2021) Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, 0(0), s. 1-17.

Engen, O. A. H. mfl. (2016) *Perspektiver på samfunnssikkerhet.* Oslo: Cappelen Damm AS.

Ericson, R.V og Haggerty, K.D (1997) *Policing the risk society*. Oxford: Claredon Press.

Eriksson, Z.U. mfl. (2015) *Organisasjonsteori*. Oslo: Cappelen Damm As.

Europol (2021) *Cybercrime*. Tilgjengelig fra: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime (Hentet: 04. mai 2021).

Farrell, G. (2010) Situational Crime Prevention and Its Discontents: Rational Choice and Harm Reduction versus 'Cultural Criminology'. *Social policy & administration,* 44 (1), s. 40-66.

Faubert, C. mfl. (2021) Law Enforcement and Disruption of Offline and Online Activities: A Review of Contemporary Challenges, i Kranenbarg, M. W. og Leukfeldt, R. (red.) *Cybercrime in Context*. Amsterdam: Springer International Publishing, s. 351 – 370.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000) A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology,* 30(2), s. 407–429.

Foucault, M. (1991) Governmentality, i Burchell, G., Gordon, C., Miller. P (red.) *The Foucault Effect: Studies in Governmentality.* Chicago: Chicago University Press, s. 87-104.

Franko, K. (2020) *Globalization and Crime.* 3.utg. London: Sage Publications.

Garland, D. (1996) The Limits of the Sovereign State. Strategies of Crime Control in Contemporary Society. *The British Journal of Criminology*, 36(4), s. 445-471.

Garland, D. (1997) ´Governmentality´ and the problem of crime: Foucalt, criminology, sociology. *Theoretical criminology*, 1(2), s. 173-214.

Giddens, A. (1997) *Modernitetens konsekvenser*. Oslo: Pax Forlag A/S.

Grabosky, P.N. (2001) Virtual Criminality: Old Wine in New Bottles?. *Social & legal studies*, 10(2), s. 243-249.

Grønmo, S. (2016). *Samfunnsvitenskapelige metoder*. 2. utg. Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Gundhus, H. O. I og Jansen, P. T. (2020) Pre-crime and Policing of Migrants: Anticipatory Action Meets Management of Concerns. *Theoretical criminology*, 24(1), s. 90-109.

Haraldsen, G. (1999) *Spørreskjemametodikk etter kokebokmetoden*. Oslo: Ad Notam Gyldendal.

Harknett, R.J. og Stever, J.A. (2009) The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management,* 6(1), s. 1-14 (793).

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems,* 18(2), s. 106–125.

Holt, T. J. (2018) Regulating cybercrime through law enforcement and industry mechanisms. *TheAnnals of the American Academy of Political and Social Science*, 679(1), s. 140–157.

Hydro (2020) *Cyberangrep på Hydro*. Tilgjengelig fra: https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/ (Hentet: 06. april 2020).

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

Jansen, J., og van Schaik, P. (2017) Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*, 25(2), s. 165–180.

Jansen, J., og Leukfeldt, R. (2018) Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice & Criminology*, 6(2), s. 205–228.

Jansen, J. (2018) *Do you bend or break? Preventing online banking fraud victimization through online resilience.* Doktoravhandling. Enschede: Gildeprint.

Johnston, L., og Shearing, C. (2003) *Governing security: Explorations in policing and justice.* New York: Routledge.

Jones, T. og Newburn, T. (1998) *Private security and public policing*. Oxford: Clarendo Press.

Jones, D. N., og Paulhus, D. L. (2014) Introducing the short dark triad (SD3): A brief measure of dark personality traits. *Assessment*, 21(1), s. 28–41.

Kranenbarg, M. W. (2021) Cyber-dependent Crime Versus Traditional Crime: Empirical Evidence for Clusters of Offenses and Related Motives, i Kranenbarg, M. W. og Leukfeldt, R. (red.) *Cybercrime in Context*. Amsterdam: Springer International Publishing, s. 195-216.

Leukfeldt, R. (2014) Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology Behavior and Social Networking*, 17(8), s. 551–555.

Leukfeldt, R. (2017) *The human factor in cybercrime and cybersecurity*. Haag: Eleven International Publishing.

Loader, I. og Percy, S. (2012). Bringing the 'outside' in and the 'inside' out: crossing the criminology/IR divide. *Global Crime*, 13(4), s. 213-218.

Lysneutvalget (2015) *Digitale Sårbarheter Olje & Gass*. 2015-0462, Rev. 1. Stavanger: Lysneutvalget.

Malmedal, B., og Røislien, H. E. (2016) *The Norwegian Cyber Security Culture.* Gjøvik: NorSIS.

Malmedal, B., og Røislien, H.E. (2019). *Nordmenn og digital sikkerhetskultur 2019*. Gjøvik: NorSIS.

Mark, M.S, Tømte, C.E, Næss, T og Røsdal, T. (2019) Leaving the windows open – økt mangel på IKT-sikkerhetskomeptanse i Norge. *Norsk sosiologisk tidsskrift*, 3(3), s. 173-190.

Martin, J. (2013). Informal security nodes and force capital. *Policing & society*, 23(2), s.145-163.

McGuire, M., & Dowling, S. (2013) *Cyber crime: A review of the evidence. In Summary of key findings and implications.* Home Office Research report 75. London: Home Office.

Michie, S., Van Stralen, M. M., og West, R. (2011) The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*: *IS*, 6(1), s. 1-11 (42).

Muller, L. P. (2016) Makt og avmakt i cyberspace: hvordan styre det digitale rom?. *Internasjonal politikk*, 74(4), s. 1-23.

Nasjonal sikkerhetsmyndighet. (2020) *RISIKO 2020.* Tilgjengelig fra: https://nsm.no/getfile.php/131421-

1587034764/Hermans%20undermappe%20med%20bilder/NSM_Risiko_2020_web_0104.pdf (Hentet: 11. januar 2021).

Nasjonal sikkerhetsmyndighet. (2021) *Sikkerhetskultur*. Tilgjengelig fra: https://nsm.no/fagomrader/sikkerhetsstyring/sikkerhetskultur/ (Hentet: 25. april 2021).

NESH: De nasjonale forskningsetiske komiteene (2016) *Forskningsetiske retningslinjer for samfunnsvitenskap, humanioria, juss og teologi*. 4. utg. Oslo: Oktan Oslo AS.

Neumann, I. (2002) *Forelesninger om regjering og styringskunst*. Oslo: Cappelens forlag.

Neumann, I. B. (2003) Innledning: Regjeringsbegreper og regjeringens historiske fremvekst, i Neumann, I. B og Sending, O. J. (red) *Regjering i Norge.* Oslo: Pax Forlag, s. 9-43.

Nilsen, H. S. og Mjaaland, O. (2018) *Hackerangrep mot bedrifter øker: - De kriminelle har alltid overtaker*, NRK, 20. september. Tilgjengelig fra: https://www.nrk.no/norge/hackerangrep-mot-bedrifter-oker_-_-de-kriminelle-har-alltid-overtaket-1.14214930 (Hentet: 20. februar 2020).

Njie, R. A. (2017) *Kripos advarer: - Stor økning i datakriminalitet*, NRK, 3. april. Tilgjengelig fra: https://www.nrk.no/norge/kripos-advarer_-_-stor-okning-i-datakriminalitet-1.13436174 (Hentet: 20. februar 2020).

Norris, D.F. mfl. (2015) Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. *Public Administration Review*, 79(6), s. 895-904.

NOU 2015: 13. *Digital sårbarhet – sikkert samfunn. Beskytt enkeltmennesker og samfunn i en digitalisert verden.*

Norsk senter for informasjonssikring (2020) *Trusler og Trender 2019-2020*. Gjøvik: NorSIS

Næringslivets sikkerhetsråd (2014) *Mørketallsundersøkelse 2014.*

Næringslivets sikkerhetsråd (2020) *Mørketallsundersøkelsen 2020*.

Nøkleberg, M. (2016) Security Governance – An Empirical Analysis of the Norwegian Context. *Nordisk politiforskning*, 3(1), s. 53-82.

Politiets sikkerhetstjeneste (2021) *Nasjonal trusselvurdering*. Tilgjengelig fra: https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/ntv_2021_final_web_1802-1.pdf (Hentet: 24. april 2021).

PWC (2020) *Fighting fraud: a never ending battle. PwC´s Global Economic Crime and Fraud Survey*. Tilgjengelig fra: https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf (Hentet: 8. april. 2021).

Renaud, K mfl. (2020) Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. *Public Administration Review*, 80 (4), s. 577–589.

Regjeringen (2019) *Digital sikkerhet*. Tilgjengelig fra: https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/digital-sikkerhet/id2340011/ (Hentet: 08. april 2020).

Ringdal, K. (2013) *Enhet og mangfold: samfunnsvitenskapelig forskning og kvantitativ metode*. 3. utg. Bergen: Fagbokforlag.

Rose, N., O´Malley, P. Og Valverde, M. (2006) Governmentality, *Annual review of law and social science*, 2(1), s. 83-104.

Sagberg, I. (2020) *Organisasjonskultur*. *Store norske leksikon*. Tilgjengelig fra: https://snl.no/organisasjonskultur (Hentet: 29. april 2021).

Schearing, C. Og Wood, J. (2003) Nodal governance, democracy, and the new "denizens". *Journal of Law and Society*, 30(3), s. 400-419.

Selzer, N and Sebastian Oelrich, S. (2021) Saint or Satan? Moral Development and Dark Triad Influences on Cybercriminal Intent, i Kranenbarg, M. W. og Leukfeldt, R. (red.) *Cybercrime in Context.* Amsterdam: Springer International Publishing, s. 175-194.

Skilbrei, M. L. (2019) *Kvalitative metoder: planlegging, gjennomføring og etisk refleksjon*. Bergen: Fagbokforlaget.

Stephenson, P., og Walter, R. (2012) Cyber crime assessment. Hawaii International Conference on System Science, 45, s. 5404-5413.

Talib, S., Clarke, N. L., og Furnell, S. M. (2010) An analysis of information security awareness within home and work environments. *ARES 2010 – 5th International Conference on Availability, Reliability, and Security*, s. 196–203.

Thaagard, T. (2013) *Systematikk og innlevelse. En innføring i kvalitativ metode.* Bergen: Fagbokforlaget.

Thaagard, T. (2018) *Systematikk og innlevelse. En innføring i kvalitative metoder*. 5. utg. Bergen: Fagbokforlaget.

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

Tjora, A. (2017) *Kvalitative forskningsmetoder i praksis.* 3. utg. Oslo: Gyldendal akademisk.

Tonry, M. (2014) Why crime rates are falling throughout the Western world. *Crime and justice*, 43, s. 1–64.

Universitetet i Oslo (2021) *Nettskjema-diktafon-appen.* Tilgjengelig fra: https://www.uio.no/tjenester/it/adm-app/nettskjema/hjelp/diktafon.html (Hentet: 6. april 2021)

van de Weijer, S. G. A., Leukfeldt, E. R., & Bernasco, W. (2019) Reporting crime to the police: a comparison between traditional crime and cybercrime. *European Journal of Criminology*, 16(4), s. 486–508.

van de Weijer, Steve G. A., Leukfeldt, R. og van der Zee, S. (2021) Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands, i Kranenbarg, M. W. og Leukfeldt, R. (red.) *Cybercrime in Context*. Amsterdam: Springer International Publishing, s. 303-326.

van der Laan, A. M., og Tollenaar, N. (2021) *Text Mining for Cybercrime in Registrations of the Dutch Police*, i Kranenbarg, M. W. og Leukfeldt, R. (red.) *Cybercrime in Context.* Amsterdam: Springer International Publishing, s. 327-350.

van 't Hoff-de Goede, S. H. mfl. (2021) The Online Behaviour and Victimization Study: The Development of an Experimental Research Instrument for Measuring and Explaining Online Behaviour and Cybercrime Victimization, i Kranenbarg, M. W. og Leukfeldt, R. (red.) *Cybercrime in Context.* Amsterdam: Springer International Publishing, s. 21-42.

Veenstra, S., Zuurveen, R., & Stol, W. P. (2015) *Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden-en Kleinbedrijf en Zelfstandigen zonder Personeel in Nederland.* Lectoraat Cybersafety: Leeuwarden.

Wall, D. (2007) Cybercrime. 1. Utg. Polity Press.

Wanamaker, K. A. (2019) *Profile of Canadian businesses who report cybercrime to police*. The 2017 Canadian Survey of Cyber Security and Cybercrime 2019-R006. Ottowa: Public Safety Canada.

Wintershalldea (2020) *Hvem vi er.* Tilgjengelig fra: https://wintershalldea.no/nb/hvem-vi-er (Hentet: 06. april 2020).

Whelan, C. (2017) Security networks and occupational culture: understanding culture within and between organisations. *Policing and society*, 27(2), s. 113-135.

Wood, J. og Dupont, B. (2006) Introduction: Understanding the Governance of Security, i Jennifer Wood og Benoît Dupont (red.) *Democracy, society and the Governance of Security*. Cambridge: University Press, s. 1-10.

Wood, J., og Shearing, C. (2007) *Imagining security*. Portland: Willan

Workman, M., Bommer, W. H., og Straub, D. (2008) Security lapses and the omission of infor- mation security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), s. 2799–2816.

Yar, M. (2005) Computer hacking: Just another case of juvenile delinquency?. *The Howard Journal of Criminal Justice*, 44(4), s. 387–399.

Yar, M. og Steinmetz, K.F. (2019) *Cybercrime and Society*. 3. utg. Sage Publications.

Zedner, L. (2009) *Security*. London: Routledge.

Vedlegg

Vedlegg A
Informasjonsskriv og samtykkeerklæring

Vil du delta i forskningsprosjektet

«Cybersecurity»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å se nærmere på hvordan organisasjoner beskytter seg mot svindel, hvilke konsekvenser svindel har for bedrifter og hvilken kunnskap ansatte har om dette. I dette skrivet gir jeg deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Formålet med prosjektet er å få en forståelse for hvordan individer og organisasjoner opplever og beskytter seg mot cyberkriminalitet. Norge er et av verdens mest digitaliserte land og står overfor store utfordringer i behovet for vern mot cyberkriminalitet. Annen hvert år gjennomfører Næringslivets sikkerhetsråd en kriminalitets- og sikkerhetsundersøkelse, KRISINO, hvor norske bedrifter i privat og offentlig sektor deltar. KRISINO 2019 viste at 15 prosent av respondentene hadde vært utsatt for løspengevirus de siste 12 månedene, og at 13 prosent hadde vært utsatt for direktørsvindel. I tillegg viste undersøkelsen at blant private virksomheter med mer enn 100 ansatte var hele 50 prosent utsatt for direktørsvindel. Med en økende grad av digitalisering er det sannsynlig å tenke at cyberangrep vil være en stor trussel for virksomheter fremover. Med dette i bakgrunn, og at teknologien stadig er i utvikling og fører til nye måter å svindle på, er det ikke usannsynlig at flere bedrifter vil utsettes for cyberangrep i tiden fremover. Det vil derfor være interessant å se hvordan et stort selskap i Norge forholder seg til dette fenomenet.

Problemstillingen for dette prosjektet er:
Hvordan beskytter selskapet seg mot svindel, hvilke konsekvenser har svindel for bedriften og hvilken kunnskap har ansatte om dette?

Hvem er ansvarlig for forskningsprosjektet?

Institutt for kriminologi og rettssosiologi ved universitetet i Oslo er ansvarlig for dette masterprosjektet. Oppgaven er et samarbeid mellom student, Siren Dysvik, og Wintershall Dea. Ole-Martin Dahle er min veileder fra selskapet.

Hvorfor får du spørsmål om å delta?

Totalt seks til ti (6-10) personer, inkludert deg selv, har blitt spurt om å delta i dette prosjektet. Du har blitt spurt basert på informasjon fra din leder om at du jobber i IT-avdelingen i Wintershall Dea.

Hva innebærer det for deg å delta?

Metode for å samle inn data er med semistrukturerte intervjuer som i stor grad er en løs samtale om prosjektets tema. Hvis du velger å delta i prosjektet innebærer det at du har en samtale med studenten, hvor du bes om å svare på spørsmål som har med din jobb og cybersecurity å gjøre. Her er noen eksempler på spørsmål du kan få:

- Hva gjør dere for å ivareta datasikkerheten til selskapet?
- Hvordan forebygger dere cyberkriminalitet?
- I hvilken grad opplever dere at ledelse og ansatte har nok kunnskap om dette?

Jeg ønsker å benytte meg av en lydopptaker under intervjuet. Da jeg er klar over at informanter fra IT-avdelingen sitter inne med mye sensitiv informasjon som bedriften ikke ønsker skal lagres noe sted, vil jeg dele intervjuene inn i to deler. En generell del hvor jeg kan ta opptak, og en mer detaljert del hvor jeg kun tar notater for hånd. Intervjuet vil vare i maksimalt en (1) time, med beregnet tid til ca. 45 minutter.

Det er frivillig å delta

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

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Jeg vil bare bruke opplysningene om deg til formålene jeg har fortalt om i dette skrivet. Jeg behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Kun student og veileder har tilgang til data.
- All data vil behandles anonymt. Dette vil si at navnet og kontaktopplysningene dine vil erstattes med en kode som lagres på egen navneliste adskilt fra øvrige data.
- All data oppbevares på sikkert nettverksområdet som kun student og veileder fra UiO har tilgang til. Skriftlig materiale vil oppbevares i innelåst skap på instituttets område som kun student har tilgang til.
- Informanter vil ikke kunne gjenkjennes i publikasjon da datamaterialet vil være fullstendig anonymisert.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er september 2021, med mest sannsynlig slutt ila. juni 2021. All datamateriale, det vil si opptak og notater fra intervju, vil permanent slettes/makuleres ved prosjektets slutt.

Dine rettigheter

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

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

Hva gir oss rett til å behandle personopplysninger om deg?

Jeg behandler opplysninger om deg basert på ditt samtykke.

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

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Institutt for kriminologi og rettssosiologi Siren Dysvik, [redacted]
- Institutt for kriminologi og rettssosiologi ved Helene O. I. Gundhus, [redacted]
- Vårt personvernombud: Roger Markgraf-Bye, [redacted], [redacted]

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

- NSD – Norsk senter for forskningsdata AS på epost ([redacted]) eller på telefon: [redacted].

Med vennlig hilsen

Helene O. I. Gundhus (Forsker/veileder)

Siren Dysvik (Student)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Cybersecurity*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

☐ å delta i intervju

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

---

(Signert av prosjektdeltaker, dato)

Vedlegg B

Godkjenning fra NSD

NSD sin vurdering

Skriv ut

Prosjekttittel
Cyber security

Referansenummer
169590

Registrert
22.05.2020 av Siren Dysvik - sirend@uio.no

Behandlingsansvarlig institusjon
Universitetet i Oslo / Det juridiske fakultet / Institutt for kriminologi og rettssosiologi

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)
Helene Oppen Ingebrigtsen Gundhus, h.o.i.gundhus@jus.uio.no, tlf: 41523351

Type prosjekt
Studentprosjekt, masterstudium

Kontaktinformasjon, student
Siren Dysvik, siren.dysvik@student.jus.uio.no, tlf: 99571697

Prosjektperiode
19.05.2020 - 30.06.2022

Status
13.01.2021 - Vurdert

Vurdering (2)

13.01.2021 - Vurdert
NSD har vurdert endringen registrert 13.01.2021.

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 13.01.2021. Behandlingen kan fortsette.

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

Lykke til med prosjektet!

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

25.05.2020 - Vurdert
Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet 09.01.2020 med vedlegg, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde:
https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html

Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 30.06.2022.

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

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

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).
NSD vurderer at informasjonen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

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

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

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

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

Lykke til med prosjektet!

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

Vedlegg C

Intervjuguide

Del 1 – Bakgrunn og kompetanse

- Hva jobber du med?
- Hvor lenge har du jobbet i selskapet?
- Hvordan vil du definere cybersecurity?
- Kan du beskrive hvilken rolle du har i forhold til arbeidet med cybersecurity i bedriften?

Del 2 – Forebygging

- Hvordan jobber dere med cybersecurity i bedriften?
- Hvordan vil du beskrive kunnskapen din bedrift har om cybersecurity?
- I hvilken grad vil du si de ansatte i bedriften har tillit bedriftens kunnskaper om cybersecurity?
- Hvordan holder du deg oppdatert på trusselbildet?
- Samarbeider dere med andre aktører om sikkerheten til bedriften? I så fall, hvem?

Del 3 – Svindel

- Hvordan definerer du svindel?
- Hva gjør selskapet for å forhindre svindel?
- Hvordan avdekker dere cybercrime og svindel?
- Hva er de vanligste svindelmetodene bedriften utsettes for?
- Har du en oversikt over hvor ofte dere blir forsøkt svindlet?
- Har selskapet i løpet av de siste 12 månedene blitt utsatt for
    - Å få tilsendt fakturaer av varer eller tjenester som ikke er bestilt?
    - Løspengevirus?
    - Direktørsvindel?
- Hvis ja, politianmelder dere hendelsene?
    - Hvorfor/hvorfor ikke?
    - Hvilke lovbrudd anmelder dere?
- Hvilke tanker har du rundt hvem som står bak slike cyberangrep?
- Har dere opplevd at noen som jobber i selskapet har vært involvert i svindelforsøk mot dere? I så fall, kan du fortelle mer om dette?

- Gir ansatte beskjed dersom de har mottatt f.eks. en mail de mener det er noe rart med? I så fall, hvordan gjør de dette, og til hvem?
- Er det spesifikke grupper/avdelinger som har en tendens til å utsettes for svindel mer enn andre?

Del 4 – Sikkerhet

- Hvilke prosedyrer har dere dersom bedriften utsettes for cyberangrep og svindel?
- Hvordan formidler dere informasjon om cybersikkerhet til ansatte?
    - Gjennomfører dere tester? I så fall,
        - hvordan fungerer dette?
        - hvor ofte sendes slike tester ut?
        - Hva gjør dere med resultatene fra slike tester?
- Hvilken opplæring gis de ansatte rundt cybersikkerhet?
- Hvilken effekt synes du opplæringen har og hvordan måles denne?
- Hvordan opplever du at ansatte tar i mot opplæringen?
- Hvilke restriksjoner har dere på hva ansatte har lov å legge ut på nett?

Del 5 – Koronapandemien

- Hvilke tiltak gjorde dere med tanke på sikkerhet når ansatte måtte flytte til hjemmekontor?
- Når tenker du at ansatte er mest utsatt for svindelforsøk? På kontoret eller hjemme?
- Har dere opplevd en økning i svindelforsøk på grunn av koronaviruset? I så fall, hva tror du dette skyldes?

Til slutt

- Er det noe du vil legge til eller gå igjennom før vi avslutter?

Vedlegg D

Informasjonsskriv og spørreskjema norsk

Cybersikkerhet

Takk for at du deltar i dette forskningsprosjektet om cybersikkerhet.

Cybersikkerhet

Den teknologiske utviklingen går i et hurtig tempo og ny teknologi tas i bruk hver dag. Dette gir virksomheter gode muligheter for effektivisering og tilrettelegging. Men digitalisering fører også med seg trusler og sårbarheter som ikke er ønskelige (NSM, 2020). Næringslivets sikkerhetsråd har den siste tiden sett en dreining fra angrep mot datamaskiner og nettverk til angrep rettet mot enkeltpersoner. Det dreier seg om alt fra rene svindelforsøk til phising, løsepengevirus eller falske utpressingsforsøk (NSR, 2020).

Det er derfor viktig at virksomheter og individer er bevisst på hvordan de skal sikre seg mot slike sårbarheter. Fokus på cybersikkerhet er sentralt i dette arbeidet, og ansatte må blant annet få informasjon, opplæring og ha fokus på sikkerhetskultur for å forebygge de trusler og sårbarheter digitaliseringen fører med seg.

Formål:

Prosjektets formål er å få en forståelse for hvordan individer og selskaper opplever og beskytter seg mot cyberkriminalitet. Institutt for kriminologi og rettssosiologi ved Universitetet i Oslo er ansvarlig for dette masterprosjektet, som er et samarbeid mellom student, Siren Dysvik, og Wintershall Dea.

Hvorfor får du spørsmål om å delta?

Undersøkelsen går til alle ansatte i Wintershall Dea.

Hva innebærer det for deg å delta?

Å delta i undersøkelsen innebærer å fylle ut et spørreskjema. Dette tar ca. 10 minutter. Spørreundersøkelsen er delt inn i åtte kategorier.

Det er frivillig å delta:

Det er frivillig å delta i undersøkelsen, og du kan når som helst trekke samtykket tilbake uten å oppgi noen grunn. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg. Det vil heller ikke påvirke ditt forhold til arbeidsplassen og arbeidsgiver.

Ditt personvern - hvordan jeg oppbevarer og bruker dine opplysninger:

Prosjektet er godkjent av NSD - Norsk senter for forskningsdata. All informasjon som samles inn behandles konfidensielt og i samsvar med personvernregelverket. Informasjon fra undersøkelsen vil kun brukes til det formål som er angitt ovenfor. Ingen data som kan identifisere den enkelte vil bli publisert.

Hvor kan du finne ut mer?

Hvis du har spørsmål til prosjektet, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Institutt for kriminologi og rettssosiologi - Siren Dysvik, 99 57 16 97
- Institutt for kriminologi og rettssosiologi - Helene O. I. Gundhus, 41 52 33 51

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

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

Ditt bidrag til denne undersøkelsen er verdsatt.

Med vennlig hilsen

Helene O. I. Gundhus. (Forsker/veileder)

Siren Dysvik (Student)

Bakgrunnsinformasjon

Kjønn

- ○ Kvinne
- ○ Mann
- ○ Annet

	18 - 30	31 - 40	41 - 50	51 - 60	Over 61
Alder	○	○	○	○	○

	1 - 3 år	4 - 6 år	7 - 10 år	Over 10 år
Hvor mange år har du vært ansatt/innleid i Wintershall Dea? (Inkludert tiden i Wintershall eller DEA)	○	○	○	○

	Stavanger	Bergen	Offshore	Ønsker ikke å besvare
Hvilken avdeling hører du til?	○	○	○	○

	Administrativ	Teknisk	Ingen av delene	Ønsker ikke å besvare

Hvilken kategori er mest gjeldende for ditt arbeidsområde?	○	○	○	○

	Leder	Ikke leder	Ønsker ikke å besvare
Hvilken stillingstype har du?	○	○	○

Nedenfor finner du en del beskrivende utsagn som du skal ta stilling til. Du kan kun velge et alternativ per utsagn.

Cybersikkerhet

	Helt uenig	Delvis uenig	Delvis enig	Helt enig	Ønsker ikke å besvare
Jeg vet hva cybersikkerhet er	○	○	○	○	○
Jeg bekymrer meg for cyberangrep	○	○	○	○	○
Dataangrep og andre sikkerhets-hendelser kan ramme alle	○	○	○	○	○
Arbeidsplassen min har regler for cybersikkerhet	○	○	○	○	○
Jeg følger de regler og prosesser arbeidsplassen anbefaler når det gjelder cybersikkerhet	○	○	○	○	○

Svindel

	Ja	Nei	Ønsker ikke å besvare
Jeg har blitt utsatt for svindelforsøk de siste 12 mnd. i jobbsammenheng (Ikke som en test/prøve fra IT)	○	○	○

Hvis du svarte ja på forrige spørsmål, hvilken svindelmetode var dette?

	Ja	Nei	Ønsker ikke å svare
Dersom du har vært utsatt for et svindelforsøk, rapporterte du hendelsen til IT?	○	○	○

Dersom du rapporterte hendelsen, hvordan gjorde du dette?

Nedenfor finner du en del beskrivende utsagn som du skal ta stilling til. Du kan kun velge et alternativ per utsagn

	Helt uenig	Delvis uenig	Delvis enig	Helt enig	Ønsker ikke å besvare
Cybersikkerhet er viktig i jobbsammenheng	○	○	○	○	○
Cybersikkerhet er viktig i privat sammenheng	○	○	○	○	○
Jeg føler meg trygg med tanke på cybersikkerhet når jeg har hjemmekontor	○	○	○	○	○
Jeg føler meg trygg med tanke på cybersikkerhet når jeg er på jobb	○	○	○	○	○

Passord

	Helt uenig	Delvis uenig	Delvis enig	Helt enig	Ønsker ikke å besvare
Jeg bruker samme passord flere steder i jobbsammenheng	○	○	○	○	○

Jeg bruker samme passord flere steder i privat sammenheng	○	○	○	○	○
Jeg bytter passord med jevne mellomrom i jobbsammenheng	○	○	○	○	○
Jeg bytter passord med jevne mellomrom i privat sammenheng	○	○	○	○	○
Jeg bruker totrinnsbekreftelse der det er mulig, for å sikre mine digitale kontoer både privat og i jobbsammenheng	○	○	○	○	○

Informasjon

	Helt uenig	Delvis uenig	Delvis enig	Helt enig	Ønsker ikke å besvare
Jeg opplever at selskapet har kunnskap om cyberkriminalitet og de trusler det medfører	○	○	○	○	○
Jeg ønsker mer informasjon om cyberkriminalitet og de trusler det medfører	○	○	○	○	○
Jeg synes at jeg får tilstrekkelig informasjon fra selskapet om de truslene som finnes på internett	○	○	○	○	○
Jeg vet hvor informasjon om IT-sikkerhet på jobb er tilgjengelig hvis jeg ønsker å lære mer eller oppdatere meg	○	○	○	○	○
Jeg vet hvilke tegn jeg skal se etter for å sjekke om noe jeg mottar kan være et svindelforsøk	○	○	○	○	○
Jeg vet hva jeg skal gjøre om noe som avviker fra normalen skjer	○	○	○	○	○
Jeg vet hvem jeg skal varsle om noe som avviker fra normalen skjer	○	○	○	○	○

Opplæring

	Helt uenig	Delvis uenig	Delvis enig	Helt enig	Ønsker ikke å besvare
Selskapet formidler kunnskap om cybersikkerhet på en forståelig måte	○	○	○	○	○
Jeg har fått opplæring i selskapets sikkerhetsrutiner når det gjelder cybersikkerhet	○	○	○	○	○
Jeg ønsker mer opplæring i cyber-sikkerhet fra selskapet	○	○	○	○	○
Jeg er trygg på hva jeg skal gjøre hvis jeg mottar noe som ligner et svindelforsøk	○	○	○	○	○
Jeg undersøker om et vedlegg eller en lenke er trygg før jeg åpner den	○	○	○	○	○
Opplæring i cybersikkerhet er vans-kelig og krevende	○	○	○	○	○
Jeg har fått opplæring i hva direk-tørsvindel er	○	○	○	○	○
Jeg har fått opplæring i hva phising er	○	○	○	○	○
Jeg har fått opplæring i hva smish-ing er	○	○	○	○	○
Jeg har fått opplæring i hva løse-pengevirus er	○	○	○	○	○

Kultur på arbeidsplassen

	Helt uenig	Delvis uenig	Delvis enig	Helt enig	Ønsker ikke å svare
Jeg synes det er ubehagelig å søke hjelp fra IT-teamet hvis jeg har åp-net noe jeg ikke skulle ha åpnet	○	○	○	○	○
Jeg opplever at jeg har tid i min ar-beidsdag til å sjekke mail og lignen-de for svindelforsøk	○	○	○	○	○

Jeg synes det er ubehagelig å si fra om egne brudd på IKT-regler	○	○	○	○	○
Jeg synes det er ubehagelig å si fra om arbeidskollegers brudd på IKT-regler	○	○	○	○	○
Jeg opplever at arbeidsgiver følger med på meg og arbeidet mitt på en måte som føles ubehagelig	○	○	○	○	○

Champion-program

Et champion-program er en ide om at enkelte personer i selskapet skal fungere som en slags førstehjelp. En champion vil få opplæring i sikkerhet og være tilgjengelig for andre i sin avdeling når det gjelder spørsmål om cybersikkerhet. For eksempel, hvis en ansatt mottar en e-post de tror kan være phishing, kan den ansatte gå til den som er champion i sin avdeling, i stedet for å kontakte IT. En champion representerer cybersikkerhet i sin avdeling.

Jeg synes champion-programmet høres fornuftig ut

- ○ Ja
- ○ Nei
- ○ Ønsker ikke å besvare

Jeg kunne tenkt meg å være en champion

- ○ Ja
- ○ Nei
- ○ Ønsker ikke å besvare

Har du ellers noen innspill eller kommentarer vedrørende cybersikkerhet?

Klikk på send for å fullføre spørreundersøkelsen.

Takk for at du deltok!

Vedlegg E

Informasjonsskriv og spørreskjema engelsk

Cybersecurity

Thank you for participating in this cybersecurity research project.

Cybersecurity

Technological development is taking place at a rapid pace and new technology is being used every day. This offers companies an opportunity for efficiency and facilitation. However, digitalisation simultaneously brings threats and vulnerabilities that are not desirable (NSM, 2020). The Norwegian Business and Industry Security Council has recently discovered a shift from computer and network attacks to attacks aimed at individuals. These vary from pure fraud attempts to phising, ransomware viruses or false extortion attempts (NSR, 2020)

Therefore, it is critical that companies and individuals are aware of how to protect themselves against such vulnerabilities. Focus on cybersecurity is central to this work, and employees must, among other things, receive information, training and focus on security culture in order to prevent the threaths and vulnerabilities that digitalisation entails.

Purpose:

The purpose of the project is to gain an understanding of how individuals and companies experience and protect themselves against cybercrime. The Department of Criminology and Sociology of Law at the University of Oslo is responsible for this master´s project, which is a collaboration between student, Siren Dysvik, and Wintershall Dea.

Why are you asked to participate?

The survey goes to all employees in Wintershall Dea.

What does it mean for you to participate?

Participating in the survey involves filling out a questionnaire. This takes approx. 10 minutes. The survey is divided into eight categories.

It is voluntary to participate:

Participation in the survey is voluntary, and you can withdraw your consent at any time without giving any reason. It will not have any negative consequences for you if you do not want to participate or later choose to withdraw. Nor will it affect your relationship with the workplace and employer.

Your privacy - how I store and use your information:

The project has been approved by NSD - Norwegian Center for Research Data. All information collected is treated confidentially and in accordance with the privacy regulations. Information from this study will only be used for purposes stated above**.** No data that can identify the individual will be published.

Where can you find out more?

If you have any questions about this study, or want to exercise your rights please contact:

- Department of Criminology and Sociology of Law - Siren Dysvik, 99 57 16 97
- Department of Criminology and Sociology of Law - Helene O. I. Gundhus, 41 52 33 51

If you have any questions related to NSD´s assessment of the project, please contact:

- NSD - Norwegian Center for Research Data AS
  - by email (personverntjenester@nsd.no)
  - or by telephone 55 58 21 17

Your contribution to this study is much appreciated.

Best regards

Helene O. I. Gundhus (Researcher/supervisor)

Siren Dysvik (Student)

Background information

Gender

- ◯ Woman
- ◯ Man
- ◯ Other

	18 - 30	31 - 40	41 - 50	51 - 60	Over 61
Age	◯	◯	◯	◯	◯

	1 - 3 years	4 - 6 years	7 - 10 years	Over 10 years
How many years have you been employed/hired at Wintershall Dea? (Including time in Wintershall or DEA)	◯	◯	◯	◯

	Stavanger	Bergen	Offshore	Do not want to answer
Which department do you belong to?	◯	◯	◯	◯

	Administra-tive	Technical	Neither	Do not want to answer
Which category applies the most to your area of work?	◯	◯	◯	◯

	Manager	Non manager	Do not want to answer
Which type of position do you have?	○	○	○

Below you will find a number of descriptive statements for you to consider. You can only select one option per statement.

Cybersecurity

	Fully disagree	Partly disagree	Partly agree	Fully agree	Do not want to answer
I know what cybersecurity is	○	○	○	○	○
I´m worried about cyber attacks	○	○	○	○	○
Computer attacks and other security incidents can affect anyone	○	○	○	○	○
My workplace has rules for cybersecurity	○	○	○	○	○
I follow the rules and processes the workplace recommends regarding cybersecurity	○	○	○	○	○

Fraud

	Yes	No	Do not want to answer
I have been a victim of fraud attempt for the past 12 months in a work context (not as a test/exercise from IT).	○	○	○

If you answered yes to the previous question, what type of fraud was it?

	Yes	No	Do not want to answer
If you have been the victim of a fraud attempt, did you report the incident to IT?	○	○	○

If you reported the incident, how did you do it?

Below you will find a number of descriptive statements for you to consider. You can only select one option per statement.

	Fully disagree	Partly disagree	Partly agree	Fully agree	Do not want to answer
Cybersecurity is important in a work context	○	○	○	○	○
Cybersecurity is important in a private context	○	○	○	○	○
I feel safe in terms of cybersecurity when I work from home	○	○	○	○	○
I feel safe in terms of cybersecurity when I am at work	○	○	○	○	○

Password

	Fully disagree	Partly disagree	Partly agree	Fully agree	Do not want to answer
I use the same password in several places in a work context	○	○	○	○	○
I use the same password in several places in a private context	○	○	○	○	○
I change my passwords on a regular basis in a work context	○	○	○	○	○

I change my passwords on a regular basis in a private context	○	○	○	○	○
I use 2-step verification where possible, to secure my digital accounts both privately and at work	○	○	○	○	○

Information

	Fully disagree	Partly disagree	Partly agree	Fully agree	Do not want to answer
I experience that the company has knowledge of cybercrime and the threats it entails	○	○	○	○	○
I want more information about cybercrime and the threats it poses	○	○	○	○	○
I receive sufficient information from the company regarding the threats online	○	○	○	○	○
I know where information about IT security at work is available if I want to learn more or update myself	○	○	○	○	○
I know what signs to look for if something I receive may be a fraud attempt	○	○	○	○	○
I know what to do if something deviates from normal	○	○	○	○	○
I know who to contact if something deviates from normal	○	○	○	○	○

Training

	Fully disagree	Partly disagree	Partly agree	Fully agree	Do not want to answer
I believe that the company conveys knowledge about cybersecurity in an understandable way	○	○	○	○	○

I have received training in the company´s safety routines regarding cybersecurity	○	○	○	○	○
I want more training in cybersecurity from the company	○	○	○	○	○
I am confident of what to do if I receive something similar to a fraud attempt	○	○	○	○	○
I check that the attachment or link is secure before opening it	○	○	○	○	○
Training in cybersecurity is difficult and demanding	○	○	○	○	○
I have received training in what CEO fraud is	○	○	○	○	○
I have received training in what phising is	○	○	○	○	○
I have received training in what smishing is	○	○	○	○	○
I have received training in what a ransomware virus is	○	○	○	○	○

Workplace culture

	Fully disagree	Partly disagree	Partly agree	Fully agree	Do not want to answer
I find it uncomfortable to seek help from the IT-team if I have opened something I should not have opened	○	○	○	○	○
I experience that I have time during my working day to check emails or similar for attempted fraud	○	○	○	○	○
I find it uncomfortable to report on my own violations of ICT rules	○	○	○	○	○
I find it uncomfortable to report on work colleagues violations of ICT rules	○	○	○	○	○

I experience that the employer follows me and my work in a way that feels uncomfortable	○	○	○	○	○

Champion-program

A champion program is an idea that some people in the company should operate as a kind of first aid. A champion will receive training in security and be available to others in their department when it comes to cybersecurity issues. For example, if an employee receives an e-mail they think may be phishing, the employee can seek the champion in their department, instead of contacting IT. A champion represents cybersecurity in his/her department.

I think the champion program sounds sensible

- ○ Yes
- ○ No
- ○ Do not want to answer

I would like to be a champion

- ○ Yes
- ○ No
- ○ Do not want to answer

Do you have any other input or comments regarding cybersecurity?

Please click send to complete the survey.

Thank you for participating!

Vedlegg F

Samarbeidsavtale

wintershall dea

AGREEMENT TO WRITE A MASTER THESIS
between

Wintershall Dea Norge AS

(the "Company")

and

Siren Dysvik

(the "Student")

Dear Siren,

In reference to our conversations with you, we confirm our willingness to support you in the writing of your master thesis during the period from 09.03.2020 to 15.06.2021 in collaboration with our HSEQ and Information Technology teams.

The title of the thesis is: **Cyber Security** - *Computer/Data attacks in the Oil industry?*

On the part of the Company, your work will be supported by **Ole Martin Dahle.**

The co-operation is subject to the principles in this agreement. To confirm the acceptance of such co-operation, please sign and return this agreement to the Company.

Prior to submitting documents to the University, including the master thesis, the Student shall present a draft to the Company in due time for the Company to review and check if the documents contain any information that cannot be published due to confidentiality reasons. If the Company discovers any such confidential information which, in the sole opinion of the Company, cannot be published, taking into account other applicable agreements between the Company, the Student and the University of Oslo ref. above, the Student shall remove or anonymize such confidential information in co-operation with the Company before submitting any documents.

After completion of the master thesis, the Student shall hand over an electronic copy of the thesis to the Company.

In the course of the co-operation, the Student will, both directly and indirectly, receive internal commercial and technical information from the Company including work processes, data etc. All information that becomes known to the Student shall be treated as strictly confidential, (also after completion of the thesis). Any use of such information in the master thesis shall be subject to the Company's above-mentioned review. Internal information may only be used in accordance with this agreement, the agreement between the Student, the Company and the University and the confidentiality agreement between the same parties.

page 1 of 2