DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram/spesialisering: SAMMAS Master i samfunnssikkerhet	Vårsemesteret, 2023 Åpen / ~~Konfidensiell~~
Forfatter: Mari Lekve Bjelle og Tonje Stamnes Lindbom	
Fagansvarlig ved UiS: Kenneth A. Pettersen Gould **Veileder:** Kenneth A. Pettersen Gould	
Tittel på oppgaven: Bevisstgjøring om cybersikkerhet i nettselskap - En studie av digital opplærings påvirkning på digital sikkerhetskultur **English title:** Cyber security awareness in Network Companies - A study of digital learning's effect on digital safety culture	
Studiepoeng: 30	
Emneord: Cybersikkerhet, bevisstgjøring, opplæring, digital opplæring, sikkerhetsstyring, sikkerhetskultur, digital sikkerhetskultur, nettselskap, kraftsektoren	**Sidetall: 89** + vedlegg/annet: 109 Stavanger, 15.06.2023

«Bevisstgjøring om cybersikkerhet i nettselskap»

Bilde hentet fra Sintef (2021)

Masteroppgave i Samfunnssikkerhet

Universitetet i Stavanger

Vår 2023

Forfatter: Mari Lekve Bjelle og Tonje Stamnes Lindbom

Veileder: Kenneth A. Pettersen Gould

Forord

To fantastiske år på Universitetet i Stavanger er på vei til å rundes av, og denne oppgaven markerer en endelig slutt. Masterstudiet i samfunnssikkerhet har vært både gøy, spennende og krevende, og er en erfaring vi ikke ville vært foruten.

Vi vil rette en stor takk til alle som har bidratt til at denne oppgaven ble til. Særlig takk til veileder Kenneth A. Pettersen Gould som har bidratt med gode råd og diskusjoner i prosessen. Vi vil også takke samtlige informanter og respondenter som har gjort prosjektet mulig, og en særlig takk til vår kontaktperson i nettselskapet som har vært positivt innstilt og til god hjelp gjennom hele prosessen.

Videre ønsker vi å rette en stor takk til Ole og Mathias, familie og venner som har støttet og hatt troen på oss gjennom masterskrivingen. Vi vil også takke våre trofaste hjemmekontor-kamerater, Billie og Thio!

Til slutt vil vi takke våre Stavanger-venner som har gjort både studiehverdagen og livet i byen ekstra fint.

Tonje Stamnes Lindbom & Mari Lekve Bjelle

Stavanger, 14.06.2023

Sammendrag

I takt med at verden digitaliseres, vokser det stadig frem sårbarheter som aktører med onde intensjoner ser muligheter for å misbruke. I dag ser man en særlig vekst der cyberkriminelle utnytter sårbarheter ved mennesker for å svindle eller få tilgang til et system. Denne tilnærmingen brukes også på ansatte som arbeider i samfunnskritiske funksjoner, som eksempelvis kraftbransjen. Dette har ført til økt behov for bevisstgjøring av ansatte for å hindre og stå imot cyberangrep. Denne oppgaven har hatt som hensikt å studere hvordan digital opplæring er med på å bevisstgjøre ansatte omkring cybersikkerhet, og om denne bevisstgjøringen påvirker den digitale sikkerhetskulturen. På bakgrunn av dette er følgende problemstilling formulert:

> "*Hvordan påvirker digital opplæring om cybersikkerhet den digitale sikkerhetskulturen i et nettselskap*?".

For å besvare problemstillingen ble det gjennomført en case-studie ved bruk av Mixed Methods der vi samlet data gjennom både intervju og spørreundersøkelse. Det ble gjennomført intervju og spørreundersøkelse med ledelsen og superbrukere for å få innblikk i hensikten bak opplæringsmetodene og deres syn på hvordan den evner å påvirke den digitale sikkerhetskulturen i nettselskapet. Det ble også sendt ut en spørreundersøkelse til de ansatte for å kartlegge deres synspunkt og for å sammenligne svarene.

Studien avdekker at nettselskapet benytter ulike former for digitale opplæring, hvor enkelte ser ut til å fremme læring hos ansatte, mens andre har svakheter som begrenser utbytte. Den digitale opplæringen ser ut til å påvirke digital sikkerhetskultur på en positiv måte både på individ- og gruppenivå. Som følge av den digitale opplæringen har mange ansatte utviklet forståelse for risikoen, samt viser årvåkenhet og kompetanse knyttet til cybersikkerhet.

Det fremkommer også at den digitale opplæringen ikke oppnår en tilstrekkelig påvirkning på den digitale sikkerhetskulturen, som kunne styrket muligheten for å verne seg mot eventuelle cyberangrep. Studien avdekker flere årsaker til at digital opplæring ikke oppnår full effekt på digital sikkerhetskultur. Deriblant begrensninger ved nettselskapets bruk av den digitale opplæringen, påvirkning av andre læringsformer, og begrensinger innen hvorvidt et sikkerhetsstyringstiltak som digital opplæring evner å påvirke en kultur.

Innholdsfortegnelse

Figuroversikt

Tabelloversikt

Diagramoversikt

Forkortelser

NVE: Noregs vassdrag og energidirektorat

HRO: High Reliability Organizations

KBO: Kraftforsyningens beredskapsorganisasjon

SCADA: Supervisory Control and Data Acquisituion

SDI: Stegvis deduktiv-induktiv

1.0 Innledning

I dagens samfunn digitaliseres mange prosesser i jakten på en effektiv og tilgjengelig hverdag for både enkeltpersoner, organisasjoner og samfunn. I takt med alle godene som digitalisering medfører, vokser det også frem sårbarheter i ethvert digitalt system, som både kan føre til tilsiktede og utilsiktede hendelser (Njå et al, 2020). Tilsiktede hendelser i form av cyberkriminalitet har vokst frem som en av de største risikoene i Norge, ifølge rapporten Risiko 2022 (NSM, 2022). Som følge av utviklingen innen digitale sårbarheter, handler det ikke lenger *om* man blir utsatt for cyberangrep, men heller *når* (Martin, 2019).

Ifølge Direktoratet for samfunnssikkerhet og beredskap (2016) regnes kraftsektoren for å være en av de mest kritiske samfunnsfunksjonene, ettersom befolkningen og øvrige samfunnsfunksjoner er totalt avhengige av stabil strømforsyning til enhver tid. Kraftsektoren består blant annet av kraftselskap og nettselskap, og det har vokst frem sårbarheter i begge som følge av digitalisering. Nettselskaper er likevel regnet for å være det mest sårbare for cyberangrep som følge av ansvaret for kontinuerlig utlevering av strøm (Skotnes, 2015). De digitale sårbarhetene i nettselskaper kommer av økt kompleksitet og tettere sammenkobling mellom driftskontroll- og administrative system, hvor systemene er blitt mer uoversiktlige (NOU, 2015:13). I tillegg eksisterer det en sårbarhet knyttet til at uvedkommende får tilgang til kraftsensitiv informasjon som i verste fall kan misbrukes til å påføre skade eller hindre strømleveranse (NOU, 2015:13). Det er nødvendig at nettselskaper jobber for å redusere disse digitale sårbarhetene, for å kunne opprettholde den samfunnskritiske funksjonen.

De mest benyttede metodene for å utføre cyberkriminalitet i dag er ved å manipulere mennesker som arbeider i organisasjoner for å få tilgang til systemene (NOU, 2015:13; Martin, 2019). Denne type angrep er også relevant for nettselskaper (NOU, 2015:13). Noregs vassdrags- og energi direktorat (NVE, 2017) viser til at flere norske virksomheter i kraftbransjen har rapportert om økende forekomst av cyberhendelser, hvor hendelsene stort sett handler om bedrageri, dataskadeverk, virus, forsøk på hacking og datainnbrudd. Dette kan kategoriseres som tilsiktede hendelser, hvor angriper har bevisste, forsettlige og ondsinnede hensikter (Jore, 2017). Det at cyberangriper benytter mennesker som inngangsport, har medført økende behov

for menneskelige barrierer, som eksempelvis kompetanse. Dette er særlig viktig da tekniske løsninger i seg selv ikke er tilstrekkelig i cybersikkerhetsarbeidet (Wiley et al. 2020).

Ifølge Malmedal (2020) er en avhengig av at samtlige ansatte i virksomheter er bevisstgjort for å øke cybersikkerheten. For å styrke et nettselskaps cybersikkerhet, er opplæring et sikkerhetsstyrende tiltak som kan styrke menneskelige barrierer (Njå et. al, 2020; Lai, 2013). Økt kunnskapsnivå gjennom opplæring har videre potensial for å påvirke sikkerhetskulturen (Roer, 2015; LaFrance (2004 referert i Talbot & Jakeman). En sterk sikkerhetskultur er egnet for å gi et høyere nivå av sikkerhet i virksomheten, og er dermed noe virksomheter bør strebe etter (Reason, 1997). Begrepet digital sikkerhetskultur handler om det samme, men retter seg spesifikt mot digitale aspekter ved sikkerhet (Malmedal, 2020). Dette synliggjør at opplæring og en sterk digital sikkerhetskultur kan styrke menneskelige barrierer for å motstå cyberangrep.

På tross av at opplæring og en styrket digital sikkerhetskultur anses som sentralt for å bygge menneskelige barrierer, er det tall som viser at opplæring om cybersikkerhet inneholder mangler. Mørketallsundersøkelsen viser at bare halvparten av Norske virksomheter gjennomfører tiltak for å øke bevissthet om cybersikkerhet, selv om mangel på sikkerhetsbevissthet hos ansatte er en sentral forklaring på hvorfor cyberhendelser skjer (NSR, 2022). Utfordringer knyttet til cybersikkerhetskompetanse er også tilfellet i kraftsektoren (NOU, 2015:13). Dette på tross av at veileder for Kraftberedskapsforskriften (NVE, 2020) oppfordrer til bevisstgjøringsarbeid av ansatte. Ettersom dagens nivå av menneskelig bevissthet ikke anses som tilstrekkelig for å fremme cybersikkerhet, indikerer dette at virksomheter ikke jobber nok, eller på rett måte, for å øke ansattes bevissthet. Mørketallsundersøkelsen (NSR, 2022) viser at elektronisk læring er blant de mest benyttede metodene for kompetanseheving om cybersikkerhet. Dette har fått oss til å stille spørsmål om hvordan digital opplæring faktisk fungerer for å øke kompetansen til ansatte i nettselskaper, og hvordan den digitale sikkerhetskulturen blir påvirket av opplæringsmetoden.

1.1 Problemstilling

For å undersøke temaet nærmere, har vi valgt å studere ett nettselskap som benytter digital opplæring for å øke bevisstheten omkring cybersikkerhet. Vi valgte et nettselskap som er lokalisert i Norge, og blir regnet for å være stort av størrelse. Vi argumenterer for at det er nyttig å studere hvordan digital opplæring faktisk fungerer for å bygge kompetanse på tvers i selskapet, og studere hvilken påvirkning dette har for den digitale sikkerhetskulturen. Dette har ført til følgende problemstilling:

> ***"Hvordan påvirker digital opplæring om cybersikkerhet den digitale sikkerhetskulturen i et nettselskap?"***

For å kunne besvare denne problemstillingen har vi utformet følgende forskningsspørsmål:

> F1: *Hvordan benytter nettselskapet digital opplæring innen temaet cybersikkerhet, og hvordan fungerer metoden for å fremme læring?*

Dette forskningsspørsmålet skal primært avklare hvordan nettselskapet benytter digital opplæring for å bygge kompetanse om cybersikkerhet. Dette vil være nyttig for å kunne få frem ulike kvaliteter ved digital opplæring, og hvordan opplæringen kan påvirke læring og bevisstgjøring hos de som jobber i virksomheten. Dette er viktig da studier viser at opplæringsmetoden har noe å si for hva mennesker får ut av læringen (Roer, 2015; Skotnes, 2014). Utbyttet fra læringen kan ha en innvirkning på momenter innen digital sikkerhetskultur, som vil bli løftet frem i forskningsspørsmål 2.

> F2: *Hvordan påvirkes de digitale sikkerhetskulturmomentene kompetanse, atferd, risikopersepsjon og interesse av den digitale opplæringen?*

For å kunne si noe om hvordan digital opplæring påvirker digital sikkerhetskultur, vil det være aktuelt å studere momenter som anses som relevante for læring. NorSIS (2019) sier at kompetanse, atferd, risikopersepsjon og interesse er momenter innen digital sikkerhetskultur som direkte påvirkes av læring. Dette muliggjør innsikt i hvordan virksomhetens ansatte vurderer at momentene har blitt påvirket av digital opplæring.

F3: *I hvilken grad skaper digital opplæring felles digital sikkerhetskultur i nettselskapet, og hvilke faktorer påvirker evnen til å gjøre det?*

Det siste forskningsspørsmålet har som formål å kunne si noe om den felles digitale sikkerhetskulturen i nettselskapet. Dette anses som relevant da digital sikkerhetskultur omfatter mer enn bare kultur på individuelt nivå (Reason, 1997). I tillegg anses det som sentralt for virksomhetens cybersikkerhet er avhengig av at alle må være bevisstgjort for å redusere digitale sårbarheter i form av menneskelige feil (Malmedal, 2020).

Ved å svare på de tre forskningsspørsmålene ovenfor, argumenterer vi for at dette vil gi en helhetlig innsikt i digital opplærings læringseffekt, og hvordan denne effekten påvirker nettselskapets digitale sikkerhetskultur. Det vil likevel være behov for å presisere avgrensninger av oppgavens fokus.

1.2 Avgrensning:

Ettersom problemstillingen tar for seg hvordan digital opplæring påvirker digital sikkerhetskultur, har vi i denne oppgaven valgt å sette søkelys på momentene som er relevant for læring (som presentert i forskningsspørsmål 2). Det er dermed deler av digital sikkerhetskultur som ikke inkluderes i oppgaven. De momentene som ikke inkluderes er vilje til digitalisering, tillit, fellesskap, samt styring og kontroll (NorSIS, 2019). Basert på at vi utelater sentrale momenter av digital sikkerhetskultur, og at læring og bevisstgjøring utgjør bare en del av sikkerhetskulturen, må det bemerkes at denne oppgaven har sine begrensninger for å studere digital sikkerhetskultur i sin helhet (Roer, 2015). Likevel trekker både NorSIS (2019), Roer (2015), Parson et al (2015) og Wiley et al (2020) frem at opplæring og bevisstgjøring har en effekt på sikkerhetskulturen. Vi anser det dermed verdifullt å studere de aktuelle momentene, da dette gir oss bedre mulighet for å belyse hvordan digital opplæring påvirker den digitale sikkerhetskulturen.

Det må understrekes at digital opplæring om cybersikkerhet ikke er det eneste som påvirker den digitale sikkerhetskulturen i nettselskapet. Nettselskapet har også digital opplæring knyttet til blant annet informasjonssikkerhet og personvern ved bruk av digitale tjenester. I tillegg kan det tenkes å være andre virkemiddel og faktorer som påvirker den helhetlige digitale sikkerhetskulturen i nettselskapet. Vi kan ikke utelukke at også disse påvirker resultatet i denne

undersøkelsen, men fokuset i denne oppgaven vil utelukkende rette seg mot digital opplæring om cybersikkerhet.

Det er flere teoretikere som er skeptisk til hvilke metoder som kan benyttes i studier av sikkerhetskultur (Engen et al, 2021; Schein, 2010; Antonsen, 2009b). Denne oppgaven presenterer et øyeblikksbilde av sikkerhetskulturen i ett nettselskapet, og benytter spørreundersøkelse og intervju for å operasjonalisere konseptet digital sikkerhetskultur. Det kan dermed diskuteres hvorvidt oppgaven kan si noe om sikkerhetskulturen, eller om sikkerhetsklima er et mer passende begrep (Pidgeon, 1998). Dette kan utgjøre en avgrensning om hva studien kan si noe om, men dette vil vi videre gå inn på i teori-, metode- og diskusjonskapittelet.

1.3 Begrepsavklaring:

1.3.1 Digital opplæring:

Elektronisk læring (e-læring) og digital opplæring er begreper som benyttes om hverandre, der digital opplæring er et bredere begrep som omfatter all læring som foregår ved bruk av teknologi (Basak et al., 2018). Denne oppgaven benytter begrepet digital opplæring som en samlebetegnelse på ulike digitale opplæringsformer nettselskapet benytter. Eksempler på digitale opplæringsmetoder kan være elektroniske kurs (e-læringskurs), informasjon på e-mail og webinar (Hrastinski, 2008).

1.3.2 Sikring- og sikkerhet

Det norske ordet sikkerhet deles ofte opp i sikkerhet og sikring, eller safety og security, innad i sikkerhetsfaget. Safety blir oversatt til sikkerhet på norsk, mens security blir oversatt til sikring (Njå et. al, 2020). Sikkerhet blir ofte omtalt i dagligtalen som frihet fra trussel og skade, og kan relateres til både en følelse og en tilstand (Jore, 2017; Engen et.al., 2021). Det finnes ingen entydig definisjon på security, men Jore (2017) vektlegger at securityhendelser handler om bevisste, forsettlige og ondsinnede handlinger forårsaket av mennesker, slik som hacking. Ettersom hacking er en form for cyberangrep, anses "sikring" som mest treffende av de to sikkerhetsbegrepene relatert til cybersikkerhet. I den forbindelse er det nyttig å introdusere og presisere kulturbegrepet i relasjon til sikring.

1.3.2.1 Sikring- og sikkerhetskultur

Sikringskultur, mer kjent som security culture, er et forskningsfelt som har fått oppmerksomhet først i senere tid. Det finnes derfor ikke like mye forskning på sikringskultur, som på sikkerhetskultur. Ifølge Jore (2020) bør sikkerhetskultur og sikringskultur ideelt sett skilles fra hverandre, men ettersom faglitteraturen hittil ikke har kommet til enighet om en felles forståelse, er det per nå ikke mulig å gjennomføre i praksis. Dette underbygges også av Malcomson (2009).

Kriaa et al. (2015) sier at selv om safety- og securitykultur ikke er det samme, så sameksisterer de og har mye til felles. Dette samsvarer med Vierendeels et al. (2018) og Jore (2020) som peker på at sikringskultur og sikkerhetskultur har klare fellestrekk ved at de omfatter alle deler av virksomheten: både menneske, teknologi og organisasjon. Videre beskriver forskerne at de to ulike kulturretningene begge har mål om å hindre uønskede hendelser ved å benytte myke barrierer som eksempelvis bevisstgjøring.

På bakgrunn av den sprikende akademiske forståelsen omkring skillet mellom sikkerhetskultur og sikringskultur, har vi i denne oppgaven valgt å benytte teorier fra begge selv om cybersikkerhet egentlig er sikringsrelatert. Dette vurderer vi som mulig da kulturretningene ikke har et klart definert skille, og begge vektlegger opplærings- og bevisstgjøringsarbeid som sentralt for å styrke kulturen. Til tross for at vi presenterer teori som benytter begrepet sikring og sikkerhet relatert til kultur, så skiller vi ikke på begrepene etter teorikapittelet. Vi velger å benytte oss av begrepet sikkerhetskultur ettersom dette er det mest etablerte innen forskning på kultur.

1.3.3 Digital sikkerhetskultur

Ifølge Malmedal (2020) er digital sikkerhetskultur en del av sikkerhetskultur, men som retter seg spesifikt mot digital sikkerhet. Sikkerhetskultur er videre en del av organisasjonskultur. Dette viser hvordan de ulike kulturbegrepene henger sammen, og muliggjør bruk av samtlige kultur-teorier i denne oppgaven. Basert på at temaet for oppgaven retter seg mot

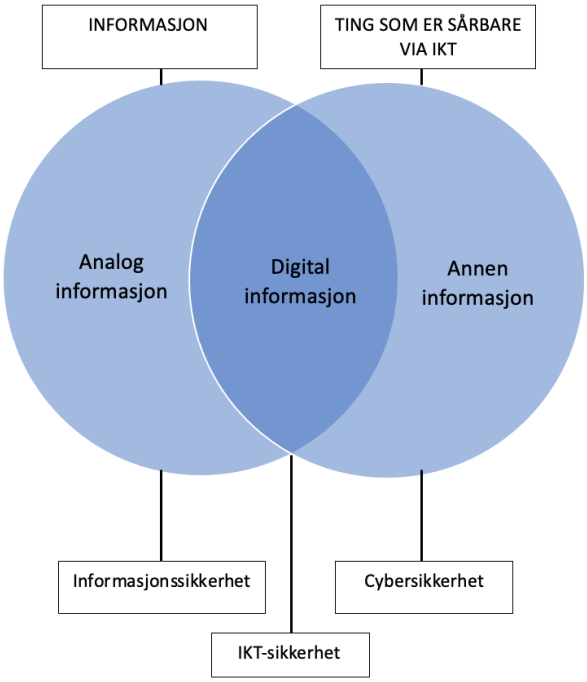
cybersikkerhet, benytter vi derfor begrepet *digital* sikkerhetskultur i problemstillingen og resten av oppgaven.

1.3.4 Hvordan skiller cybersikkerhet seg fra informasjonssikkerhet og IKT-sikkerhet

I dagens samfunn benyttes ulike begreper når en snakker om digital sikkerhet, hvorav begrepene informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet benyttes om hverandre. Ettersom denne oppgaven tar for seg digital opplæring om cybersikkerhet, er det nyttig å avklare betydningen av begrepet og hvordan det skiller seg fra de andre.

Informasjonssikkerhet handler om sikring av digital og fysisk informasjon. IKT-sikkerhet handler også om beskyttelse av informasjon, men har et tilleggsmoment som omhandler beskyttelse av kommunikasjonsteknologi. Eksempel på kommunikasjonsteknologi kan være maskinvare og programvare (NVE, 2017). Innenfor IKT-sikkerhet foreligger tre sentrale elementer for å ivareta IKT-sikkerheten. Disse tre elementene er konfidensialitet, tilgjengelighet og integritet (NOU 2015:13).

Når det gjelder cybersikkerhet, som denne oppgaven tar for seg, handler det om hele cyberdomenet. Cybersikkerhet omhandler alt fra datasystem og kommunikasjonsinfrastruktur, samt lagring og formidling av informasjon. Cybersikkerhet handler derfor om å beskytte alt som er koplet opp mot, eller er avhengig av, informasjons- og kommunikasjonsteknologi. Teknologien må anses som sårbar for at cybersikkerhetsbegrepet skal benyttes. Cybersikkerhet handler ikke bare om digitale sikkerhetstiltak, men også om prosedyrer, konsekvensreduserende tiltak, samt økt kompetanse og bevisstgjøring av de ansatte (NVE, 2017). Dette viser at bevisstgjøring er sentralt innen cybersikkerhet, og er dette som blir studert videre i oppgaven.



Figur 1: Sammenhengen mellom informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet (Basert på NVE, 2017)

1.4 Kontekst

1.4.1 Norsk kraftforsyning og nettselskap

Kraftnett kan deles inn i sentral-, regional- og distribusjonsnett. Ifølge NOU (2015:13) knytter sentralnettet sammen forbrukere, produsenter og overføringsledninger til utlandet. Regionalnettet binder sammen sentral- og distribusjonsnettet. Distribusjonsnettet står for den endelige leveringen av kraft til husholdninger, tjenesteytere og annen næringsvirksomhet (NOU, 2015:13). Kraftleverandører er de som produserer og selger strøm, mens nettselskaper er de som frakter strømmen ut til forbrukere. Det eksisterer over 100 nettselskaper i Norge, og nettselskapene har monopol på sine tjenester innenfor sine geografiske områder (NVE, u.å.; NVE, 2015). Et nettselskap driftes ved bruk av driftskontrollsystem (SCADA) og administrativt system. Det administrative system tar for seg funksjoner som økonomistyring, kundestøtte og handel. Driftskontrollsystemet blir knyttet direkte til drift av strømforsyning (NVE, 2017).

1.4.2 Hvorfor studere nettselskap opp mot cybersikkerhetsarbeid

Nettselskaper står for overføring av elektrisk energi ut til forbruker. De er ansvarlige for en stabil og pålitelig strømforsyning, noe som er helt avgjørende for viktige samfunnsoppgaver og kritiske samfunnsfunksjoner (DSB, 2016). Ifølge Skotnes (2015) er cybersikkerhet relevant for hele kraftbransjen, men nettselskaper og deres forsyningssikkerhet kan antas å være det mest sårbare leddet i strømforsyningen. Det administrative systemet og SCADA-systemet har lenge blitt ansett for å være skilt fra hverandre på en trygg måte, men i takt med fremsteg innen den digitale verden, har det også vokst frem sårbarheter i SCADA-systemet (Jaatun et al, 2017). Dette styrker Skotnes (2015) sitt argument om at forsyningssikkerheten er sårbar. Tall fra NVE (2021) viser til at det hovedsakelig er de administrative systemene som har blitt utsatt for cyberhendelser de siste årene i Norge. Rapporten viser videre at omtrent 3% har hatt cyberhendelser med konsekvens for driftskontrollsystemenes funksjon. På tross av lav prosentandel knyttet til konsekvenser for driftskontrollsystemet, finnes det eksempler som viser alvoret av omfanget ved en eventuell cyberhendelse. I 2015 ble flere regionale strømnett i Ukraina utsatt for cyberangrep. Deler av angrepet var målrettet mot menneskelige operatører. Angrepene fikk konsekvenser for hundretusener av mennesker i flere timer, noe som illustrerer sårbarheten og viktigheten av å prioritere cybersikkerhetsarbeid (Liang et al, 2016).

På bakgrunn av denne informasjonen mener vi det er nyttig å studere hvordan digital opplæring fremmer læring og påvirker den digitale sikkerhetskulturen i et nettselskap. Dette da kompetanse om cybersikkerhet anses som nødvendig for å redusere sårbarheter både relatert til det administrative- og driftskontrollsystemet, som beskrevet i innledningen.

1.4.3 Ulike Cybertrusler

Cybersikkerhetsarbeidet handler om å beskyttelse mot ulike cybertrusler. Et cyberangrep handler om at en aktør benytter et datasystem som redskap for å utføre ondsinnede handlinger som tyveri, spionasje, overbelastning, sabotasje eller overvåkning. Cyberangrep benyttes ofte av cyberkriminelle da det er relativt enkelt, billig, transnasjonalt og kan få massive konsekvenser (Martin, 2019). Konsekvenser av et cyberangrep på et nettselskap kan som nevnt være brudd i strømleveranse og lekking av sensitiv informasjon (NOU, 2015: 13).

NorSIS (2021) har laget en oversikt over de mest aktuelle cybertruslene som kan treffe ulike sektorer i samfunnet, og denne samsvarer med NVE (2021) sin liste over de vanligste digitale truslene i kraftsektoren. Det er disse cybertruslene ansatte i nettselskaper bør bli bevisstgjort om for å hindre uvedkommende i systemet eller fra å få tak i sensitiv informasjon. De ulike cybertruslene presenteres i tabellen nedenfor:

Trusler	Beskrivelse
Løsepengevirus	Løsepengevirus kan forekomme ved at en klikker på en link eller laster ned skadelig innhold på offerets datamaskin. Den skadelige programvaren kan videre kryptere eller lamme hele virksomhetens IT-system, og cyberangriper krever ofte penger for å frigjøre det.
Kontokapring	En ondsinnet aktør utgir seg for å være en ansatt i virksomheten, og ber om opplysninger som kan skade virksomhetens verdier. Den ondsinnede aktøren får ofte tilgang til en konto som følge av svakt passord eller andre svake sikkerhetsrutiner.
Verdikjedeangrep	Cyberkriminelle når gjennom til virksomheter ved å angripe virksomheter de er avhengige av, som gjerne har et svakere sikkerhetssystem. Derfra kan angriper nå hovedmålet.
Svindel	Svindel er en metode hvor den kriminelle aktøren misbruker tillit, fristelser eller skaper frykt for å få en til å trykke på en link eller laste ned et vedlegg som gir tilgang til sensitiv informasjon.
Phishing	Phishingangrep er en metode hvor ondsinnede aktører lurer til seg sensitiv informasjon. Enkeltpersoner i virksomheter kontaktes gjennom e-post eller SMS, hvor den ondsinnede aktøren utgir seg for å være en reell aktør/virksomhet. Ansatte blir lurt til å dele informasjon som senere kan misbrukes. Phishing er i dag en av de største truslene mot virksomheter.
Direktørsvindel	Ondsinnede personer utgir seg for å være sjef i virksomheten, og sender e-post eller SMS til personer med tilgang til midler som kan misbrukes. Eksempelvis kan de be økonomiansvarlig om å gjennomføre betaling av falsk faktura.

Tabell 1: NorSIS tabell over ulike cybertrusler (2021)

1.4.4 Relevant lovverk

1.4.4.1 Kraftberedskapsforskriften og Energiloven

Formålet med Kraftberedskapsforskriften (2012) er å sikre at "kraftforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene". Kraftforsyningens beredskapsorganisasjon (KBO), som består blant annet av ulike nettselskaper, har særlig ansvar for kontinuerlig opprettholdelse av strømforsyning i landet. Ifølge §4-2 må KBO-enhetene ha personell med kompetanse til å håndtere ekstraordinære situasjoner. §7-1 viser til at virksomheter med driftskontrollsystem skal sikre at disse fungerer til enhver tid og beskytte de mot alle typer uønskede hendelser.

I tillegg skal KBO-enhetene, ifølge Energiloven (1990) §9-3, drive effektiv avskjerming og beskyttelse av sensitiv informasjon, samt hindre at andre rettmessige brukere får adgang til sensitiv informasjon om kraftforsyningen. I veileder for Kraftberedskapsforskriften (NVE, 2020) står det at virksomheter bør iverksette organisatoriske tiltak som bevisstgjøring av ansatte. Kraftberedskapsforskriften og Energiloven belyser dermed betydningen av at nettselskapene beskytter skjermingsverdig informasjon. For å beskytte skjermingsverdig informasjonen, er en blant annet avhengig av tilstrekkelig opplæring.

2.0 Teori

For å kunne besvare problemstillingen og tilhørende forskningsspørsmål, skal det her presenteres teorier som anses relevante. Teorikapittelet er delt inn i to hoveddeler. I første del presenterer vi teori om sikkerhetsstyring, for å belyse at både opplæring og sikkerhetskultur er sentrale elementer innen cybersikkerhetsarbeidet i virksomheter. Videre presenterer vi teori om organisasjons-, sikkerhets- og digital sikkerhetskultur for å belyse hvordan en kultur har potensial for å påvirke sikkerheten, samt hvorvidt digital sikkerhetskultur kan styres. Underveis vil det rettes særlig fokus på opplærings relevans til kultur. Andre del av teorikapittelet tar for seg teorier knyttet til læring og spesifikt digital opplæring som læringsmetode. Avslutningsvis presenterer vi en opplæringsteori rettet mot cybersikkerhet. Dette blir gjort for å belyse hvordan prioritering og tilrettelegging av opplæring, kan påvirke effekten på læringsutbyttet, og hvordan dette i sin helhet kan påvirke den digitale sikkerhetskulturen.

Del 1: Teorier om sikkerhetsstyring og sikkerhetskultur

2.1 Sikkerhetsstyring

For å studere hvordan digital opplæring påvirker den digitale sikkerhetskulturen i et nettselskap, anser vi det nyttig å presentere teori om hvordan virksomheter jobber med sikkerhetsstyring. Sikkerhetsstyring blir benyttet av virksomheter for å styre sikkerheten i samsvar med definerte mål (Njå et al., 2020). Nettselskap som har mål om å opprettholde cybersikkerhet og kontinuerlig drift, kan benytte opplæring som et virkemiddel for å skape menneskelige barrierer som bevissthet og kompetanse hos de ansatte. Dette kan hjelpe virksomheten å verne seg mot cyberangrep. På bakgrunn av dette anses sikkerhetsstyringsteori som relevant for å besvare problemstillingen, og vil dermed bli presentert i det følgende.

Virksomheter kan styre sikkerheten ved å kombinere mål, virkemidler og rammebetingelser for å fremme eller begrense forskjellige aktiviteter. Sikkerhetsstyring består av virkemidler, løsninger og tiltak som er tilpasset rammebetingelsene, og som samsvarer med andre faktorer som sikkerhet, økonomi og andre forhold (Njå, et al., 2020). Når virksomheter skal sette mål og tiltak, må de være innenfor rammebetingelsene. Rammebetingelser kan for eksempel være lovmessige, slik som energiloven og kraftberedskapsforskriften fungerer for nettselskaper (Njå et al, 2020). Lovverket setter rammer for deres mål og tiltak relatert til cybersikkerhetsarbeidet.

Styring forutsetter at den som styrer vet hvor en skal, altså at en har et mål. Sikkerhetsmål utrykker en tilstand eller et sikkerhetsnivå som virksomheten ønsker å oppnå (Njå et al, 2020). Virksomheter kan sette seg cybersikkerhetsmål, hvor et eksempel kan være "alle ansatte i virksomheten skal kjenne til hva de må være bevisst på for å verne selskapet mot cybertrusler". Sikkerhetsmålene skal fungere som struktur på planlegging og opprettholdelsen av sikkerhetstiltaket i virksomheten, og kan på den måten medvirke til reduksjon av risikoen for digitale angrep over tid (Njå, et al., 2020).

Virksomheten kan benytte ulike virkemidler for å styre sikkerheten, og eksempel kan være stimulering. Stimulering kan foregå på ulike måter, men særlig relevant for denne oppgaven er opplæring (Njå et al, 2020). Opplæring relatert til cybersikkerhet er et tiltak for å redusere menneskelige sårbarheter og fungerer på denne måten som tiltak for å nå sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet (Malmedal, 2020). Opplæring kan gjøre at ansatte utvikler ferdigheter som kan være med på å styrke cybersikkerheten i bedriften, og anses som spesielt viktig da mangel på kunnskap og bevissthet er den største trusselen mot cybersikkerhet (Daler et al., 2019). En velfungerende opplæring har potensial for å øke sikkerhetskulturen i en virksomhet, noe som blir ansett som nødvendig innen cybersikkerhetsarbeidet, ettersom trusselbildet er i stadig endring og utgjør en stor risiko (Malmedal, 2020). Malmedal sier videre at virksomheter som over tid nedprioriterer sikkerhetsstyring relatert til cyberhendelser, øker sannsynligheten for at noe risikofylt kan skje.

2.2 Sikkerhetskultur

Vi har over presentert sikkerhetsstyringsteori som viser at opplæring av ansatte kan fungere som tiltak for å hindre cyberangrep. Som nevnt, beskriver Malmedal (2020) at opplæring har potensial for å øke sikkerhetskulturen i en virksomhet. Da opplærings påvirkning av digital sikkerhetskultur er kjernen i vår problemstilling, anser vi det som nyttig å presentere teori om sikkerhetskultur. Her vil både teori om organisasjonskultur, sikkerhetskultur og digital sikkerhetskultur presenteres. Dette gjør vi på bakgrunn av Malmedals (2020) argument om at de ulike kulturteoriene henger sammen. Det vil videre bli presentert teori om hvorvidt sikkerhetskultur kan styres. Dette anses som relevant for å besvare problemstillingen, da opplæring er et sikkerhetsstyrende tiltak som kan brukes for å påvirke sikkerhetskulturen.

Begrepet sikkerhetskultur har sitt utspring fra forskningen på organisasjonskultur (Antonsen, 2009a). Edgar Schein var i sin bok "Organisatorisk kultur og lederskap" (1985) tidlig ute med å beskrive organisasjonskultur. Schein beskriver organisasjonskultur som et stabilt, konstruert og flerdimensjonalt sett med antagelser, verdier og atferd i en organisasjon. Organisasjonskulturen beskytter ansatte mot det ukjente og uønskede da det skaper regelmessigheter i atferd (Schein, 1985). Ved å knytte begrepene organisasjonskultur og sikkerhet sammen, muliggjør det studier av sikkerhetskulturen i en organisasjon (Engen et al, 2021).

Det er en rekke forskere som har forsøkt å definere begrepet sikkerhetskultur. Innen forskningsfeltet finner man et spekter av ulike forståelser, og en viss uklarhet rundt begrepet sikkerhetskultur (Cooper, 2016; Edwards et al., 2013; Guldenmund, 2018; Haukelid, 2008; Hopkins, 2016; Le Coze, 2019). Blant annet vektlegger Cox & Cox (1991) holdninger, tro, oppfatninger og verdier i sin definisjon om sikkerhetskultur, mens Richter og Koch derimot vektlegger betydning, erfaring og tolkning. Videre har andre vektlagt konsensuelle verdier, tro og atferd i forhold til risiko og sikker atferd (Henriqson et al, 2014). Dette synliggjør ulike tolkninger av begrepet sikkerhetskultur. Det eksisterer likevel fellesmomenter innenfor de ulike forståelsene, som vi mener kommer frem i Reasons definisjon. Vi har på bakgrunn av dette valgt å benytte Reasons (1997, s.194) definisjon på sikkerhetskultur i denne oppgaven. Denne definisjonen vektlegger holdninger, verdier, kompetanse og atferd hos individer og grupper innad i en organisasjon:

"The safety culture of an organization is the product of individual and group values, attitudes, competencies, and patterns of behavior that determine the commitment to, and the style of proficiency of, an organization's health and safety programmes. Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety, and by confidence in the efficacy of preventative measures".

2.2.1 Sikkerhetskultur som del av organisasjonskulturen

Grunnet sprikende meninger innen forskning om sikkerhetskultur, kan det være hensiktsmessig å presentere de to ledende perspektivene innen organisasjonskultur, og relatere det til sikkerhet. De to perspektivene er funksjonalistiske og fortolkende. De ulike perspektivene har ulikt syn på hvorvidt en kultur kan styres, og som nevnt er dette relevant for vurdering av hvorvidt digital opplæring kan påvirke sikkerhetskulturen.

Det funksjonalistiske perspektivet baserer seg på en ledelsesmessig, instrumentell ovenfra-og-ned tilnærming. I dette perspektivet blir kultur sett på som noe en organisasjon *har*, hvor kulturens primære funksjon er å støtte opp under ledelsesideologi, mål og strategier (Huang et al., 2007; Lee & Harrison, 2000). Kulturen formes med andre ord fra sikkerhetsstyringsstrategier utviklet av ledelsen, hvor det eksisterer en forventning om at de blir implementert og overholdt (Nævestad, 2009). Dette kan relateres til en sikkerhetsstyringsstrategi som opplæring. Alvesson (2002) sier at kulturforståelsen er preget av en tanke om at det eksisterer en årsakssammenheng mellom organisasjonskulturen, og atferden, holdningene og resultatene medlemmene i organisasjonen får. Smiricich (1983) forklarer det som et fellesskap med verdier eller sosiale ideer som fører medlemmer av organisasjonen sammen. Med andre ord, handler kulturforståelsen om at samtlige medlemmer i organisasjonen har felles forståelse og felles verdier. Schultz (2004) beskriver det som en kollektiv meningsdannelse som blir skapt i organisasjonen. Det funksjonalistiske perspektivet på kultur er det mest dominerende innenfor organisasjon og sikkerhetsstudier Cooper, 2016; Cox & Flin, 1998; Reason, 1997; Furnham & Gunter, 2015; Harvey et al., 2002; Kono, 1990; Lundberg, 1990).

Det andre perspektivet er fortolkende, og ser på kultur som noe en organisasjon *er* eller *gjør*, og produseres av individer og grupper. Dermed er fortolkende kultur noe som produseres nedenfra-og-opp (Henriqson et al., 2014). I dette perspektivet kan ikke kulturen karakteriseres eller endres ved generiske egenskaper og tiltak, som eksempelvis opplæring (Alvesson, 2002). Ethvert forsøk ledelsen gjør for å "raskt" endre kulturen, vil mislykkes, etter som det ikke er ledelsen som skaper kulturen, men medlemmene (Haukelid, 2008). Dette underbygges av Alvesson (2002) som sier at kultur ikke kan styres, den vokser frem gjennom orientering om forståelser og meningsinnhold. Alvesson argumenterer videre for at organisasjonskultur vil

være påvirket av ulike aktørers kjønn, yrke, alder, etnisitet og nasjonalitet. Dette poenget kan sees i sammenheng med teori om subkultur.

Det kan eksistere flere ulike kulturer i en organisasjon, og de kalles gjerne subkulturer (Kaufmann & Kaufmann, 1996; Bang, 1995; Schein, 1984). Flere subkulturer utgjør til sammen en storkultur, eller en organisasjonskultur. Innad i hver subkultur deler de gjerne felles normer, verdier og virkelighetsoppfatninger, og etablerer på denne måten en egen kultur. Bang (2011) sier at subkulturer gjerne etableres mellom personer som har delt erfaringer eller jobber tett sammen, eksempelvis i en avdeling eller et team. I tillegg beskriver Bang (2011) at faktorer som alder, kjønn og utdannelse kan forsterke subkulturen, ved at de opparbeider seg felles normer, verdier og virkelighetsoppfatninger. Det kan oppstå utfordringer når det eksisterer flere subkulturer, hvor det eksempelvis kan oppstå motarbeidende krefter mot ledelsens sikkerhetsstyringsmål og verdier (Haukelid, 2001).

2.3 Sammenhengen mellom læring og sikkerhetskultur

Som teorien presentert hittil viser, kan det diskuteres hvorvidt sikkerhetstiltaket opplæring har mulighet til å endre eller påvirke sikkerhetskultur i en organisasjon. Her vil vi presentere teori som viser at det foreligger en sammenheng mellom opplæring og sikkerhetskultur, og at formuleringen av problemstillingen vår dermed er nyttig å studere. Forskningen som presenteres her vil legge grunnlag for at opplæring kan påvirke sikkerhetskultur.

Både Cheng og Wang (2022), Alshaikh (2020), van Niekerk & von Solms (2005) og Alnatheer et al., (2012) har kartlagt hvilke nøkkelelementer som er nyttig for virksomheter å arbeide med for å bygge sikkerhetskultur, hvorav opplærings- og bevisstgjøringsarbeid av de ansatte er trukket frem som sentralt. Dette samsvarer med en studie gjennomført av Sas et al. (2021) som viste hvordan opplæring påvirket kunnskap, holdning, atferd og egenvurdert nivå av bevissthet rundt cybersikkerhet. Parsons et al. (2015) og Wiley et al. (2020) sine studier viser korrelasjon mellom sikkerhetskultur og bevisstgjøringsarbeid om cybersikkerhet. Parsons et al. (2015) viser videre at ansatte i virksomheter med bedre sikkerhetskultur hadde mer kunnskap, bedre holdninger og adferd som førte til bedre utførelse av cybersikkerhetsarbeid, noe som støttes av funnene i D'Arcy og Greene (2014). Hagen et al. (2008) har i sin studie kartlagt organisatoriske cybersikkerhetstiltak og vurdert effekten av disse tiltakene. Funnene viser at organisatoriske cybersikkerhetstiltak kan deles i fire grupper, hvorav bevisstgjøring og opplæring er det mest

effektive tiltaket. Dette samsvarer med funn fra Johnson (2006) som i sin artikkel skriver at opplæring av ansatte er det beste sikkerhetstiltaket en organisasjon kan ha.

Forskningen som er presentert over, viser en klar sammenheng mellom opplæring og sikkerhetskultur. Dette samsvarer med LaFrancés definisjon av sikringskultur:

"*Security culture is the logical result of a well-driven security awareness program. Once people become aware of threats it is in their nature to react to it. Motivated people want to solve a problem if they feel concerned about it*" (oversatt og referert i Talbot & Jakeman, 2009, s. 37).

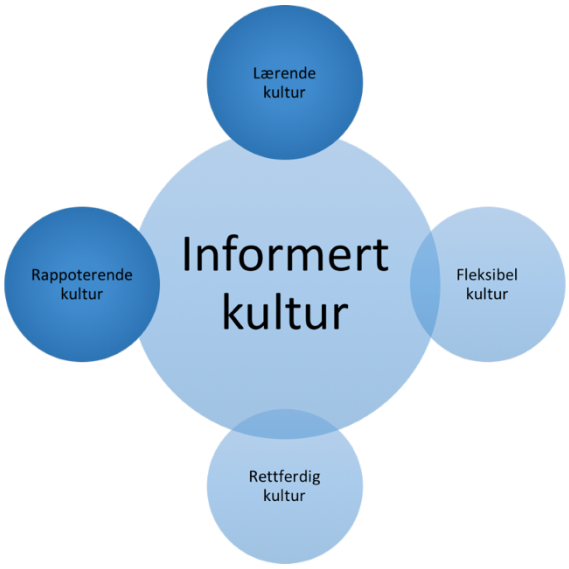
Definisjonen vektlegger at opplæring og bevisstgjøring kan ha direkte innvirkning på menneskers motivasjon for å motvirke sikkerhetsproblemet, som igjen påvirker sikkerhetskulturen. Definisjonen vektlegger at virksomheten har oppnådd en sikkerhetskultur når ansatte viser bevissthet og har motivasjon til å arbeide mot truslene, eller løse utfordringene de står ovenfor.

2.4 James Reason – Sikkerhetskultur

James Reason (1997) er en etablert teoretiker innen sikkerhetskultur. Som vist tidligere vektlegger definisjonen hans verdier, holdninger, kompetanse og atferd på individ- og gruppenivå innad i organisasjonen. Reason argumenterer for at sikkerhetskultur kan implementeres i organisasjoner ved inkludering av sentrale faktorer, og er et nøkkelelement for å drive effektiv og velfungerende sikkerhetsstyring. Teorien til Reason har dermed likhetstrekk med den funksjonalistiske tilnærmingen av kultur. Reason (1997) løfter frem at sikkerhetskultur bør eksistere hos alle involverte aktører, for å nå et høyere nivå av sikkerhet. En god sikkerhetskultur er kjennetegnet av felles oppfatning av sikkerhet og tiltro til organisasjonens sikkerhetsmål (Reason, 1997). Det som kan være noe av utfordringen med sikkerhetsarbeid, er at det er lite synlig frem til en eventuell ulykke oppstår. Med andre ord blir en sikkerhetskultur heller synlig ved sitt fravær, enn tilstedeværelse (Reason, 1997).

Reason hevder at organisasjonen må ha en informert kultur for å oppnå god sikkerhetskultur. En informert kultur kan redusere sjansen for organisatoriske ulykker og uønskede hendelser (Reason, 1997). Ettersom cyberangrep er en uønsket hendelse som potensielt kan ha store

konsekvenser for både drift, forsyningssikkerhet og sensitiv informasjon om nettselskapet, kan denne hendelsen ses i sammenheng med Reasons teori. De fire komponentene innen informert kultur er: rapporterende-, rettferdig-, fleksibel- og lærende kultur. Disse momentene overlapper hverandre i stor grad, men i denne oppgaven velger vi ut to av momentene ettersom de anses som relevant for problemstillingen. Hovedfokuset vil ligge på den lærende kulturen, men rapporterende kultur vil også kort beskrives grunnet dens relevans knyttet til ønsket atferd innen cybersikkerhet.



Figur 2: Informert kultur (Reason, 1997)

Det å være en lærende kultur vil si at organisasjonen legger til rette for læring og kompetanseheving. Denne tilretteleggingen må skje fra ledelsesnivå, og gjør det mulig for medlemmene å ha kompetanse til å trekke riktige konklusjoner. I tillegg må organisasjonen og medlemmene ha vilje til å implementere nødvendige endringer ved behov. Det er sentralt i en lærende kultur at de ansatte viser ønske og vilje til å tilegne seg økt kompetanse (Reason, 1997). Dette poenget kan ses i relasjon til cybersikkerhet, hvor det er sentralt at virksomheter og medlemmene må drive kontinuerlig læring for å holde seg oppdatert, slik at de kan sikre seg mot cyberangrep (Bergsjø, 2020). Ved fravær av uønskede hendelser mener Reason at det er viktig å informere om ulykker og nesten-ulykker som har rammet andre organisasjoner, for å opprettholde respekten for og det proaktive arbeidet mot truslene som kan ramme organisasjonen (Reason, 1997).

En *rapporterende kultur* handler om at organisasjonen bør ha et system som gjør det enkelt å registrere og rapportere meldinger om feil eller nesten-ulykker. Dette samsvarer med det Bergsjø (2020) beskriver om at ansatte i virksomheten må vite hvem og hvordan de skal ta kontakt med relevant personell ved mistanke om et cyberangrep.

2.5 High Reliability Organization

High Reliability Organizations (HRO) er organisasjoner som beskrives som høyteknologiske, hvor alvorlige ulykker og hendelser sjeldent skjer grunnet deres sikkerhetsfokus (Engen et al., 2021). Om nettselskaper kan kategoriseres som komplekst, høyteknologisk system kan muligens diskuteres, men nettselskap er system som benytter teknologi for å holde den kritiske samfunnsfunksjonen, strømleveranse, oppe og gå til enhver tid. Basert på dette, kan nettselskapets cybersikkerhetsarbeid ses i sammenheng med HRO. I denne oppgaven er HRO relevant ettersom teorien vektlegger kontinuerlig sikkerhetsarbeid for å bygge kunnskap, kompetanse og sikkerhetskultur.

Teorien om High Reliability Organizations (HRO) er utviklet av en rekke forskere ved Universitetet i Berkeley (LaPorte, 1996; Rochlin, 1993; Weick et al., 1999). HRO-teorien tar utgangspunkt i at verden og fremtiden er uforutsigbar, men at selv komplekse, høyteknologiske system kan forhindre ulykker ved rett fokus, organisering og prioritet i systemet (La Porte, 1996; Weick et al., 1999). Komplekse og høyteknologiske organisasjoner har ikke råd til å gjøre feil, da eventuelle feil kan føre til stopp i funksjon eller store ødeleggelser. Dette kan ses i sammenheng med at et cyberangrep på et nettselskap har potensialet for å føre til store konsekvenser. Det er viktig å påpeke at HRO-virksomheter ikke er feilfrie. Det er heller sånn at en velfungerende organisering kan føre til at feil oppdages før det får fatale konsekvenser (Weick & Sutcliffe, 2007).

La Porte (1996) har beskrevet kulturen i HRO-virksomheter og hvordan den kan relateres til sikkerhet. De ansatte i virksomheten prioriterer sikkerhet og viser egenansvar for at sikkerhet

skal ha høy prioritet. Tanken bak teorien er at de alle ansatte skal være årvåkne, ha god situasjonsforståelse og hands-on kunnskap som gjør dem kompetent til å oppdage situasjoner når de oppstår (La Porte, 1996). De har en felles tanke hvor det å oppdage feil er nødvendig for å forhindre ulykker. For å etablere den felles forståelsen av sikkerhet, er det nødvendig å drive kontinuerlig læring, både på organisasjonsnivå og på ansattnivå. Weick & Sutcliffe (2007) sier at kontinuerlig læring er et sentralt kjennetegn ved sikkerhetskulturen i HRO-virksomheter. La Porte (1996) sier videre at kompetanse i alle ledd er nødvendig for å effektivt forhindre ulykker, og at det kan knytte sterkere bånd til ledelsen. Dette kan ses i sammenheng med teori om cybersikkerhet, hvor Bergsjø (2020) beskriver at ansatte er en viktig brikke for å oppdage eventuelle cyberhendelser, og at det må være klare rutiner for hvem de skal kontakte oppover i systemet ved et eventuelt angrep.

2.6 NorSIS - Digital sikkerhetskultur

Vi har tidligere i oppgaven presentert mye brukte og godt etablerte organisasjons- og sikkerhetskultursteorier. Disse teoriene er sentrale innen sikkerhetsfaget og vektlegger læring, men er noe eldre og handler ikke spesifikt om cybersikkerhet. Dermed er det nyttig å benytte teori om digital sikkerhetskultur for å spisse fokuset mot temaet og problemstillingens formulering (Malmedal, 2020).

Rapporten Nordmenn og digital sikkerhetskultur (NorSIS, 2019) hadde som mål å beskrive og kartlegge digital sikkerhetskultur i Norge, og rapporten ble utarbeidet på oppdrag fra Justis- og beredskapsdepartementet (Malmedal, 2020). NorSIS sin teori om digital sikkerhetskultur er også beskrevet i boken "Digital sikkerhet" av Bergsjø et al (2020). NorSIS (2019) identifiserer åtte kjernefaktorer som til sammen utgjør digital sikkerhetskultur. De åtte faktorene dekker et vidt spekter, hvorav alt fra offentlig styring og individuell kompetanse er påvirkende dimensjoner. Som modellen under viser, er de åtte aktuelle faktorene: styring og kontroll, tillit, vilje til digitalisering, risikoforståelse, kompetanse, interesse, atferd og fellesskap.

Figur 3: Faktorer som påvirker digital sikkerhetskultur (NorSIS, 2019)

Som beskrevet tidligere i oppgaven, er det en bred forskningsbasert enighet om at opplæring er viktig for sikkerhetskulturen. Dette samsvarer med NorSIS sin teori hvor det beskrives at kompetanse, læring og risikoforståelse er nært knyttet sammen (2019). NorSIS (2019) skriver at faktorene kompetanse, atferd, risikooppfattelse og interesse er relevante for læring, og er dermed det som vektlegges videre i denne oppgaven. Underveis i gjennomgangen av de ulike momentene av teorien, vil vi trekke inn teori som underbygger opplæringens mulighet til å påvirke momentene. Dette mener vi vil få frem NorSIS sitt poeng om at momentene er relevant for læring.

2.6.1 Kompetanse:

Ifølge NorSIS (2019) har man et sett med ferdigheter for å benytte teknologi, og de henger sammen med kompetansen man har på feltet. Det en blir opplært til å gjøre påvirker kompetansen, som igjen har følger for hvordan kulturen former seg. Bergsjø et al (2020) vektlegger at virksomheter bør være oppmerksomme på hvor ansatte får informasjon om cybersikkerhet, for å sikre at det er pålitelig informasjon. En er avhengig av å hyppig oppdatere

kompetansen for å opprettholde et sikkerhetsnivå som følger den digitale utviklingen (NorSIS, 2019).

Filstad (2016) har beskrevet skillet mellom kunnskap og kompetanse. Kunnskap er en individuell, sosial og kulturell prosess hvor en tilegner seg informasjon gjennom læring som kan videreutvikles i praksis. Det er når kunnskap blir anvendt i praksis at den kan kalles *kompetanse* (Filstad, 2016). Sett i sammenheng med opplæring innen cybersikkerhet, betyr dette at de ansatte først får utbytte av kunnskapen når de på en selvstendig måte kan anvende den i praktisk arbeid. Til sammen utgjør både kunnskap og kompetanse nødvendige forutsetninger for kompetanseutvikling og bevisstgjøring (Filstad, 2016). På bakgrunn av dette er det dermed noe virksomheter bør ta stilling til i bevisstgjøringsarbeid om cybersikkerhet.

2.6.2 Atferd:

Som nevnt under beskrivelsen av kompetanse, fører gjerne økt kompetanse til endrede handlinger i praksis. Flere forfattere har beskrevet hvordan bevisstgjøring kan være en sentral faktor for å endre atferd (Hopkins, 2002; Borys et al, 2009; Roer, 2015). Ifølge Bergsjø (2020) handler atferd relatert til digital sikkerhetskultur om hvilke type atferd ledelsen oppfordrer til, og hva man advarer mot. Et viktig moment her er at rådene endres hyppig etter hvert som digitale tjenester utvikles, noe som krever kontinuerlig oppdatering. Relatert til opplæring, handler det om forebyggende tiltak som å følge gjeldende anbefalinger, samt være bevisst og årvåken hvis det oppstår tegn til trussel. Broys et al (2009) underbygger at bevisstgjøring kan føre til endret atferd hvor ansatte blir mer oppmerksomme og årvåkne mot risikoen. I tillegg argumenterer Hopkins (2002) for at bevisstgjøringen kan føre til økt rapportering, og gjør ansatte mer rustet til å komme med innspill for å bedre sikkerheten. I cybersikkerhetsarbeidet er virksomheter avhengige av ansattes evne til å rapportere raskest mulig ved mistanke om cyberangrep, for å begrense skadeomfanget (Bergsjø, 2020; Malmedal, 2020).

2.6.3 Risikoforståelse:

Risikoforståelse, eller risikopersepsjon, er sentralt innen digital sikkerhetskultur ettersom det handler om hvordan hver enkelt vurderer og oppfatter en risiko som cybertrusler. Dette er i stor grad subjektivt, men spiller likevel en rolle som kan ha direkte påvirkning på tanker og handling, som igjen spiller en rolle for kulturen (NorSIS, 2019). En vanlig metode for å gi ansatte innblikk i risikoer som eksisterer på arbeidsplassen, er ved å drive opplæring (Veccio-

Sudus & Griffiths, 2004). Dette samsvarer med Renn (2008) som sier at risikopersepsjonen er i konstant endring gjennom å svekkes eller forsterkes gjennom læring. Mearns og Flin (1995) sier at økt bevissthet omkring risiko, kan føre til større varsomhet i utførelsen av arbeidet og redusere sannsynligheten for at uønskede hendelser og ulykker oppstår. Mearns og Flin (1995) beskriver risikopersepsjon som enkeltmenneskets vurdering av risiko. Den subjektive risikopersepsjonen blir påvirket av hvor godt individet kjenner til risikoens eksistens, og at den kan oppstå. Videre beskriver teoretikerne at risikopersepsjonen henger sammen med kunnskapen og kompetansen man har om temaet, og at den spiller en direkte rolle for hvilke adferdsmønster og holdninger en får. En svak kjennskap til risikoen kan dermed være med på å skape negative holdninger, og større sannsynlighet for å bryte med gjeldende anbefalinger og regelverk (Mearns & Flin, 1995).

2.6.4 Interesse:

Ifølge NorSIS (2019) former interesse både holdninger, ferdigheter og kunnskap. Interesse skaper bevissthet og nysgjerrighet rundt temaet, og fører dermed til at man ønsker å sette av tid til det. På den måten er interesse et nøkkelelement i all læring. Et sentralt element i opplæringen er dermed å skape interesse, som igjen vil ha en direkte påvirkning på den totale digitale sikkerhetskulturen (NorSIS, 2019). Dette samsvarer med Lafrancé (2004, i Talbot & Jakeman, 2009) som argumenterer for at sikkerhetskultur er avhengig av motiverte personer som ønsker å jobbe mot et problem, og at dette skapes gjennom et veldrevet opplæringsprogram. NorSIS (2019) mener at de som er interessert i temaet, har en bedre forutsetning for å lære enn de uten tilsvarende interesse. På denne måten kan en si at interessen er sentral for å gjennomføre og få utbytte av opplæring.

2.7 Sikkerhetsklima

Studier av kultur er ansett som krevende å gjennomføre, ettersom en trenger ulike tilnærmingsformer for å virkelig få innsikt i medlemmers verdier, oppfatninger, meninger og symboler (Engen et al, 2021; Alvesson, 2002). Vi velger derfor å presentere teori om sikkerhetskultur og sikkerhetsklima, da dette gir mulighet til å diskutere hvilken innsikt oppgavens empiri gir.

Schein (2010) illustrerer organisasjonskultur gjennom tre ulike lag. Det ytterste laget handler om artefakter, det mellomste laget består av uttrykte verdier og holdninger, mens det innerste laget består av meningssystem, oppfatninger og forståelser. Antonsen (2009b) sier at de ulike lagene i Scheins modell, er i ulik grad synlig for forsker. Ifølge Schein (2010) handler meningssystem, oppfatninger og forståelser, som er det innerste laget i modellen, om felles antagelser som eksisterer i en sosial enhet. Det mellomste og ytterste laget er synlige og overflatiske uttrykk i kulturen, samt uttrykte oppfatninger om sikkerhet i organisasjonen. Dette gjøres gjerne gjennom å kartlegge meninger knyttet til sikkerhet hos medlemmene.

Figur 4: Ulike lag av organisasjonskultur (Schein, 2010)

Schein (2010) uttrykker skepsis til å kunne si noe om kulturen ved å bare undersøke det mellomste og ytterste laget, ettersom selve kjernen i kulturen eksisterer i det innerste nivået. Det innerste nivået må undersøkes ved å studere kulturen på et dypere nivå enn uttrykte verdier. Dette samsvarer med Engen et al (2021) sin påstand om at kultur må studeres gjennom diskurser, symboler og meninger.

Reichers & Schneider (1990) har studert utviklingen av sikkerhetskultur og sikkerhetsklima og sier «culture exists on a higher level of abstraction than climate, and climate is a manifestation of cuture». Flin et al (2000) sier at sikkerhetsklima kan betraktes som et «øyeblikksbilde» av sikkerhetsrelaterte aspekter i organisasjonskulturen. Sikkerhetsklima kan med denne forståelsen, ses på som et øyeblikksbilde som gir en indikasjon på

sikkerhetskulturen i en organisasjon, men kan ikke gi beskrivelser som er like grundige som kultur. Ved undersøkelser av sikkerhetskultur gjennom spørreundersøkelser, er det mer hensiktsmessig å bruke begrepet sikkerhetsklima, argumenterer Pidgeon (1998). Likevel viser studien Teo & Feng (2008) at sikkerhetsklima har en påvirkning innen sikkerhetskultursdimensjonen atferd. Dette underbygger Reichers & Schneider (1990) poeng om at sikkerhetsklima kan si noe om sikkerhetskultur.

Del 2: Teorier om læring

Hittil har vi presentert teori om organisasjons- sikkerhets- og digital sikkerhetskultur, og forskning som viser til at det foreligger en sammenheng mellom læring og sikkerhetskultur. Under teori om digital sikkerhetskultur har vi presentert hvordan opplæring har potensial for å styrke de ulike momentene som er relevante for læring. Ettersom problemstillingen tar for seg hvordan digital opplæring påvirker den digitale sikkerhetskulturen, er det nødvendig å presentere ytterligere teori om læring. Da oppgaven tar for seg spesifikt digital opplæring som læringsmetode, velger vi å presentere teori om dette først.

2.8 Digital opplæring

Som beskrevet i innledningen er elektronisk læring en av de mest benyttede læringsmetodene for kompetanseheving innenfor cybersikkerhetsarbeidet (NSR, 2022). Som nevnt i innledningen, er kompetansen ofte er noe mangelfull knyttet til cybersikkerhet. Vi ønsket derfor å studere om det kunne knyttes til opplæringsmetoden. Vi skal i det følgende presentere teori om hva digital opplæring er, for å kunne studere temaet videre. Vi gjør igjen oppmerksom på at digital opplæring er et videre begrep enn elektronisk læring, og omfatter all læring som foregår ved bruk av teknologi (Basak et al, 2018). På bakgrunn av dette skiller vi ikke videre mellom begrepene.

Digital opplæring er en mye benyttet form for læring på arbeidsplasser, og er en form for fjernundervisning som muliggjør gjennomføring av læring uten fysisk deltakelse. Datateknologi har gjort det mulig for deltakere å få informasjon når de selv har tid og mulighet til å gjennomføre det (Katz, 2000). Læringsinnholdet består gjerne av ren tekst eller

videoinnhold med instruktør eller visuelle effekter (Katz, 2000). Utviklingen av digitale tjenester og elektronisk kommunikasjon har fjernet barrierer som tid og rom. Dette har gjort det mulig å innhente og levere kunnskap når som helst og hvor som helst (Horton, 2000).

Welsh et al (2022) har beskrevet ulike fordeler ved bruk av digital opplæring. Det muliggjør opplæring på tvers av ulike lokasjoner, og er ansett som en mer effektiv opplæringsform sammenlignet med eksempelvis klasseromsundervisning. Fordeler ved effektivitet kan direkte relateres til sparing innen økonomi og tid. Andre fordeler ved bruk av digital læring er muligheten til å spore brukerens aktivitet, og om mottaker har mestret og forstått innholdet. Dette kan eksempelvis gjøres ved å benytte quizresultater (Welsh et al.,2022).

Det finnes to ulike former for digital opplæring: synkron og asynkron. Førstnevnte gjennomføres gjerne som personlig deltakelse i sanntid gjennom chat eller videokonferanser. Mesteparten av digital opplæring som benyttes i virksomheter er asykron. Dette er digital opplæring som er innspilt på forhånd, er tilgjengelig på alle døgnets tider og kan gjennomføres fra hvilket som helst sted (Rosenberg, 2001). Asynkron digital læring gjennomføres ofte ved bruk av innspilte videosnutter og informasjonstekster. Denne formen er gjerne lettere å gjennomføre når en har tid, og muliggjør læring med refleksjon i større grad (Hrastinski, 2008). Synkron læring er mindre vanlig å benytte. Innenfor disse formene av digital læring finner en ulik grad av utforminger. En mindre avansert asynkron digital læringsmetodikk består gjerne av enkle lysbilder, mens en mer avansert metode benytter gjerne animasjon, video og lydkomponenter (Hall, 1997).

I en studie gjennomført av Hagen og Albrechtsen (2009) fant de at digitale læringskurs økte de ansattes kunnskap, holdning og atferd knyttet til cybersikkerhet. På tross av fordelene med digital opplæring, kan det virke som enkelte digitale opplæringsmetoder også har sine begrensninger. Skotnes (2014) trekker blant annet frem i sin studie at digitale enveiskommunikasjons-verktøy, som informasjonsplansjer og informasjon på e-post, ofte fører til at mottaker av opplæringen mangler motivasjon og bevissthet til å holde ved like kunnskapen. Dette viser uenighet om hvorvidt digital opplæring kan påvirke bevissthet knyttet til cybersikkerhet.

2.9 Læring

Som presentert over, er digital opplæring en mye benyttet opplæringsmetode i virksomheter, og er den opplæringsmetoden som benyttes i nettselskapet som skal studeres i denne oppgaven. Som beskrevet er målet med opplæring relatert til cybersikkerhet å øke kompetansen slik at de blir årvåkne, bevisste og utfører rapportering. Videre vil det være nødvendig å presentere teori om læring for å få inngående forståelse om målet med opplæring, og hvordan virksomheter bør tilrettelegge sin opplæring for å oppnå størst læringsutbytte.

Læring kan defineres som «tilegnelse av ny eller endret kompetanse – i form av kunnskaper, ferdigheter eller holdninger – som gir relativt varige endringer i en persons atferdspotensial» (Lai, 2013, s. 119). Definisjonen legger vekt på at læring kan føre til endret kompetanse, som også kan komme til uttrykk gjennom ens handlinger. Ifølge Filstad (2010) kan læring være av både formell og uformell karakter, hvorav formell gjerne skjer ved at ledelsen organiserer kurs, trening eller klasseromsundervisning. Denne læringsformen handler i korte trekk om at den som lærer får presentert informasjon og kunnskap fra en annen part gjennom et strukturert læringsopplegg. Målet med formell læring er at en gruppe skal få felles forståelse, samt legge grunnlag for et kollektivt, standardisert handlingsmønster under bestemte hendelser og situasjoner. Uformell læring skjer gjerne gjennom sosial interaksjon mellom kollegaer i praktisk arbeid, og skjer dermed uten fast struktur eller målsetting (Filstad, 2010, 2017). Denne oppgaven vil ha hovedfokus på formell læring, da vi ser på digital opplæring som nettselskapet benytter for å lære opp de ansatte.

Ifølge Filstad (2016) er en gunstig læringsmetodikk å kombinere forklaring, med mulighet for selvstendig, praktisk utførelse. Dette samsvarer med Olsens (2016) argument om at læring ikke bare handler om individuell kunnskapstilegnelse, men også om interaksjon og aktiv deltakelse. På en arbeidsplass er det viktig at både de ansatte benytter seg av læringsmulighetene de blir tilbudt, og at arbeidsplassen tilrettelegger for læring (Filstad, 2010). Ettersom fomell læring ønsker å oppnå en felles forståelse og kollektivt handlingsmønster, kan teori om felles læring trekkes inn. For at en organisasjon skal oppnå felles læring, er individuell læring helt sentralt, men det er viktig at læringen ikke stopper på individuelt nivå, ettersom felles læring krever mer (Jacobsen og Thorsvik, 2016). Jacobsen og Thorsvik argumenterer videre for at felles læring

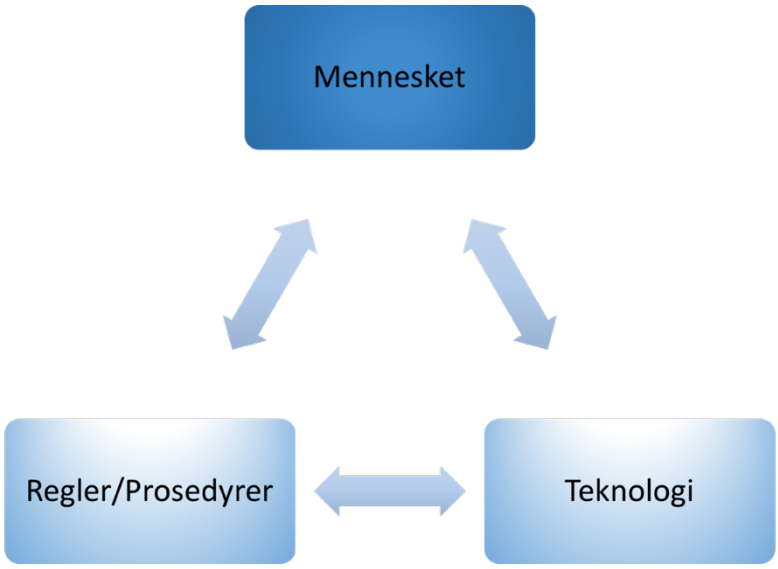
starter når individet formidler den nye kunnskapen og kompetansen til andre i organisasjonen. Dermed oppstår det en felles enighet om å endre hvordan man praktiserer arbeidet.

Formell læring har også sine begrensninger. Blant annet argumenterer Bednall & Sanders (2016) for at en svakhet med formell læring er at læringen skjer i en situasjon som ikke er lik arbeidssituasjonen. Det kan dermed ta tid å få alle ansatte til å implementere den i sin arbeidshverdag. Dette kan relateres til Tennants (1999) argument om at opplæringen ofte er for generell, og dermed ikke kan overføres direkte til de ulike hendelsene en kan møte på. Det er dermed en svakhet at mange tror at opplæringen kan overføres til et mangfold av situasjoner, ifølge Tennant.

2.10 Kai Roer - Opplæring og sikringskultur

Under læringsteoriene har det blitt presentert teori knyttet til generell læring og digital opplæring, men uten direkte tilknytning til temaet cybersikkerhet. Videre vil det derfor være nyttig å løfte frem Kai Roer (2015) som har forsket på bevisstgjøring og opplæring innen cybersikkerhet. Han knytter også opplæringsteorien direkte til påvirkning av sikringskultur, noe som anses som svært relevant for å kunne besvare problemstillingen om hvordan digital opplæring påvirker digital sikkerhetskultur. Før vi går nærmere inn på selve opplæringsteorien, velger vi å beskrive hvordan Roer argumenterer for at bevisstgjøring kan styrke sikringskulturen.

Roer (2015) beskriver hvordan sikringskulturen dannes og endres i en organisasjon via tre elementer: mennesker, regler/prosedyrer og teknologi. Disse tre elementene er både avhengige av, og påvirker hverandre. Roer (2015) hevder at endring i et av elementene, vil føre til endring i den helhetlige sikringskulturen. Til tross for at disse tre elementene utgjør en helhetlig sikringskultur, velger vi i denne oppgaven å fokusere på elementet "*mennesket"* ettersom det anses som relevant for problemstillingen. Innenfor elementet "mennesket" finner man bevisstgjørings- og opplæringsarbeid. Bevissthet og kompetanse er avgjørende faktorer for at ansatte skal gjøre det rette for å styrke cybersikkerheten, og kan dermed være viktige element for å bygge sikringskultur (Roer, 2015). Det er viktig å belyse Roers poeng om at security-bevissthet og sikringskultur ikke er det samme, da kultur er mer enn bare bevissthet.



Figur 5: Faktorer som påvirker sikringskultur (Roer, 2015)

Ifølge Roer (2015) finnes det ingen felles definisjon på hva security-bevisstgjøring er, men han har valgt å definere det som "Knowledge or perception of a situation or fact". Med dette menes det at sikkerheten kan øke ved å ha evne til å bruke rett kunnskap, og til å anvende kompetansen i spesifikke situasjoner (Roer, 2015). Security-bevissthet hjelper folk å vite om, og være oppmerksomme på, sikkerhetstruende hendelser som cyberangrep. Det å vite om noe medfører ikke nødvendigvis en atferd som samsvarer med kunnskapen, noe som er målet med opplæring innen cybersikkerhet. Det å vite om problemet er bare ett av trinnene for å endre atferden, ifølge Roer (2015). Roer har på bakgrunn av dette utviklet læringsteorien "Firetrinns kognitiv prosess", som er inspirert av Bandura og Walters (1963). Læringsprosessen består av 1. Oppmerksomhet, 2. Bevaring, 3. Reproduksjon og 4. Motivasjon. Denne teorien er utarbeidet for at organisasjoner kan bygge opp et opplærings- og bevisstgjøringsprogram som øker kunnskapen, blant annet innen cybersikkerhet, til et nivå der den blir anvendt.

Trinn	Beskrivelse
1. Oppmerksomhet	Oppmerksomhet handler om at den som lærer må være til stede, være oppmerksom og interessere seg for det som foregår. Påvirkende faktorer her er den ansatte selv, og innholdet i opplæringen. For å øke oppmerksomheten, vil det være en fordel å gi opplæringen relevans og forklare hvorfor dette er viktig å trene på. Opplæring som stanser på dette nivået, kan kun måle om ansatte har deltatt på kurset.
2. Bevarings-trinnet	Bevarings-trinnet handler om ansattes evne til å holde på den lærte informasjonen. Faktorer som kan hjelpe for å bevare kunnskapen, kan være å skape et miljø som muliggjør enkel læring, samt tilpasse innholdet til den ansattes kunnskap. I tillegg må opplæringen gjentas etter behov. Mennesker lærer på forskjellige måter, og trenger derfor forskjellige tilnærminger for å få utbytte av opplæringen. Security-bevissthetsprogrammer som stanser på dette nivået, vil måle oppmøte og gjenta det samme opplæringsprogrammet med noen intervaller.
3. Reproduksjons-trinnet	Reproduksjonstrinnet handler om å vise at atferden er lært. På dette nivået fører opplæringen til at de ansatte reproduserer den lærte kunnskapen til atferd. De viser at de vet hva de skal gjøre, og hvordan de skal gjøre det. Mange bevisstgjøringsprogrammer stopper på dette nivået, hvor en benytter seg av ferdighetstester, spørreskjemaer og andre kvalitetstester, både under og etter opplæringen.
4. Motivasjon	Det siste trinnet handler om å motivere ansatte til å reprodusere atferden utenfor læringssituasjonen, og dette står arbeidsplassen ansvarlig for å tilrettelegge. Dette kan eksempelvis gjøres ved å tilrettelegge et rapporteringssystem som er lett anvendelig for ansatte. Opplæringen kan her måle atferd på en rekke nivåer. En kan

	se på deltakelse på kurs, samt måle effekten av opplæringen. En kan også måle effekt av atferd på systemene ved hjelp av logger og dataanalyse. Organisasjoner som implementerer opplæring på dette nivået, benytter seg av en strukturell tilnærming til opplæringen som hjelper dem å fokusere og forbedre sikringskulturen i organisasjonen. Dette vil være med på å bygge og opprettholde den sikringskulturen organisasjonen ønsker.

Tabell 2: Firetrinns kognitiv prosess (Roer, 2015)

2.11 Oppsummering av teori

I teorikapittelet har det blitt presentert teori som anses som nyttig for å kunne besvare problemstillingen om hvordan digital opplæring om cybersikkerhet påvirker digital sikkerhetskultur i et nettselskap. Det har blitt presentert ulike sikkerhetskulturteorier med relevans til opplæring som tiltak. Videre har vi presentert digital opplæring, og rundet av teorikapittelet med generell opplæringsteori og opplæring knyttet til cybersikkerhet for å styrke sikkerhetskulturen.

Videre skal metodekapittelet presenteres. Dette vil gi innsikt i hvordan vi valgte å studere temaet hos det aktuelle nettselskapet.

3.0 Metode

I dette kapittelet vil det metodiske grunnlaget for oppgaven bli lagt frem. Gjennom metodedelen vil vi beskrive forskningsdesignet i sin helhet, samt begrunne hvilke metodiske valg vi har tatt underveis for å kunne besvare problemstillingen. I tillegg vil alle ledd i forskningsprosessen bli presentert og forklart. Avslutningsvis vil det også bli lagt frem refleksjon rundt metodisk kvalitet og etiske betraktninger rundt prosjektet.

3.1 Forskningsdesign

Ifølge Yin (2014, s.28) er et forskningsdesign "a logical plan for getting from here to there, where here may be defined at initial set of questions to be answered, and there is some set of conclusions (answers) about these questions". Ut fra denne forståelsen, er det nyttig å presentere vår plan for prosjektet for å kunne svare på problemstillingen. Med andre ord skal vi beskrive hvordan prosessen ble operasjonalisert. Leddene i oppgavens forskningsdesign er illustrert i figuren under (figur 6). I det følgende skal forskningsdesignet forklares i dybden.

Figur 6: Forskningsdesign

3.2 Forskningsmetode

Ifølge Johannessen et al. (2016) er det problemstillingens formulering som må være førende for hvilken metode som passer. Problemstillingen i denne oppgaven er:

> «*Hvordan påvirker digital opplæring om cybersikkerhet den digitale sikkerhetskulturen i et nettselskap?*»

I tillegg har vi valgt ut tre forskningsspørsmål som fungerer som støtte og spesifisering av problemstillingens formål. Det første forskningsspørsmålet retter seg mot hvordan nettselskapet benytter digital opplæring, og hvordan metoden fungerer for å fremme læring. De to andre spørsmålene retter seg mot utbyttet av den digitale opplæringen, og hvordan det kan

relateres til momenter innen teori om digital sikkerhetskultur både på individuelt nivå og gruppenivå.

For å få svar på de aktuelle forskningsspørsmålene var det nødvendig å samle empiri fra både ledelsen og ansatte. Dette gav oss grunnlag for å kunne si noe om digital opplærings påvirkning av læring, læringseffekt og den digitale sikkerhetskulturen i nettselskapet. Det var sentralt å få tak i empiri som kunne si noe mer om den digitale sikkerhetskulturen enn utelukkende på individuelt nivå. Ved å både få tak i empiri fra ledelse og andre ansatte, kunne vi si noe om individuelle og gruppers kultur, noe Reason (1997) vektlegger i sin definisjon av sikkerhetskultur. I forskningsspørsmål to og tre har vi valgt å bare inkludere ansattes effekt av opplæring, sett fra både ledelsen og ansatte sitt perspektiv. Valget om å bare studere ansattes effekt har vi gjort på bakgrunn av at ledelsen er involvert i opplæringsarbeidet, og kan dermed ha en mer positiv innstilling. Ved å utelukke ledelsens egen effekt av opplæringen, vil en trolig gi en mer sann representasjon av den faktiske digitale sikkerhetskulturen i nettselskapet.

På bakgrunn av hva vi ønsket svar på i problemstilling og forskningsspørsmålene, måtte vi finne en forskningsmetode som kunne gi svar på den aktuelle problemstillingen og forskningsspørsmålene. Kvalitativ metode gir mulighet for å innhente dybdekunnskap, noe som fremstår som sentralt i studier av kultur (Johannessen et al, 2016; Schein, 2010; Engen et al, 2021). Dermed fremstod intervju som en passende metode for å studere den digitale sikkerhetskulturen i nettselskapet. Samtidig ville bruk av intervju som datainnsamlingsmetode begrenset muligheten for å studere et større utvalg. Dette ville igjen påvirket vår mulighet til å få funn som kunne vært representative for nettselskapets felles kultur på gruppenivå (Johannessen et al, 2016). Kvantitativ metode gir derimot mulighet til å samle inn større datamengder. Dette gjorde at vi kunne samle inn datamengder fra flere respondenter. Dermed var det nyttig å supplere med kvantitativ metode for å et datamateriale som kunne fortelle mer enn om kulturen på individnivå (Johannessen et al, 2016). Vi kom derfor frem til at det var nødvendig å benytte begge metodene for å besvare oppgavens problemstilling og tilhørende forskningsspørsmål.

Blaike & Priest (2019) argumenterer for at Mixed Methods er en pragmatisk blanding av kvantitative og kvalitative metoder, hvor en kombinerer elementer av kvalitative og kvantitative forskningstilnærminger, med et mål om dybdeforståelse og bekreftelse. Det gir en mulighet for å få innsikt i temaet fra ulike perspektiver. Ifølge Grønmo (2016) kan datainnsamlingen innen Mixed Methods gjennomføres på fire ulike måter, hvor den aktuelle metoden for denne oppgaven er: *kvalitative undersøkelser som forberedelse til kvantitative undersøkelser.* Tanken bak dette valget var at vi først kunne gjennomføre kvalitativ metode ved bruk av intervju for å undersøke ledelsen og superbrukeres beskrivelse av hvilke digitale opplæringsmetoder de benytter i selskapet knyttet til cybersikkerhet. I tillegg kunne de gi dybdebeskrivelser av hvordan de opplever at opplæringen påvirker de ansattes kompetanse, atferd, risikopersepsjon og interesse. Basert på funnene fra ledelsen og superbrukerne, kunne vi samle inn informasjon om hvordan et bredt spekter av ansatte vurderer funnene som kom frem i intervjuene. Ved å benytte Mixed Method kunne vi dermed si noe om dyptgående beskrivelser av opplæringens påvirkning av digital sikkerhetskultur. I tillegg gav metoden mulighet til å undersøke om de ansatte hadde samme forståelse og opplevelse av opplæringens effekt. Dette er sentralt da opplæring innen sikkerhet ikke har en hensikt, med mindre den blir forstått og mottatt av de ansatte (Roer, 2015).

På tross av at Mixed Method har sine styrker, eksisterer det også svakheter ved metoden som vi måtte ta høyde for. Mixed Methods krever blant annet kunnskap og ferdigheter til å mestre flere metoder, og forskningsprosjektene kan ofte bli både tid- og ressurskrevende (DeCuir-Gunby, 2008). Vi vurderte likevel at fordelene ved metoden gav et sterke grunnlag for å svare på problemstillingen, enn ved å bare benytte kvantitativ eller kvalitativ metode alene. I tillegg kunne det bidra til en mer komplett forståelse av temaet, som igjen kan styrke tilliten til konklusjonene (Johannessen et al, 2016). Vi vurderte det også som en styrke at vi var to som gjennomførte prosjektet sammen, da metoden fremstod tid- og ressurskrevende.

3.2.1 Forskningsstrategi

Ifølge Blaikie (2010) handler forskningsstrategi om å bygge opp et sett av prosedyrer for å kunne besvare problemstillingen. Ulike forskningsstrategier som kan benyttes er induktiv, deduktiv, abduktiv og retroduktiv, og de kan benyttes enkeltvis eller i kombinasjon (Blaikie, 2010). Basert på det metodiske valget og temaet for oppgaven, ble det benyttet abduktiv strategi

i forskningsprosjektet. Abduktiv strategi tar utgangspunkt i å tolke et fenomen innenfor et teoretisk rammeverk, og fremstod passende ettersom oppgaven skal studere hvilken påvirkning digital opplæring har på fenomenet digital sikkerhetskultur. Fenomenet sikkerhetskultur fremstår komplekst å studere, og det var dermed hensiktsmessig å benytte seg av en strategi som gav rom for teoretisk forankring. Strategien gir også mulighet for å studere sosiale meninger og motiver fra innsiden, noe som anses som relevant for å få innsikt i ansatte og ledelsens meninger knyttet til digital opplæring og sikkerhetskultur (Blaikie & Priest, 2019). Det ble også benyttet induktiv strategi i forskningsprosjektet. Induktiv strategi kjennetegnes av at vi som forskere er åpne til empiriske funn, og finner teori som passer til empirien som samles inn (Johannessen et al, 2016). Dette var hensiktsmessig i vår studie ettersom vi ønsket å ha en åpen tilnærming til hvordan nettselskapet jobber med digital opplæring innen cybersikkerhet, og hvordan de mener den påvirker den digitale sikkerhetskulturen i selskapet. Ettersom datainnsamlingsmetoden er bygd opp ved å innhente kvalitative data først, for så å studere det kvantitative, kan en argumentere for at det kvantitative arbeidet også er preget av induksjon (Grønmo, 2016). Denne oppgaven benytter seg dermed ikke av den klassiske hypotesetestings-tilnærmingen som kvantitativ forskning ofte gjør (Johannessen et al, 2016). Mixed methods i kombinasjon med induktiv og abduktiv strategi gav rom for fleksibilitet i forskningsprosessen. Det gav mulighet for å justere teoretisk rammeverk, problemstilling og forskningsspørsmål etter hvert som vi fikk mer innsikt i temaet underveis i forskningsprosessen.

3.2.2 Case studie

Studie vårt ble gjennomført som en casestudie. I følge Yin (2014) er casestudie den metoden som er best egnet for dagsaktuelle problemstillinger med forskningsspørsmål av typen «*hvordan» og «hvorfor».* Ettersom problemstillingen vår ser på *hvordan* digital opplæring påvirker den digitale sikkerhetskulturen, vurderte vi metoden som passende.

Styrken med casestudier er at en kan få helhetlig forståelse og inngående kunnskap om et fenomen innen enheten en studerer (Wæhle et al. 2020). Ifølge Johannessen et al (2016) vil casestudie som forskningsdesign ta for seg en eller flere analyseenheter. I dette prosjektet ønsket vi å fokusere på fenomenet opplærings påvirkning på digital sikkerhetskultur i en enhet. Denne enheten var det studerte nettselskapet. Ifølge Johannessen et al. (2016) kan dette beskrives som et *enkelt casedesign* med flere analyseenheter. Dette vil si at man samler

informasjon innenfor en avgrenset kontekst, som i dette tilfellet vil være vanlige ansatte, ledelsen og superbrukere som jobber i nettselskapet. Johannessen et al. (2016) beskriver videre at denne type casedesign er hensiktsmessig hvis forskeren ønsker å avdekke sentrale fenomen og belyse det fra ulike sider, noe som gir mulighet for fyldige beskrivelser av det aktuelle fenomenet.

Yin (2014) argumenterer for at casestudier med fordel kan gjennomføres ved kombinasjon av forskjellige metoder for å skaffe mye og detaljert data, slik vi gjør i denne oppgaven ved bruk av Mixed Methods. Casestudie integreres godt med Mixed Methods, da det gir en mer fullstendig forståelse. Kombinasjonen av disse metodene vil gi oss en mulighet til å belyse nettselskapets opplærings påvirkning av den digitale sikkerhetskultur fra flere ulike vinkler. Ifølge Malterud (2017) styrker en studiens validitet ved å belyse fenomenet fra flere perspektiver.

Grønmo (2016) trekker frem en svakhet med metoden, hvor det vises til vanskeligheter med å generalisere funn ettersom det er utfordrende å utlede generelle betraktninger basert på en studert enhet. I vårt tilfelle kan vi ikke si noe om de andre nettselskapene enn det studerte, noe som legger begrensninger til studiens ytre validitet (Johannessen et al, 2016). Ytre validitet handler om i hvilken grad funn fra en studie kan generaliseres til andre lignende grupper. Casestudiers manglende evne til å generalisere, vil dermed være en svakhet med metoden.

3.3 Utvalg

3.3.1 Utvalg til intervju

Vi startet tidlig med å kontakte ulike nettselskaper av ulik størrelse, og var i dialog med flere av dem. Vi endte med et nettselskap av stor størrelse, noe vi anså som en fordel. Dette da de trolig hadde et bredere spekter av relevante informanter, sammenlignet med et selskap av mindre størrelse. Vi kom i kontakt med en ansatt i det aktuelle selskapet, som siden den dag har vært vår kontaktperson. Kontaktpersonen listet opp relevante kandidater som kunne stille til intervju. Utvalget informanter ble derfor valgt på bakgrunn av et strategisk utvalg. Et strategisk utvalg innebærer at valget av informanter er basert på forhåndsdefinerte kriterier og

relevans (Thaagard, 2018). Dette var nødvendig da vi ønsket å komme i kontakt med personer som jobbet direkte eller indirekte med opplæring omkring cybersikkerhet.

I stor grad består informantene av personell som har ledende stillinger, og hvor opplæring av cybersikkerhet inngår i deres arbeid. Informantene S1, L1 og L4 jobber direkte opp mot opplæring innen cybersikkerhet. De andre informantene er mer indirekte involvert, hvorav enkelte har lederstillinger og noen er superbrukere. De med lederstillinger har et ansvar for å være oppdatert på aktuelle cybertrusler og sikre at de ansatte er bevisstgjort på temaet. I tillegg har de et ansvar for å tilpasse opplæringen etter behov. Superbrukerne består av personer med fagkompetanse innen cybersikkerhet rettet mot spesifikke avdelinger, og har en rådgivende funksjon knyttet til hva opplæringen bør fokusere på og hvordan de ansatte opplever den. Vi argumenterer for at sammensetningen av informanter gir grunnlag for en bred innsikt i temaet i problemstillingen, og at det er en styrke at vi har fått intervju med samtlige aktuelle informanter i nettselskapet. I tabellen under skilles det mellom ledelse (L) og superbrukere (S).

Informant	**Stilling**
L1	Ledelsen
L2	Ledelsen
L3	Ledelsen
L4	Ledelsen
L5	Ledelsen
S1	Superbruker
S2	Superbruker
S3	Superbruker
S4	Superbruker

Tabell 3: Informanter og stilling

3.3.2 Utvalg til spørreundersøkelse

Utvalget til spørreundersøkelsen var også basert på strategisk utvelgelse av ansatte, hvor vår kontaktperson stod for utvelgelsen av respondenter. Kontaktpersonen har en ledende stilling, og dermed en god oversikt over ansatte. Det strategiske utvalget er utført med ønske om å få forskjellige aldersgrupper, ulike arbeidsformer og spredning i ulike avdelinger (Johannessen et al, 2016).

Spørreundersøkelsen ble sendt ut til 100 ansatte, i tillegg til at samtlige av informantene fikk tilsendt samme spørreundersøkelse. Årsaken til at vi sendte ut spørreundersøkelsen til informanter vi allerede hadde intervjuet, var å unngå feiltolkning mellom kvalitative og kvantitative data i de deler av analysen der det var aktuelt. Spørreundersøkelsen til ledelsen og superbrukere ble dermed også valgt på bakgrunn av strategisk utvalg. Totalt var det 66 ansatte som svarte på spørreundersøkelsen, noe som gav en svarprosent på 61,9%. Ifølge Johannessen et al (2016) anses en svarprosent på over 50% som en bra respons.

3.4 Datainnsamling

Datainnsamlingen ble som beskrevet gjennomført ved å først samle inn kvalitative data, for så å benytte funnene til avgrensning for hva vi ønsket å undersøke i den kvantitative datainnsamlingen (Grønmo, 2016).

3.4.1 Kvalitativ datainnsamlingsmetode

Det ble gjennomført dybdeintervju med både ledere og superbrukere i nettselskapet som var involvert i opplæringsarbeidet. Det ble benyttet en semistrukturert intervjuguide, noe som fungerte som støtte for å holde temaet tett opp til problemstillingen (Brinkmann & Tanggaard, 2012). Vi hadde listet opp flere spørsmål som vi anså som relevante for den digitale opplæringen selskapet benytter innen cybersikkerhet, og spørsmålene gav rom for informantenes beskrivelser av hvordan det fungerer for de ansatte, og hvordan det påvirker den digitale sikkerhetskulturen. Ved å benytte en semistrukturert intervjuguide, ga dette fleksibilitet under intervjuet. Vi kunne hoppe mellom spørsmål etter hvert som samtalen foregikk. Dette gjorde at vi kunne være åpne for nytt innhold dersom uventede, men relevante temaer dukket opp (Kvale og Brinkmann, 2015). Intervjuene ble gjennomført på kommunikasjonsplattformen Teams etter informantenes ønske. Ifølge Kvale og Brinkmann (2015) legger kjente atmosfærer til rette for et intervju der informantene lettere kan åpne opp om det aktuelle temaet, og det

anses derfor som en fordel at Teams er en tjeneste informantene er vant til å benytte i arbeidshverdagen. Likevel kunne en ønske at intervjuene ble gjennomført fysisk, da dette trolig ville ha skapt en intervjusetting preget av tillit i økt grad (Jacobsen, 2005).

Før de faktiske intervjuene tok til, gjennomførte vi intervju på både hverandre og andre bekjente for å sikre oss at spørsmålene var forståelige og tilstrekkelig åpne (Kvale & Brinkmann, 2015). Intervjuguiden ble også sendt til kontaktpersonen i nettselskapet for å sikre oss at dette var spørsmål informantene kunne og hadde lov til å svare på. Før intervjuene tok til, fikk de aktuelle informantene informasjon om prosjektet og hva intervjuet skulle omhandle. Gjennom intervjuene ble det benyttet lydopptak etter samtykke fra informantene. Dette anså vi som en fordel for å få flyt i samtalen, for å finne tilbake til informasjonen og benytte direkte sitat i framstilling av funn (Kvale & Brinkmann, 2015). Ettersom vi var to forskere, byttet vi på å lede intervjuene. Når den ene stilte spørsmålene, noterte den andre, og fikk tilføye noen spørsmål på slutten om det skulle være noe som fanget interesse eller ikke ble besvart godt nok. På den måten kunne vi unngå å gå glipp av viktige detaljer som fremkom i intervjuet (Kvale & Brinkmann, 2015). Varigheten av intervjuene varierte fra 20-60 minutt.

3.4.2 Kvantitativ datainnsamlingsmetode

For å få innsikt i ansattes syn på digital opplærings påvirkning av digital sikkerhetskultur, valgte vi å sende ut spørreskjema. Her var det viktig å få svar fra mange respondenter, for å få innsikt i mangfoldet i ansattes meninger. Spørreundersøkelser er en effektiv metode for å samle data fra mange representanter (Johannessen et al, 2016). Ledelsens spørreundersøkelse ble hovedsakelig benyttet for å besvare forskningsspørsmål 1 som tar for seg hvilke digitale opplæringsmetoder de benytter i nettselskapet, og hvordan de tror det fungerer for å fremme læring.

Ettersom prosessen med å lage et spørreskjema av god kvalitet er svært tidkrevende, valgte vi å hente inspirasjon fra Digitaliseringsdirektoratet (u.å) sitt kartleggingsverktøy for måling av digital sikkerhetskultur. Spørreskjemaet er ikke laget med hensikt om å måle digital opplærings påvirkning av digital sikkerhetskultur, så enkelte spørsmål som var lite relevant for opplæring, måtte endres og fjernes. I tillegg la vi til enkelte spørsmål for å tilpasse det til funn fra den

kvalitative datainnsamlingen. De fleste spørsmålene omhandler faktorene kompetanse, atferd, risikopersepsjon og interesse, ettersom det er disse momentene vi har valgt å fokusere på innen digital sikkerhetskultur. Dette var essensielt for at spørreskjemaet kunne gi svar på problemstillingen (Johannessen et al., 2016).

Spørreskjemaene til ansatte og ledelsen ble laget og levert ut gjennom programmet SurveyXact, som Universitet i Stavanger anbefaler i studentprosjekt. Vår kontaktperson i nettselskapet sendte ut link til skjemaet på e-post, og sendte ut to purremeldinger før skjemaet ble stengt av etter en uke. Dette gjaldt både spørreundersøkelsen til de ansatte, og ledelsen og superbrukerne. Ved å la kontaktpersonen sende ut link til spørreundersøkelsen kunne vi lettere opprettholde krav til anonymitet. I tillegg kunne vi hindre at ansatte fikk mistanke om at linken inneholdt skadevare som kunne true cybersikkerheten, ettersom e-posten ble sendt fra en ekstern adresse.

3.4.3 Datainnsamlingsmetode og sikkerhetskultur

Som presentert i teorikapittelet er det ulike synspunkt om hvorvidt en kan undersøke sikkerhetskultur ved bruk av ulike datainnsamlingsmetoder (Engen et al, 2021; Shein 2010; Pidgeon, 1998). I denne studien har vi valgt å benytte spørreundersøkelse og intervju. Ifølge Shein (2010) kan det si noe om verdier og holdninger, men gir ikke et fullt innblikk i kulturen. Spørreundersøkelsen vil kan dermed ha en begrensning for å kunne si noe om den digitale sikkerhetskulturen i nettselskapet. Derimot har intervju en mulighet for å samle dybdekunnskap, noe som gir tro på at vi kan studere kulturen på et dypere nivå enn bare verdier og holdninger (Shein, 2010; Johannessen et al, 2016). I tillegg argumenterer vi for at rekkefølgen vi gjennomførte datainnsamlingen, gir grunnlag for at spørreundersøkelsen er relevant spesifikt nettselskapets digitale sikkerhetskultur.

3.5 Analysemetode

I analyseprosessen valgte vi å studere de kvalitative og kvantitative dataene hver for seg, for å til slutt se de kvantitative funnene i lys av de kvalitative. Dette kan ses i sammenheng med det Tashakkori & Teddlie (2010) kaller for "sekvensielt eksplorerende design". Dette lar seg gjennomføre ettersom vi samlet kvalitative data først som utgangspunkt for hva vi ønsket å se på i det kvantitative (Grønmo, 2016). På denne måten kunne vi vurdere om ansatte hadde

samme opplevelse av digital opplærings påvirkning av digital sikkerhetskultur, som ledelsen beskrev. Dette ville også gi oss et bedre innblikk i den digitale sikkerhetskulturen. Konseptet sikkerhetskultur kan være komplekst å kartlegge, og ved å benytte to metodetilnærminger gav det tro på at vi kunne studere nettselskapets digitale sikkerhetskultur på en grundigere måte enn vi hadde gjort ved bruk av bare en.

Figur 7: Analyseprosess

3.5.1 Kvalitativ analyse

For å slippe unna det velkjente problemet Kvale og Brinkmann (2015) beskriver som «1000-sidersproblemet», hvor forsker blir overveldet av store mengder intervjumateriale, startet vi analysearbeidet underveis mens vi gjennomførte intervju. Dette gav oss mulighet til å justere spørsmålene og innholdet i intervjuguiden ved behov. Vi valgte å benytte oss av en kvalitativ analysemetode for å holde en struktur i analysearbeidet. Analysemetoden *stegvis-deduktiv induksjon* (SDI) er utarbeidet av forfatteren og forskeren Aksel Tjora (Tjora, 2018). SDI-analysen består av en trinnvis modell, og tanken bak analysemetoden er at man benytter en induktiv strategi ved å holde seg så tett opp til datamaterialet som mulig. Til slutt ender en opp med å kunne se empirien i lys av teorien, noe som samsvarer med vårt valg av induktiv og abduktiv strategi. Ved å benytte en induktiv strategi var det mulig for oss å avgrense påvirkningen av teorier fra start, og dermed styrke vår evne til å se uventede funn i datamaterialet. Ved å følge Tjoras analysemetode, endte vi til slutt opp med tre temaer, som la grunnlag til hvordan vi bygde opp analysekapittelet (Tjora, 2018). Dette gjorde det også mulig å bygge opp en struktur i analysekapittelet som samsvarer med "sekvensielt eksplorerende design", hvor vi først presenterer den kvalitative analysen, for så å se de kvantitative funnene i lys av de kvalitative.

3.5.2 Kvantitativ analyse

Spørsmålene i spørreskjemaet hadde et målenivå som tilsvarer nominal- og ordinalnivå, noe som la føringer for hvilke statistiske analyser vi kunne gjennomføre (Johannessen et al, 2016). I denne oppgaven har vi hovedsakelig benyttet univariat analyse ved hjelp av prosentfordeling, men også enkelte bivariate analyser i form av uavhengig t-test hvor en sammenligner gjennomsnittsverdier (Johannessen, 2019). Dette gjorde vi hovedsakelig for å undersøke om det var statistisk sammenheng i funn fra det kvalitative intervjumaterialet. De univariate analysene gjorde det mulig å fremstille hvordan ansatte, ledelsen og superbrukerne vurderte digital opplæring for å fremme læring. Vi benyttet også prosentfordeling for å vurdere ansattes egenrapportering av hvordan digital opplæring påvirket de sentrale momentene innen digital sikkerhetskultur. Vi valgte å ikke presentere kvantitative data fra ledelsen under spørsmål om effekt av opplæringen, hovedsakelig grunnet tanken om at personer som er involvert i opplæringsarbeidet kan ha en sterkere tro på effekten av opplæring, enn andre. Dermed benyttes de kvantiative dataene fra ledelsen og superbrukerne for å besvare forskningsspørsmål 2 og 3.

For å utføre de statistiske analysene benyttet vi oss av SurveyXacts fremstilling av deskriptiv statistikk som utgangspunkt. Vi fremstilte egne tabeller for prosentfordeling. I tillegg utførte vi t-testene og Cronbach Alpha-test i Excel.

3.6 Refleksjon rundt prosjektet

I dette delkapittelet vil vi løfte frem refleksjoner rundt kvalitet i arbeidet, både ved å belyse oppgavens validitet, reliabilitet og svake sider. Det vil avslutningsvis bli trukket frem etiske vurderinger som er gjort underveis.

3.6.1 Validitet og reliabilitet

For å vurdere datakvaliteten er det sentralt å diskutere gyldigheten og påliteligheten, også kalt validitet og reliabilitet. Ifølge Kvale og Brinkman (2015) handler validitet om mer enn det metodiske valgets relevans for problemstillingen, og at en heller bør stille spørsmål om gyldighet i alle ledd av forskningsprosessen. Noen av validitetsvurderingene er presentert over, men de resterende vil i det følgende utdypes.

Siden vi var to forfattere av oppgaven, har vi benyttet hverandre underveis for å konferere og diskutere hvordan vi best mulig kan få svar på oppgavens problemstilling. Ifølge Malterud (2017) er det en styrke at forskere diskuterer materialet sammen. Begge deltok på intervjuene, transkriberte all tekst, og utførte analysen hver for seg, for deretter å diskutere materialet i fellesskap. Det at begge deltok på intervjuene gjorde det lettere å legge merke til motstridende utsagn fra informanter, og fange opp hvis enkelte deler av informasjonen var mangelfulle. Dette kan relateres til det Malterud (2017) kaller deltakersjekk som er en form for validering av informasjon som kommer frem i intervju.

Som beskrevet var svarprosenten på spørreundersøkelsen 61,9%, men antall representanter fra ledelsen og ansatte var på henholdsvis 7 og 59 personer. Dette kan anses som et relativt lavt antall respondenter i kvantitative analyser (Johannessen et al, 2016). Et lavt antall respondenter kan være med på å påvirke validiteten i resultatene i den kvantitative analysen, særlig relatert til analysene med t-test (Johannessen et al, 2016). Av bivariate analyser er t-test den statistiske metoden som ikke krever et så stort antall respondenter, sammenlignet med eksempelvis krysstabellanalyser (Gripsrud et al., 2021). Dette styrker tro på at de bivariate analysene er basert på en analysemetode som gir mest mulig valide svar.

Ved utarbeidelse av spørreskjemaet ble det hentet inspirasjon fra Digitaliseringsdirektoratets (u.å) spørreundersøkelse. Det kan ifølge Johannessen et al (2016) være en metodisk styrke å benytte et allerede validert spørreskjema. Ettersom vi måtte endre en del av spørsmålene for at det skulle passe hensikten i vår oppgave, gjennomførte vi Cronbach Alpha-test for å vurdere om spørsmålene vi endte med, faktisk målte det de var ment å måle. Cronbach Alpha-test er ifølge Pallant (2010) en måte å måle reliabiliteten ved å vurdere graden av indre konsistens på de ulike skalaene i måleinstrumentet. En høy Cronbach alpha er regnet for å ha høy indre konsistens, hvor 0,7 er ansett som akseptabel verdi. Testen ble utført på spørreundersøkelsens kategorier kompetanse, atferd, risikopersepsjon og interesse. Resultatene fra Cronbach alpha-testen viste følgende:

Kategorier	Cronbach Alpha-verdi
Kompetanse	0,7684
Atferd	0,5847
Risikopersepsjon	0,4704
Interesse	0,6751

Tabell 4: Cronbach alpha

Vi ønsker også å trekke frem at det ble inkludert kontrollspørsmål i spørreundersøkelsen for å vurdere om respondentene var konsekvente i svarene. Dette gjorde at vi kunne vurdere om respondentene svarte det samme, tross ulik formulering. Dette styrker validiteten av spørreskjemaet (Johannessen et al, 2016).

Det å gjennomføre en prestudie er ifølge Johannessen et al (2016) noe som styrker studiens indre validitet ettersom man kan oppdage feil som ellers kunne ført til svakheter i analysen. Det ble gjennomført en prestudie før spørreskjemaet ble sendt ut. Spørreskjemaet ble sendt ut til fire ansatte i nettselskapet. Samtlige jobbet i nettselskapet og hadde gjennomført deres digitale opplæringen om cybersikkerhet. Respondentene gav relevant tilbakemelding om spørsmålsformuleringene og utforming av spørreskjemaet.

Ifølge Johannessen et al (2016) handler reliabilitet om hvilke data som blir benyttet, hvordan de ble samlet inn og hvordan de prosesseres. Det kan være utfordrende å etterprøve samfunnsvitenskapelige studier, og gjerne kvalitative studier generelt av flere årsaker. Johannessen et al (2016) løfter frem at samfunnsmessige problem endrer seg over tid. Malterud (2017) sier at en som forsker må være bevisst sin egen forutinntatthet, og ikke misbruke sin makt som forsker ved å mistolke deler av datamaterialet. På bakgrunn av dette har vi hele veien forsøkt å være bevisst på vår rolle. Dette har hjulpet oss til å holde en så nøytral posisjon som mulig, og ikke latt våre egne antagelser prege retningen i arbeidet.

3.6.2 Mulige svake sider ved prosjektet

Som mye av teorien omkring sikkerhetskultur viser til, er sikkerhetskultur et fenomen som er utfordrende å beskrive og måle (Schein, 2010; Guldenmund, 2018; Haukelid, 2008; Hopkins, 2016). Grunnet fenomenets kompleksitet og sprikende forskningsbaserte forståelse, har det vært noe utfordrende å gjennomføre kvalitativt arbeid uten å bli preget av teori. Malterud

(2017) benytter begrepet teoretisk bakteppe for å beskrive hvordan kvalitative forskere kan bli farget av forutinntatthet og teori i induktivt arbeid. Denne balansen har vært noe utfordrende å gjennomføre ved bruk av Mixed Methods. Som forskere har vi aktivt vært bevisst på denne sårbarheten, noe vi argumenterer for at har gjort det mulig å balansere påvirkningen av det teoretiske bakteppet til et moderat nivå.

Det å gjennomføre intervju før utsendelse av spørreundersøkelsen kan ha ført til begrensninger for hvilke spørsmål som ble inkludert i den kvantitative datainnsamlingen (Johannessen et al, 2016). For å redusere sjansen for dette, inkluderte vi mulighet for å avgi tekstsvar i deler av spørreskjemaet slik at respondentene kunne bevege seg litt utenfor spørreskjemaets begrensende rammer. I tillegg benyttet vi gradering av svar i form av Likert skala med verdier fra en til fem, for å få frem spekteret av ulike meninger hos ansatte (Johannessen et al, 2016).

Det å utføre grundige validitets- og reliabilitetskriterier av en spørreundersøkelse er som oftest svært tidkrevende (Johannessen et al, 2016). Som resultatene fra Cronbach Alpha-testen viser, kan det ses på som en svakhet i reliabiliteten av studien (Pallant, 2010). Årsaken til dette kan være flere, men noe av det vi ønsker å trekke frem er tidsavgrensning for gjennomføring av masterprosjektet. I tillegg er det få spørsmål innenfor enkelte av kategoriene. Det er derfor nyttig å bemerke at spørreskjemaet vi har benyttet oss av, har metodiske begrensninger (Johannessen et al, 2016). Vi har likevel tro på at de analysene vi gjennomfører, har mulighet for å belyse enkelte sentrale momenter innen digital opplærings påvirkning av digital sikkerhetskultur.

Både informanter og respondenter av spørreundersøkelsen ble valgt ut av vår kontaktperson i selskapet ved bruk av strategisk utvelgelse. Strategisk utvelgelse er ansett som en utvelgelsesmetode med svakheter. Det kan med større sannsynlighet føre til utvelgelse av personer som ikke er representative for resten av nettselskapet (Johannessen et al, 2016). Det kan for eksempel føre til at det bare trekkes ut informanter med interesse for temaet cybersikkerhet. Johannessen et al (2016) argumenterer for at det er helt nødvendig å gjennomføre et randomisert utvalg for å kunne si at funnene er representative, og strategisk utvalg er ikke en utvelgelsesstrategi som kvalifiserer til det. I dette prosjektet ble strategisk

utvelgelse likevel valgt, da kontaktpersonen i nettselskapet hadde god oversikt over de ansatte i selskapet, og tok høyde for å spre utvalget basert på ulike faktorer. Dette er beskrevet under delkapittelet "3.3.2 Utvalg til spørreundersøkelse".

Johannessen et al (2016) anbefaler omtrent 10-15 informanter i kvalitative prosjekter, og på bakgrunn av dette kunne antallet informanter vært høyere. I dette nettselskapet var antallet aktuelle informanter avgrenset til ni, og dermed ses det på som en styrke at vi har intervjuet samtlige. I tillegg opplevde vi at vi hadde nådd et metningspunkt når de siste intervjuene ble gjennomført, da det ikke ble tilført ny informasjon. Dette taler for at vi hadde fått kartlagt store deler av ledelsen og superbrukeres synspunkt omkring temaet (Malterud, 2017).

Det ble gjennomført enkelte bivariate analyser i oppgaven. Antallet bivariate analyser ble noe begrenset ettersom det var få variabler i spørreundersøkelsen som kvalifiserte som uavhengige variabler. Ifølge Johannessen et al (2016) må en klart kunne skille hva som kvalifiserer som uavhengige variabler, for å kunne gjennomføre bivariate analyser som viser kausal sammenheng. Dette har ført til at vi ikke har gjennomført like mange bivariate analyser som ønsket. Vi argumenterer likevel for at mange spørsmål i spørreundersøkelsen er formulert på en måte som kan indikere en sammenheng mellom digital opplærings påvirkning av digital sikkerhetskultur.

3.6.3 Etiske vurderinger

Blaikie & Priest (2019) argumenterer for at en som forsker bør ta stilling til etiske hensyn innen fire områder: frivillig deltagelse, beskyttelse av deltakernes interesser, informert samtykke og forske med integritet. Vår rolle som forskere har tidligere blitt beskrevet, men resterende momenter vil bli presentert og beskrevet i det følgende.

Alle informanter og respondenter ble informert om frivilligheten til deltagelse. Informantene fikk tilsendt og skrev under informert samtykke, som inkluderte beskrivelse av prosjektet og deres rettigheter til å trekke seg. Før oppstart av kvalitativ datainnsamling sendte vi søknad til NSD, ettersom vi skulle benytte lydopptak, samt fikk tilgang til navn og stillingstittel. Søknaden ble godkjent av NSD før intervjuene tok til. Lydopptak ble gjort ved bruk av en

applikasjon utviklet av UiO som er godkjent til studentprosjekter (UiO, 2017). Vi tok stilling til at bruken av opptak kunne gjøre informantene mer lukket (Jacobsen, 2005). På bakgrunn av dette informerte vi og fikk bekreftelse på å benytte det før hvert intervju.

Selv om informantene kjente til prosjektets hensikt og ga sitt samtykke til å være med på studien, kan det tenkes at det er en påkjenning at et materiale som er basert på deres meninger, skal bli publisert (Kvale & Brinkmann, 2015). Det var derfor viktig å anonymisere både informantene og nettselskapet. Alt av personidentifiserbart materiale og lydopptak ble slettet like etter intervjuene ble transkribert, og transkribert intervju vil bli slettet ved prosjektets innleveringsdato. For å samle inn og analysere de kvantitative dataene benyttet vi oss av Survey Xact som er en plattform anbefalt av Universitetet i Stavanger. Denne plattformen gjorde det mulig å holde datamaterialet utilgjengelig for alle andre enn forskerne og veilederen av oppgaven. Også dette materialet vil bli slettet ved prosjektets slutt.

4.0 Analyse

I analysekapittelet vil hovedfunnene fra intervjuene og spørreundersøkelsene presenteres. Først skal bakgrunnsvariabler fra spørreundersøkelsen presenteres for å gi et innblikk i respondentene. Videre vil vi gå inn på opplæringen som benyttes i nettselskapet, for senere å komme inn på fordeler og ulemper med digital opplæring som metode. Avslutningsvis vil det presenteres analysefunn knyttet til effekt av digital opplæring. Dette presenteres ut ifra de fire momentene i rammeverket til NorSIS (2019) om digital sikkerhetskultur.

Som beskrevet i metodekapittelet (3.2 Forskningsmetode), har vi valgt å utelate ledelsen og superbrukernes egenvurdering av digital opplærings effekt på digital sikkerhetskultur. Deres beskrivelser av digital opplærings effekt, handler derfor om hvilken påvirkning det har på de *ansatte*. Dermed blir ledelsens spørreundersøkelse utelukkende benyttet for å studere digital opplæring som metode. Dette illustreres i følgende tabell:

Oversikt over bruk av datamaterialet:	
Intervju ledelsen og superbrukere:	Benyttes i hele analysen
Ansattes spørreundersøkelse:	Benyttes i hele analysen
Ledelsens spørreundersøkelse:	Benyttes i analysen for å vurdere digital opplæring

Tabell 5: Datamaterialet og analysekapittelet

Vi vil her gjøre oppmerksom på at "superbrukere" og "ledelsen" blir skilt fra hverandre ved intervjusvar, mens i spørreundersøkelsen blir de to gruppene omtalt som "ledelsen". Ledelsens svar fra spørreundersøkelsen vil hovedsakelig kommenteres ved svarresultat som skiller seg betydelig fra de ansattes svar, eller de tidligere gitte intervjusvarene. Spørreundersøkelsen til ledelsen blir dermed benyttet som supplement til intervjuene, og for å lettere kunne se de kvantitative funnene opp mot de kvalitative. Vi gjør også oppmerksom på at begrepet "digital sikkerhet" har blitt benyttet i intervju og spørreundersøkelse. Dette ble gjort på grunnlag av at digital sikkerhet kan være et mer benyttet og forklarende begrep enn hva cybersikkerhet er. Som beskrevet i konteksten (delkapittel 1.3.4) av oppgaven, er begrepene innen temaet mye benyttet om hverandre, noe som kunne skapt ytterligere forvirring.

4.1 Bakgrunnsvariabler

Alder	**Ledelsen og ansatte N (%)**	
21-30 år	3 (4%)	
31-40 år	17 (26%)	
41-50 år	13 (20%)	
51-60 år	25 (38%)	
> 61 år	4 (6%)	
Ikke oppgitt	4 (6%)	
Totalt (N)	**66 (100%)**	
Arbeidsform	**Ansatte**	**Ledelsen**
Kontorarbeid	32 (54%)	7 (100%)
Ute i felt	8 (15%)	0 (0%)
Kombinasjon av ute og kontor	18 (31%)	0 (0%)
Totalt (N)	**59 (100%)**	**7 (100%)**
Digitale verktøy i arbeidshverdagen	**Ansatte**	**Ledelsen**
PC	52 (88%)	7 (100%)
Nettbrett	13 (22%)	0 (0%)
Mobil	59 (100%)	7 (100%)
Totalt (N)	**59 (100%)**	**7 (100 %)**

Tabell 6: Bakgrunnsvariabler

4.2 Digital opplæring innen digital sikkerhet i nettselskapet

Gjennom intervjuene beskrev informantene at nettselskapet har krav på å drive bevisstgjøringsarbeid ifølge kraftberedskapsforskriften, og at kravene blant annet omfatter opplæring av ansatte. Samtlige informanter fortalte om et delt opplæringsansvar mellom nettselskapet og konsernet, der selve målet med cybersikkerhetsopplæring er at de ansatte skal bli bevisst nok til at en reflekterer og tenker seg om to ganger før de handler.

Når det kommer til hvordan nettselskapet driver opplæringen, var det flere informanter som trakk frem at det ikke eksisterer krav til gjennomføring av opplæring. En av superbrukerne argumenterte for at nettselskapet mangler policyer på repetisjoner knyttet til gjennomføring av opplæringen innen cybersikkerhet. Informanten mente at dette temaet skiller seg fra andre temaer de har opplæring i, hvor det vanligvis er rutiner for gjentagelse av kursene. To av superbrukerne og en av ledelsen trakk frem viktigheten av repetisjon for å oppnå mest mulig læringsutbytte.

> *"Selskapet mangler struktur på repetisjon av kursene, og noe av grunnen er at en ildsjel i konsernet har sluttet (...). Blant annet uteble kursene i sikkerhetsmåneden i fjor siden personen hadde sluttet".* (L5)

En annen superbruker mente derimot at det er obligatoriske kurs en gang årlig. På tross av motstridende svar på om det eksisterer krav eller ikke, viser spørreundersøkelsen at størsteparten av både ansatte og ledelsen gjennomfører opplæringen en gang årlig eller oftere.

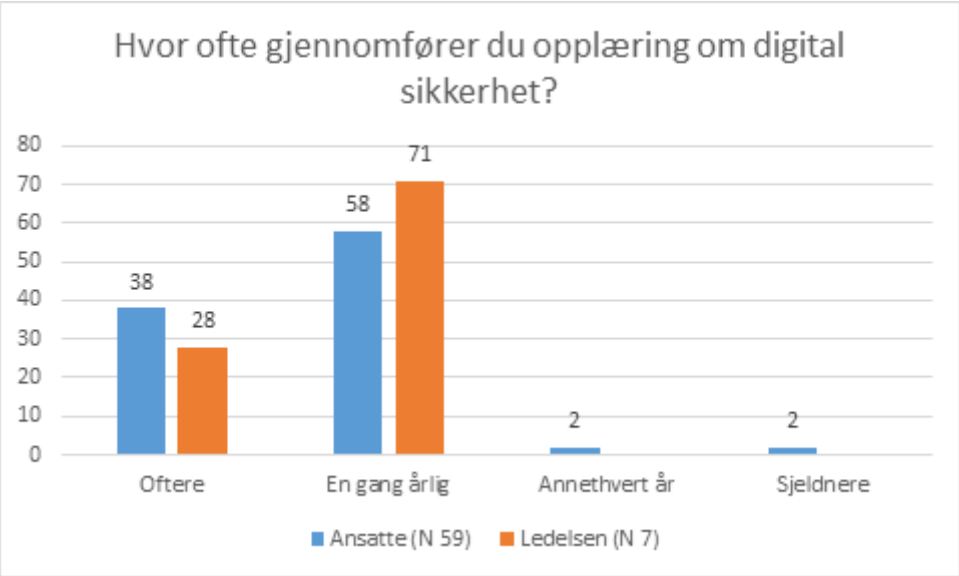


Diagram 1: Opplæring om digital sikkerhet - Svarene oppgitt i prosent %

Selv om flere informanter hevdet at det mangler repetisjon og struktur på opplæringen, kommer det frem at mesteparten av opplæringen innen cybersikkerhet gjennomføres i løpet av sikkerhetsmåneden (oktober hvert år). Gjennomføringen av sikkerhetsmåneden har dog vært noe varierende, ifølge flere informanter. Funnene fra ledelsen samsvarer med ansattes tekstsvar i spørreundersøkelsen, hvor det særlig etterlyses kontinuitet og obligatoriske digitale kurs.

> «*Opplæringen slik den er i dag er for dårlig. Flere og oftere kurs vil gjøre folk mer bevisst og oppdaterte på trusler*» (Spørreundersøkelsen til ansatte).

En annen respondent underbygger dette:

> *«Det burde være obligatorisk kurs med tanke på situasjonen vi er under i dag. Alle burde få lik informasjon om forventningene til digital sikkerhet blant de ansatte. Jeg sitter med en usikker følelse på hva som er forventet. Ved obligatoriske og hyppige*

kurs blir informasjonen lik for alle, og man vet hva som er forventet av den enkelte» (Spørreundersøkelsen til ansatte).

Når det kommer til hvor ofte opplæring *bør* gjennomføres, var det delte meninger blant informantene. En av superbrukerne mente at en gang årlig under sikkerhetsmåneden blir for lite, mens flertallet av informanter mente dette var nok.

> *"(...) men det er jo ferskvare den bevisstheten, så den må nok repeteres minst en gang i året."* (S1)

I spørreundersøkelsen til ledelsen kommer det frem noe ulike svar sammenlignet med intervjuene. Her fremkommer det at størsteparten fra ledelsen mener det er nødvendig med opplæring oftere enn en gang årlig, og en mindre del mener en gang årlig. Dette samsvarer ikke med hva de formidlet under intervjuene, da de fleste var enige at opplæring en gang årlig var tilstrekkelig.

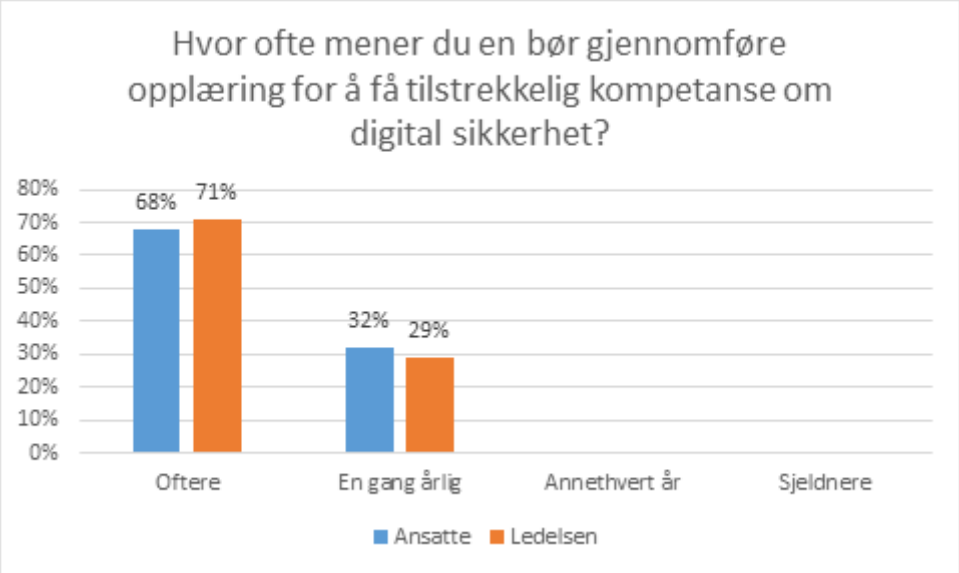


Diagram 2: Hvor ofte bør opplæring gjennomføres

Det er stor enighet mellom hva ledelsen og ansatte anser som tilstrekkelig repetisjon av opplæringen. Opplæringen gjentas ikke oftere enn en gang årlig, selv om størst andel anser det som nødvendig å gjennomføre den oftere.

Informantene var samstemt om at det er nødvendig med opplæring, og at manglende opplæring kan føre til hendelser som kan true cybersikkerheten. Det ble også trukket frem viktigheten av

at samtlige ansatte må være bevisstgjort. En informant fra ledelsen trakk frem cyberangrepet på et annet selskap som et eksempel for å tydeliggjøre hvor viktig det er at alle ansatte må være bevisstgjort. Potensialet for at en cyberangriper kan trenge seg inn i deres system, vil være større om ikke alle er bevisstgjort, beskrev informanten. Gjennom spørreundersøkelsen og spørsmålet om hvorvidt opplæring innen digital sikkerhet kan gjøre selskapet bedre rustet til å stå imot digitale trusler og angrep, er nesten samtlige av både ansatte og ledelsen enig eller helt enig.

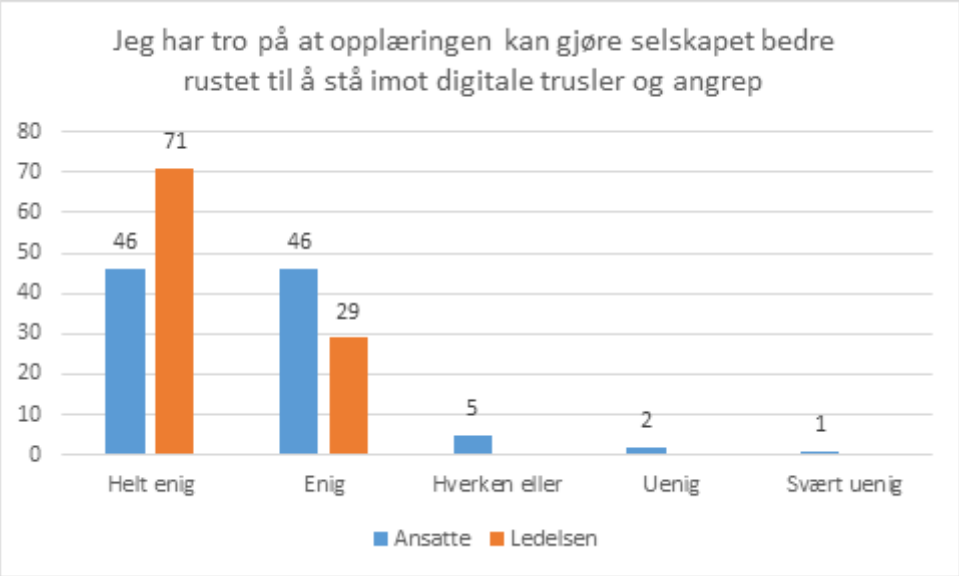


Diagram 3: Tro på at opplæring gjør selskapet rustet - Svarene er oppgitt i prosent (%)

4.3 Digital opplæring som metode

Nettselskapet benytter digital opplæring for å drive opplæring og informasjonsdeling om cybersikkerhet. De benyttede metodene er illustrert i en tabell under.

Nettselskapets digitale opplæringsmetoder:
E-læringskurs med quiz
E-læringskurs uten quiz
Informasjonsplansjer på intranett
Informasjon på e-post
Webinar
Videokurs på interne nettsider
Temaet blir tatt opp som del av digitale allmøter

Tabell 7: Nettselskapets digitale opplæringsmetoder

To informanter fra ledelsen beskrev at informasjon på intranett blir benyttet om det er behov for at de ansatte skal være ekstra oppmerksomme. Ulike påminnelser på mail er et krav fra

NSM under ekstraordinære omstendigheter. Flere av informantene fra ledelsen og superbrukerne trakk frem at e-læringskurs ofte består av tekst, illustrasjoner, og i noen tilfeller inneholder spørsmål på slutten. Når det kommer til hvorfor nettselskapet benytter seg av digital opplæring trakk en informant fra ledelsen frem tidseffektivitet og fleksibilitet. Det gir mulighet til å gjennomføre opplæring når en selv har tid, ifølge informanten.

> "*Det er jo mye enklere og kjappere å bruke de (digitale opplæringsmetoder). De har sine styrker med at det er lettere å få noe ut. Skal en ha fysiske samlinger, selv om en er deler de ansatte opp i grupper, så tar det mye lengre tid å ha et fysisk møte.*" (L2)

En informant fra ledelsen trakk frem at effekten av fysiske kurs sikkert er like bra, men at det er mer ressurskrevende. To superbrukere og en fra ledelsen mente at årsaken til at digital opplæring blir benyttet, er at det er enkelt å både oppdatere og gjennomføre kursene, samt nå ut til alle ansatte. Det ble også trukket frem at det er positivt for de ansattes læring ved bruk av digital opplæring.

> "*Jeg syns jo det er greit med sånn e-læringskurs for da får man god tid og ro til å følge med, og hvis det er noe en lurer på så kan en spole tilbake og kjøre den på ny igjen. Så jeg føler det jo er veldig ryddig og greit.*" (S2)

De ansatte er i stor grad enig i ledelsens utsagn om at fleksibiliteten skaper bedre læring, men svarprosenten er også fordelt utover de andre svaralternativene.

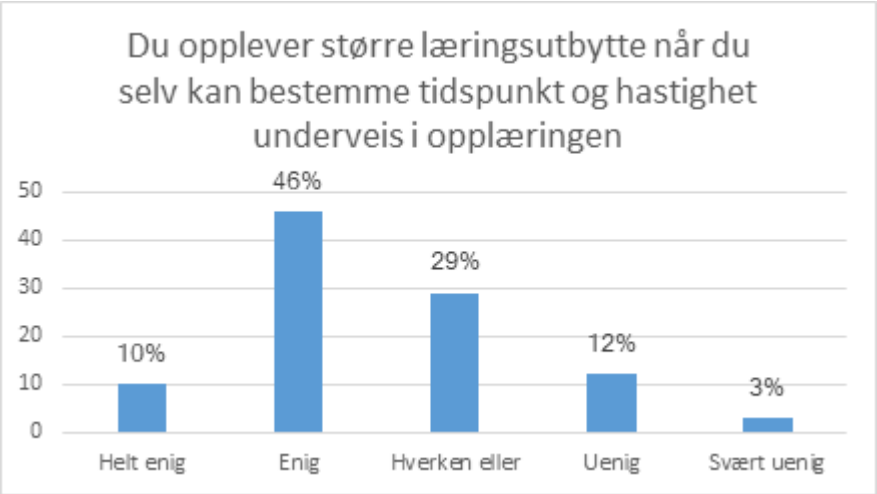


Diagram 4: Læringsutbytte når du selv kan bestemme tidspunkt og hastighet

Gjennom intervjuene kom det frem at nettselskapets digitale opplæring ofte består av korte kurs på omtrent 5-15 minutter, noe de kaller "Nano-learning". Der blir ulike tema innen cybersikkerhet tatt opp. Flere fra ledelsen uttrykte tro på at disse kursene er med på å motivere de ansatte til å gjennomføre opplæringen, samt at de gir større læringsutbytte. Kursene er effektive å gjennomføre, og som oftest inneholder de små sekvenser med spørsmål på slutten.

> *"Personlig liker jeg kurs som er korte og konsise. I stedet for de lange kursene, som er veldig lite effektive egentlig. De korte e-læringskursene kan en ta når en har anledning. Det syns jeg er veldig greit. Da har man motivasjon for å ta de og".* (S3)

Denne måten å gjennomføre opplæringskurs, ser ut til å samsvare med preferansene til mange av de ansatte, da det gjennom spørreundersøkelsen kommer frem at over halvparten foretrekker kurs som varer 5-15 minutter. Dette funnet samsvarer også med en av respondentenes svar knyttet til hvorvidt digital opplæring er med på å påvirke sikkerhetskulturen i nettselskapet:

> *"Viktig at vi hele tiden får små "drypp" med opplæring og informasjon. Så vi hele tiden har fokus på dette og ikke glemmer det. Hvis vi får noe som kun tar et par minutt i uken og lese, så vil det bli lest. Hvis vi får et skriv på 20 sider, så blir det ikke lest"* (Respondent, ansatt)

Samtlige i ledelsens spørreundersøkelse svarte også 5-15 minutt. Ledelsen og ansatte er i stor grad samstemt om at korte kurs om cybersikkerhet fenger mest.

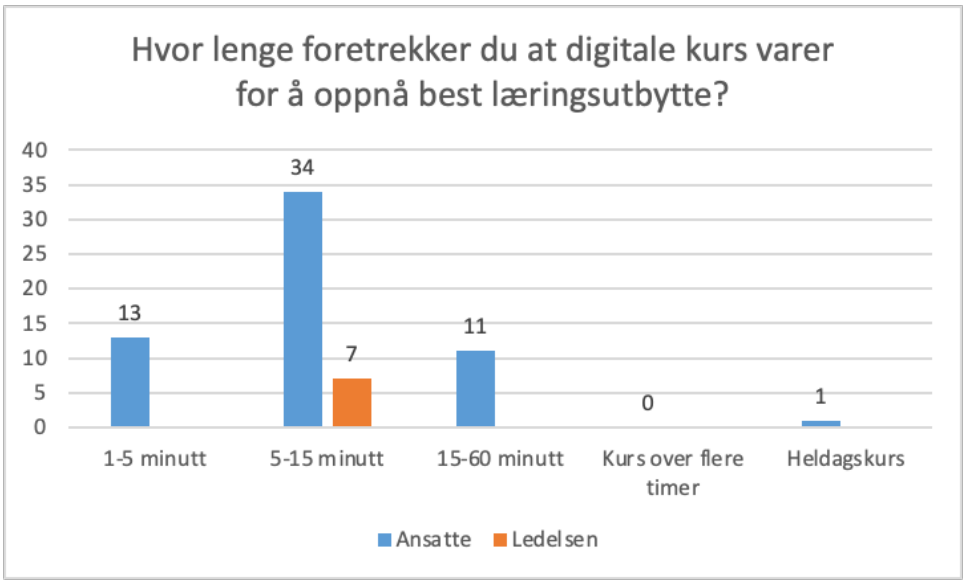


Diagram 5: Foretrukket varighet på kurs - Svarene oppgitt i antall (N)

Når det kommer til innholdet i kursene sa to informanter fra ledelsen at de foretrekker spesifikke hendelser og eksempler. Dette for å skape en slags nærhet til risikoen. Det kommer frem gjennom de ansattes spørreundersøkelse at innhold i opplæringen med spesifikke eksempler også fungerer best for dem. Derimot skaper generell informasjon interesse hos en betydelig mindre andel, og innhold som er relevant på andre arenaer ligger en plass imellom de overnevnte.

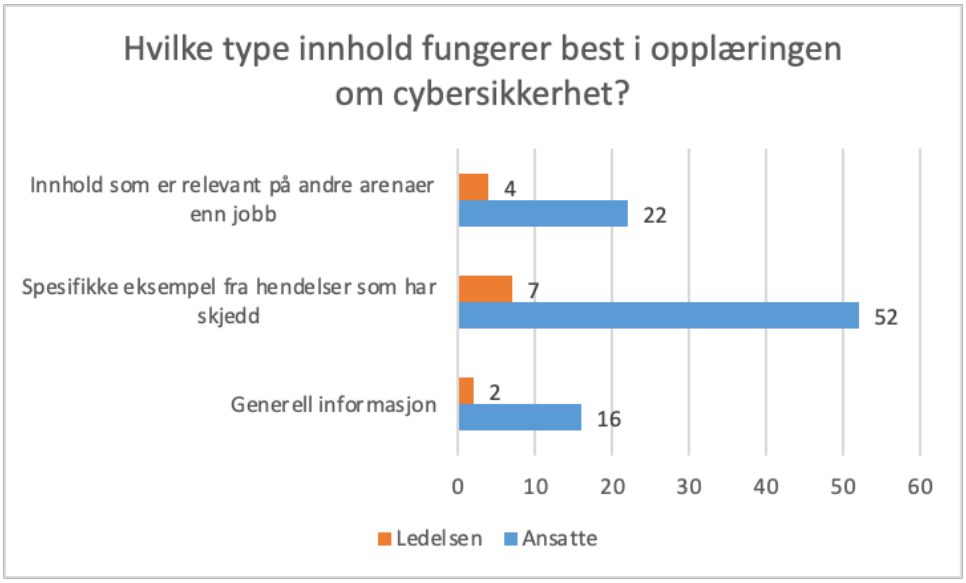


Diagram 6: Foretrukket innhold i opplæringen

Svarene er oppgitt i antall (N) med mulighet for flervalg.

På tross av at de fleste foretrekker spesifikke eksempler i opplæringen, består det meste av opplæringen av generell informasjon, ifølge to superbrukere og tre fra ledelsen. Samtlige av informantene trakk frem at det er viktig med opplæring som fenger, og som gjerne får kursdeltageren til å interagere og reflektere underveis. Det fremkom gjennom intervjuene at dette ofte gjøres gjennom aktiv deltagelse ved bruk av spørsmål og oppgaver en får etter, eller underveis, i opplæringen. En av superbrukerne mente at digital opplæring som er interaktiv er den beste formen for opplæring. Superbrukeren sa også at disse bør være konkrete i forhold til hendelser for å gjøre opplæringen aktuell. En fra ledelsen mente det er bra med praktiske tester da en må være bevisst, påkoblet og kritisk.

Når det kommer til spørreundersøkelsen ser en tydelig at de ansatte og ledelsen verdsetter aktiv deltagelse i opplæringen, hvorav de fleste svarer at de er helt enig eller enig. Det er også enkelte

som svarer verken eller, uenig og svært uenig, hvorav størst prosent av de som er uenig er representanter fra ledelsen.

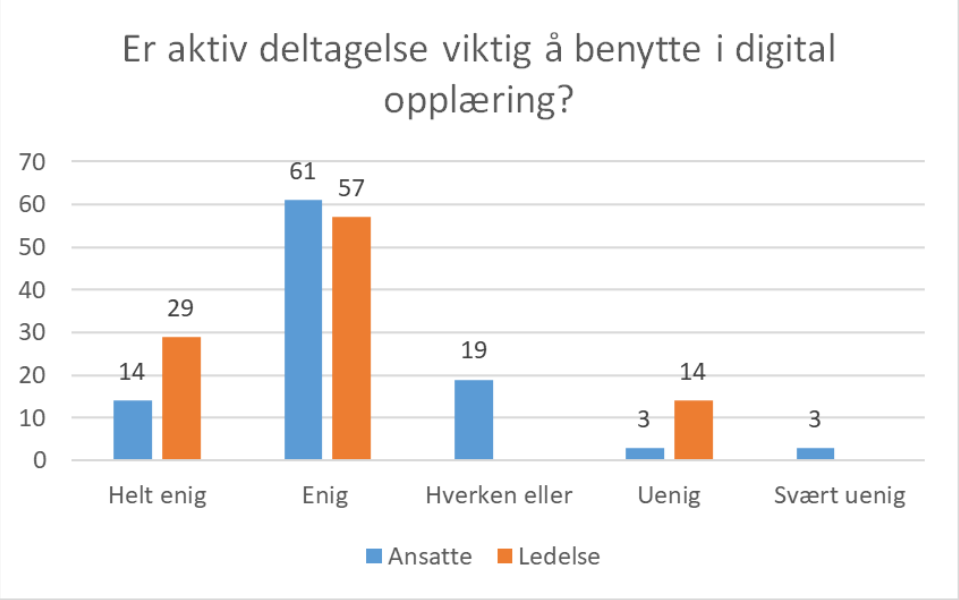


Diagram 7: Aktiv deltagelse i opplæringen - Verdiene oppgitt i prosent (%)

To fra ledelsen og tre superbrukere beskrev at den beste måten å skape aktiv deltagelse fra kursdeltager i digitale kurs, er gjennom spørsmål på slutten av e-læringskursene. På spørsmål om hvilken opplæringsmetode som skaper mest refleksjon, ble e-læring med quiz trukket frem.

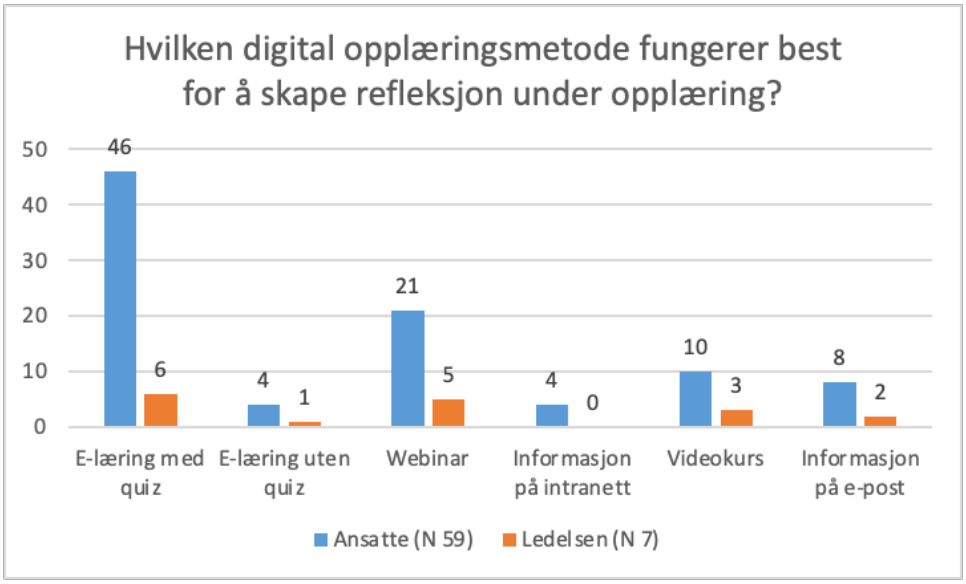


Diagram 8: Foretrukket opplæringsmetode for refleksjon

Svarene oppgitt i antall (N) med mulighet for flervalg.

Det fremkommer det gjennom spørreundersøkelsen at opplæringsformene e-læringskurs uten quiz, informasjon på e-post og intranett, skaper refleksjon hos betraktelig færre ansatte. Dette er likevel noen av selskapets mest benyttede digitale opplæringsmetoder (som presentert i tabell 7). På spørsmål om nettselskapet benytter nok aktiv deltagelse i den digitale opplæringen, fordeler svarene seg omtrent likt mellom *ja* og *nei.* Hos de ansatte er det en overvekt av svar som indikerer at nettselskapet benytter nok aktiv deltagelse, mens det på ledelsens side er flest som svarer nei.

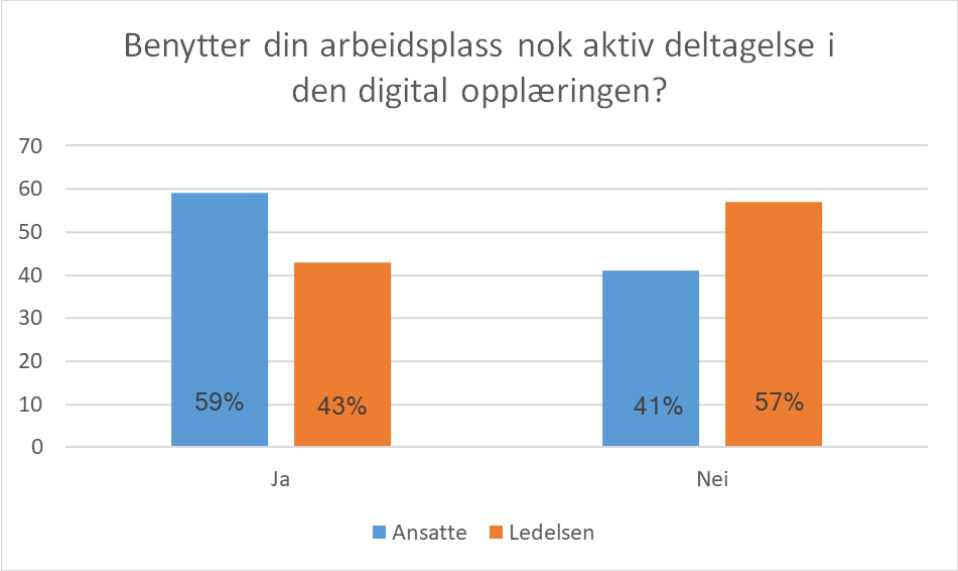


Diagram 9: Benyttes det nok aktiv deltagelse

På spørsmål om informantene tenker at digital opplæring er tilstrekkelig for å lære opp de ansatte, var de fleste av informantene enig i at det er tilstrekkelig for å oppnå det nivået de ønsker at de ansatte skal ha. En forutsetning er likevel at kursene må repeteres ofte nok, og at de er gode nok. En av superbrukerne mente at digital opplæring fungerer godt på brukernivå, da det allerede eksiterer tekniske barrierer i systemet som vil fange opp de fleste varseltegn.

4.3.1 Ulemper med digital opplæring som metode

Enkelte av informantene mente at den digitale opplæringen som benyttes i dag ikke er optimal for å skape læring. To superbrukere og en fra ledelsen mente at selskapet burde benytte en kombinasjon av flere digitale opplæringsmetoder for å nå ut til flest mulig ansatte. En superbruker trakk også frem at det er en svakhet ved digital opplæring at ikke alle ansatte følger like godt med på de ulike digitale kommunikasjonsplattformene. Tre informanter fra ledelsen mente at selskapet burde ha en kombinasjon av digital og fysisk opplæring for å treffe flere av

de ansatte. Digital opplæring i kombinasjon med fysisk, vil skape ytterligere dialog og interaksjon i opplæringen, ifølge informantene. Dette samsvarte med meningene til informant L4.

> "*Det er nok gjerne en kombinasjon av digitalt og klasserom som er best. Når man bare kjører digitalt tror jeg nok en del vil synes det er for ensformig, pluss at man mister mulighetene til å spør. Jeg ser jo hvis man har klasseromsundervisning og man har en veldig "oppegående" foreleser, for å si det sånn, så vil jo det fort engasjere, og da vil det jo gjerne bli mange gode spørsmål og diskusjoner."* (L4)

En fra ledelsen mente at de har forsøkt å tilrettelegge for diskusjon under digitale allmøter, men at de ansatte ikke tar ordet under disse møtene. I spørreundersøkelsen kommer det frem at noen av de ansatte savner klasseromsundervisning og praktisk øvelse, da det gir større mulighet for diskusjon og refleksjon. Ettersom det var rom for tekstsvar på dette spørsmålet i spørreundersøkelsen, refererer vi to respondenter:

> "*E-læring huskes i kort tid, det eneste som gir varig læring er foredrag/ klasseromsundervisning med pedagogisk utdannet instruktør".* (Respondent, ansatt)

> *"Hvis alle på samme avdeling/gruppe deltar på fysiske kurs sammen, får man felles kultur og forståelse og kan spille hverandre gode hver dag, lang tid etter kurset. Digital læring er glemt en time etter fullført (selv med quiz)"* (Respondent, ansatt)

Enkelte av informantene mente at digital opplæring er godt tilrettelagt for de som jobber på kontor, men at de er litt usikre på om det er like godt tilrettelagt for de som jobber ute. En av superbrukerne mente at arbeidsformen til de som jobber ute, trolig er mindre egnet for å benytte digitale hjelpemiddel. Dette samsvarer med en annen informant fra ledelsen, som beskrev at de som jobber ute burde hatt fysiske foredrag i stedet for digital opplæring, grunnet lite tilgang på digitale hjelpemiddel til å gjennomføre opplæringen når de er jobber ute. I intervjuet med en annen informant fra ledelsen ble det nevnt at de som jobber ute er utenfor brannmurene, noe som også gjør digital opplæring mindre tilrettelagt for dem. Det fremkom også gjennom intervjuene med to superbrukere og en fra ledelsen at alder kan være en faktor som preger deres synspunkt og mulighet for å gjennomføre digitale opplæring, og dermed påvirker effekten av læringen.

For å undersøke om dette stemte, stilte vi spørsmål i spørreundersøkelsen om de ansatte føler selskapet legger til rette for at de kan gjennomføre opplæringen i sin arbeidshverdag. Her svarer de fleste at de er enig, men også noen uenig og hverken eller.

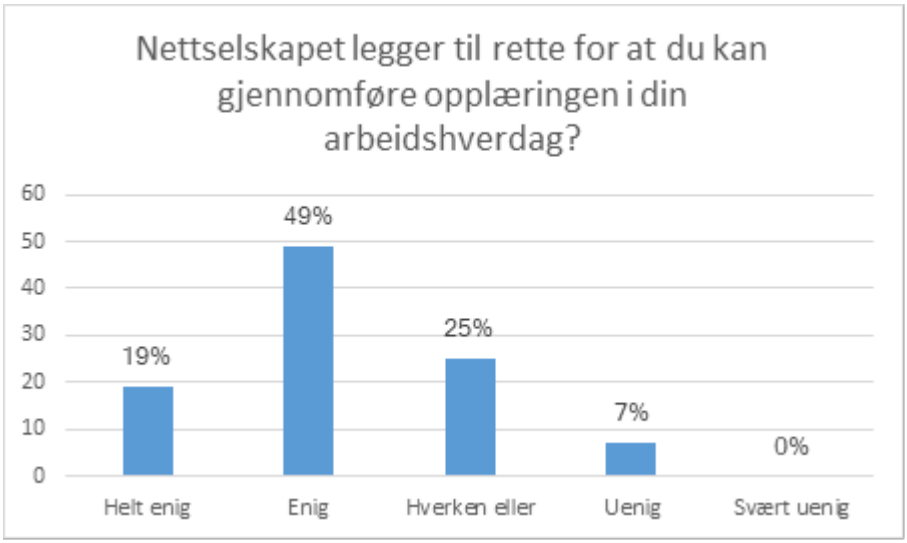


Diagram 10: Tilrettelegging av opplæring

Oppsummering:

Det er noe delte meninger omkring digital opplæring generelt, og hvordan det praktiseres i nettselskapet i dag. Samtlige av ledelsen ser behovet for å gjennomføre opplæringen for å styrke bevisstheten hos de ansatte. Dette ser ut til å samsvare med synet til de ansatte ettersom de faktisk gjennomfører opplæringen en gang årlig, og mange gir i tillegg uttrykk for at opplæringen med fordel kunne vært gjennomført oftere. Mangelen på repetisjon av kursene er noe både ledelsen og ansatte gir uttrykk for at kan svekke læringsutbyttet.

Ledelsens argumenterer for at de benytter digital opplæring i nettselskapet da det skaper fleksibilitet, tidseffektivitet, en rolig læringssituasjon, og det når ut til alle ansatte. De fleste ansatte er enig i noen av disse fordelene.

Selskapet har valgt å benytte korte kurs, med generelt innhold, og inkluderer gjerne aktiv deltagelse i en del av opplæringen. De fleste ansatte synes korte kurs passer godt, men når det kommer til innholdet og bruk av aktiv deltagelse, er svarene noe varierende. En del av de ansatte liker generelt innhold i opplæringen, men de aller fleste skulle gjerne sett at det inneholdt spesifikke eksempler. Når det gjelder aktiv deltagelse, liker de fleste ansatte e-læring med quiz for å skape refleksjon underveis i kurset. Det blir i dag benyttet flere digitale

opplæringsmetoder uten aktiv deltagelse i selskapet. Selv om det er tilfellet, ønsker bare omtrent halvparten av de ansatte og ledelsen at det skulle vært mer aktiv deltagelse.

Det eksisterer et par svake sider ved den digitale opplæringen i nettselskapet. Ledelsen trekker selv frem at digital opplæring generelt ikke når ut til alle, og at de gjerne burde hatt flere digitale kommunikasjonskanaler for å få dette til. I tillegg peker en informant fra ledelsen, samt flere av de ansatte, på at de digitale opplæringsmetodene som benyttes i dag skaper lite rom for diskusjon. Noen av de ansatte trekker også frem ulemper ved digital opplæring som at de glemmer informasjonen lett, og at det skaper lite felles forståelse.

Tross enighet i ledelsen om behovet for opplæring, beskriver flere informanter at målet med opplæringen er å gjøre de ansatte bevisst nok til å reflektere to ganger før de gjennomfører en handling. De mener at de ikke trenger egeninteresse for temaet.

4.4 Effekt av digital opplæring

Videre skal det settes lys på hvilken effekt digital opplæring om cybersikkerhet har på de ansatte. Effekten på de ansatte skal relateres til de sentrale momenter innen digital sikkerhetskultur, som er relevant for læring. For å få svar på dette, blir både empiri fra intervjuene med ledelsen og spørreundersøkelsen til de ansatte benyttet.

4.4.1 Kompetanse

To superbrukere og tre informanter fra ledelsen argumenterte for at opplæringen har vært vesentlig for å hindre ondsinnede aktører inn i nettselskapet, og at opplæringen har ført til at de ansatte i økende grad har fått kjennskap til hva som er forventet av dem. En informant fra ledelsen beskrev at de ikke hadde blitt utsatt for vellykkede cyberangrep. På spørsmål om den digitale opplæringen fører til økt kompetanse omkring cybersikkerhet, svarer informant S1:

> *"Ja, det er det helt klart at det gjør. Om en ikke bevisstgjør, er det gjerne bare en halvfull engasjerte medarbeidere som får det med seg (...) Opplæring er vesentlig, fordi at om en ikke kjenner trusselbildet, vil en heller ikke være oppmerksom på hva en skal fange opp".* (S1)

En superbruker og en informant fra ledelsen mente at de ansatte tar cybersikkerhet alvorlig, men de har samtidig et inntrykk av at de ansatte kunne vært enda mer bevisst og vist sin kompetanse i ytterligere grad i det daglige. Videre beskrev flere av informantene at de var usikre på hvilket kompetanseutbytte de ansatte får av den digitale opplæringen. To informanter fra ledelsen forteller videre at de tror og håper at opplæringen øker de ansattes kompetanse, men at de ikke har en god måte å måle det på.

> *"Ja, jeg tenker de fleste blir mer bevisst. Så er heller spørsmålet om det er nok, eller i hvilken grad de blir bevisst. Det er jo vanskelig å vurdere hvor mye informasjon folk trenger".* (L3)

En fra ledelsen beskrev at alle gjennomfører den samme opplæringen, men kompetanseutbyttet henger nok mye sammen med hvilken jobb og hvilket fokus en selv har på temaet. En annen informant fra ledelsen mente at kompetansen til de ansatte trolig ligger på 60-70% av det kunnskapsnivået de burde hatt. Flere informanter fra ledelsen hadde en formening om at kompetanseutbyttet fra opplæringen er noe avgrenset i forhold til hva det burde være, men at det nåværende nivået de ansatte nå ligger på, tross alt har effekt på cybersikkerheten.

For å sammenligne svarene fra intervjuene, stilte vi de ansatte spørsmål relatert til kompetansen de har fått gjennom den digitale opplæringen. Gjennom kartleggingen i spørreskjemaet synes det å være noe varierende effekt relatert til kompetanse hos de ansatte etter digital opplæring.

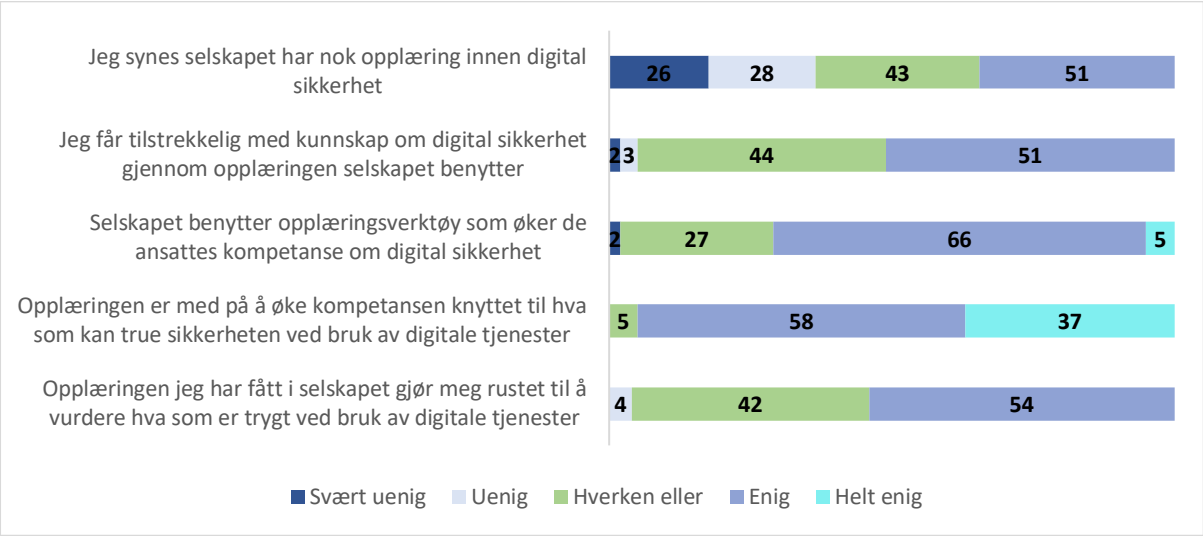


Diagram 11: Kompetanse - Svarene er oppgitt i prosent (%)

Nærmest samtlige av de ansatte svarer enig eller helt enig på spørsmål om de digitale opplæringsverktøyene nettselskapet benytter øker de ansattes kompetanse om cybersikkerhet. Over halvparten av de ansatte er enig i at opplæringen gjør de rustet til å vurdere hva som er trygt, men svarene er også fordelt på de andre svaralternativene. I spørreundersøkelsen var det mulighet for å avgi tekstsvar på spørsmål om hvordan digital opplæring påvirker kultur. En av respondentene skrev: *«Ved bevisstgjøring og opplæring så klarer de fleste å vite hva de skal se etter ved en eventuell trussel på sikkerheten».* Dette tekstsvaret underbygger dermed svarprosenten som svarer "enig" på at den digitale opplæringen påvirker de ansattes kompetanse. På spørsmål om selskapet har nok opplæring kan det se ut til at en stor del av respondentene mener de burde hatt mer opplæring. Likevel svarer over halvparten at de får tilstrekkelig informasjon om temaet gjennom selskapets opplæring.

Oppsummering:

Ledelsens synspunkt på hvordan digital opplæring om cybersikkerhet påvirker kompetansen til de ansatte, fremstår sprikende. Enkelte er overbevist om at kompetansen og bevisstheten har økt etter opplæring, mens andre mener det ikke er nok, eller at det er vanskelig å vurdere. Likevel er samtlige overbevist om at opplæringen har hatt en viss effekt på cybersikkerheten i nettselskapet. Funnene i spørreundersøkelsen skiller seg til en viss grad fra funnene i intervjuene. Mens flere av informantene gav uttrykk for at kompetanseutbyttet fra opplæringen trolig var litt begrenset i forhold til hva det burde være, svarer over halvparten av de ansatte at de får god nok kompetanse om cybersikkerhet. Det er også mange som svarer hverken eller på spørsmålet, og samsvarer dermed mer med ledelsens utsagn. Det fremstår som de ansatte vurderer at kompetanseutbyttet blir noe begrenset siden nettselskapet har litt for lite opplæring. Det er også relativt mange respondenter fra de ansatte med varierende svar på de ulike spørsmålene, noe som viser en uenighet i opplæringens effekt på kompetansen.

4.4.2 Atferd

To av informantene fra ledelsen mente at opplæringen er tilstrekkelig for at de ansatte skal få en atferd som nettselskapet anser som trygg. Tre fra ledelsen og to av superbrukerne mente de at de fleste ansatte tar i bruk informasjonen fra opplæringen, og dette har vært synlig ved at de ansatte har sikkerhet i fokus. Dette kommer frem ved at de ansatte viser og kommuniserer mer

skepsis rundt digitale tjenester. Samsvarende funn kom også frem hos informant L1 som fortalte at rapporteringen har økt etter angrep på samarbeidspartnere eller andre nettselskap.

> *"Folk er mer skeptiske til alt som går inn. Mer skeptiske til innholdet i mailer ved å dobbeltsjekke avsender i mailene. Det er jo først og fremst der den største trusselen er. Der du kan slippe inn folk (uvedkommende) gjennom den enkelte bruker".* (L1)

Videre beskrev en av superbrukerne at de ansatte viser mer årvåkenhet og rapportering etter opplæringen. En annen informant fra ledelsen mente at de gangene de har opplevd sikkerhetstruende cyberhendelser, har de sett økt oppmerksomhet hos de ansatte.

> *"Med en gang noen blir usikre, så blir det en del diskusjoner rundt det, og hvordan dette skal håndteres (...) Men altså, det er jo ikke IT-folk som sitter her, så helt komplett forståelse har de ikke. Men det er årvåkenhet, det er det".* (S2)

> "*Med jevne mellomrom kommer det gjerne en kollega som forteller at de har fått en mail som ser noe mystisk ut. Så det viser at de sånn sett er bevisst på dette"* (L5)

På spørsmål om opplæringen er tilstrekkelig for å oppnå ønsket adferd hos ansatte, svarte informant S1 følgende:

> *"Ja, men folk er veldig forskjellige.. Jeg tror nok at enkelte uansett hvor mye bevisstgjøring de hadde fått, så hadde de klikket på den ene linken som en ikke skulle. Men i det store og det hele, så er svaret ja"* (S1)

Flere informanter uttrykte at de er enig med argumentet til S1 om at utbyttet fra opplæringen er individuelt, og at det derfor er vanskelig å si om det har vært tilstrekkelig for å endre atferden til de ansatte. To av informantene fra ledelsen kunne derimot ikke svare på om atferden til de ansatte hadde endret seg etter den digitale opplæringen, ettersom de manglet en konkret måte å måle det på. På tross av dette, var det flere informanter som beskrev en rapporteringskanal der ansatte kan melde inn eventuelle hendelser til ansatte med IT-kompetanse. Ifølge to av informantene fra ledelsen bruker de ansatte rapporteringskanalen de har i nettselskapet, men var usikker på om den blir benyttet mer nå, enn før.

> "*Jeg har sett at folk spør om linker som er lagt ut er trygge. Da kommenterer folk på innlegget og spør om det er en trygg link. Det er en ganske stor endring gjennom de*

par-tre siste årene". (...) De ansatte melder inn, men om de gjør det mer eller mindre nå, det.. det er jeg usikker på." (L5)

Informant L3 løftet frem samme poeng, men uttrykte at det trolig er stor forskjell på rapporteringen mellom avdelinger.

> "*Nå jobber jo jeg på en plass der IT er i fokus, så da er det jo.. de kollegaene jeg sitter med vet jeg at sender inn om en e-post er trygg eller ikke. Men det er sikkert veldig forskjellig i ulike avdelinger i nettselskapet".* (L3)

I tillegg til rapporteringssystemet, beskrev flere informanter at resultater fra phishingtester også har vært nyttige for å vurdere opplæringens effekt på ansattes atferd. En superbruker og to fra ledelsen fortalte om gjennomførte phishingtester før og etter opplæring om cybersikkerhet i nettselskapet. Informant S1 beskrev dog at resultatene etter phishingtesten ikke viste effekt på atferd:

> *"(...) Men da viste det seg at det var flere som ble lurt enn før bevisstgjøringskampanjen. Så enten viser jo det seg at opplæringskampanjen var mislykket, eller så var den siste testen bedre utformet".* (S1)

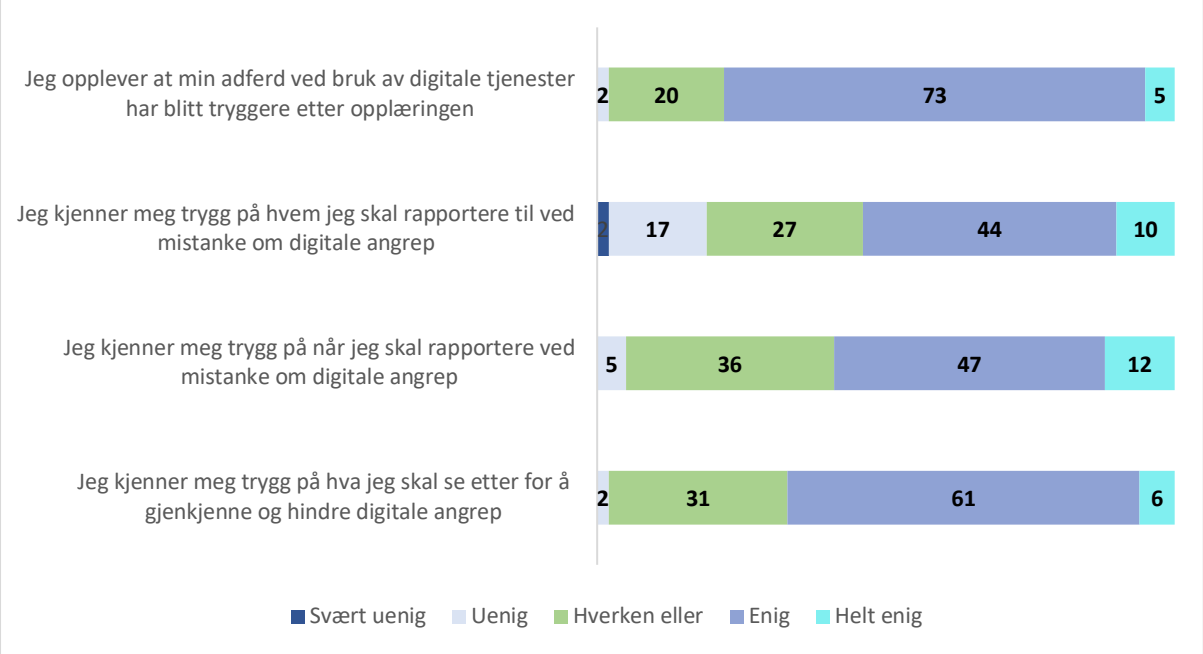


Diagram 12: Atferd - Svarene oppgitt i prosent (%)

Ut fra respondentenes svar i spørreundersøkelsen kan en se at flertallet av de ansatte er enig i at atferden har blitt tryggere etter opplæringen i nettselskapet. Dette kommer også frem i en respondents tekstsvar:

> *«Opplæringen forbedrer den individuelles selvstendige digitale sikkerhetsvurdering, slik at en eventuell underlig ting og hendelse oppdages tidligere»* (Respondent, ansatt)

Det er stor enighet hos de ansatte på spørsmålet om atferden har blitt tryggere, om de kjenner til hva de skal se etter for å hindre digitale trusler, og når de skal rapportere. Andelen som har svart hverken eller, eller er uenige i bedret atferd, er relativt lik på alle spørsmålene. Det er en del som har svart hverken eller, mens andelen er relativt liten på svarene uenig, eller svært uenig. Respondentene viser derimot mest sprikende svar på spørsmål om de vet hvem de skal rapportere til ved mistanke om digitale angrep.

Oppsummering:

Ledelsen og superbrukerne ser en økt skeptisk og årvåken holdning hos de ansatte ved at de rapporterer og diskuterer omkring temaet. Enkelte av ledelsen og superbrukerne argumenterer for at dette er grunnet den digitale opplæringen i nettselskapet, mens andre tror det kan relateres til økt oppmerksomhet generelt i samfunnet. Mange av respondentene fra de ansatte er enig i at opplæringen har hatt effekt på hva de skal lete etter for å hindre angrep, og at atferden har blitt tryggere. Det er likevel verdt å bemerke at en del svarer hverken eller, og enkelte uenig.

Ledelsen har fått en direkte innsikt i atferden ved å studere rapporteringssystemet og resultat fra phishingtester, hvorav begge viser en viss effekt, men også mangler. Respondentene viser derimot mest sprikende svar på spørsmål om de vet hvem de skal rapportere til ved mistanke om digitale angrep. Dette samsvarer dermed med funnene fra intervjuene, der flere informanter har uttrykt at de var usikre på om de ansatte vet hvem de skal kontakte.

4.4.3 Risikopersepsjon

En av informantene fra ledelsen beskrev at de ansatte tenker sikkerhet i sin arbeidshverdag, og at de er klar over at de må overholde sikkerheten på arbeidsplassen. På spørsmål om sikkerhetsfokuset også kan relateres til cybersikkerhet, svarte informanten at oppmerksomheten og innsikten på temaet utvilsomt har økt. En superbruker utrykket tro på at

opplæringen direkte påvirker de ansattes evne til å se alvoret i risikoen. To fra ledelsen mente at angrep på andre selskap gir de ansatte innsikt i at det kan skje de også, og på den måten kan øke innsikten i risikoen.

En informant fra ledelsen mente at opplæringen gjør at ansatte forstår at cyberhendelser kan forekomme, men at innsikten i konsekvensene kan være noe mangelfull. En superbruker og en fra ledelsen argumenterte for at eventuelle forskjeller i synet på risikoen og dens konsekvenser, kan relateres til individuelle faktorer som eksempelvis arbeidsform. Også her løftet informantene frem poenget med at de manglet en måte å vurdere ansattes innsikt i temaet.

> "*De som sitter på driftsorganisasjonen (SCADA) er jo fokusert på risiko osv. Og så vet jeg.. en kan jo tenke at en annen avdeling er montører som er ute og skrur og bygger osv. på strømnettet. De montørene har for så vidt tilgang til mye data de også, men jeg har ikke peiling på hvor oppdatert de er på ting".* (L3)

Som tidligere trukket frem, beskrev en superbruker at effektivitet og muligheten for å tilpasse innholdet i opplæringen etter hvert som trusselbildet er i endring, er noen av styrkene ved digital opplæring. Likevel mente han at disse fordelene ved opplæringsmetoden, ikke påvirker risikopersepsjonen til de fleste ansatte:

> *"Så du tenker at de ansatte lærer etter hvert som trusselbilde endrer seg, og at de holder seg oppdatert?"* (Intervjuer)
>
> *"Nei, jeg vil ikke akkurat si at alle gjør det, men de mest interessert gjør gjerne det"* (S1)

Risikopersepsjon som resultat av opplæringen ble også kartlagt i spørreundersøkelsen. De fleste ansatte er enig i at opplæringen gjør de bevisst på hvilke hendelser og risikoer som kan true sikkerheten, og at de har fått innsikt i hvilke forventninger nettselskapet har til dem. Dette samsvarer med et tekstsvar avgitt av en ansatt:

> *"Opplæringen hjelper oss til å være "ajour" på hvilke trusler som er aktuelle, og minner oss på at vi alltid må være på vakt overfor digitale trusler"* (Respondent, ansatt).

Funnene viser også at de fleste ansatte ikke tillater seg å gjøre handlinger som opplæringen fraråder. En del av de ansatte svarer dog at de er enig i at de kan gjøre det. Funnene viser også at mange vet at det eksisterer en risiko for at en som ansatt kan være inngangsport for et angrep, selv om en har fått opplæring. Dette samsvarer dermed i stor grad med det som fremkommer gjennom intervjuene med ledelsen.

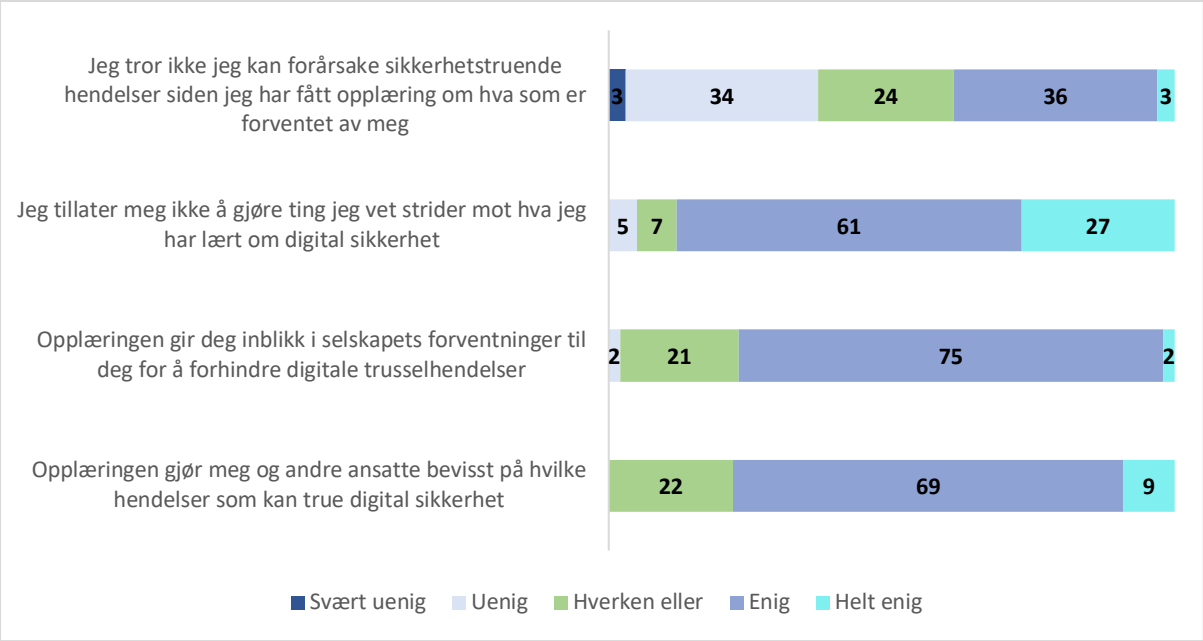


Diagram 13: Risikopersepsjon - Svarene oppgitt i prosent (%)

Oppsummering:

Ledelsen mente at de ansatte har en sikkerhetstankegang i arbeidshverdagen. Det kommer også frem at opplæring er med på å få de ansatte til å se alvoret i risikoen. Noen fra ledelsen trakk også frem hvordan hendelser hjelper de ansatte til å få en nærhet til risikoen, og hvor en får en forståelse av at dette kan skje de og. Derimot er ledelsen usikker på hvorvidt de ansatte forstår hvilke konsekvenser et cyberangrep ville hatt på nettselskapet. Det trekkes blant annet frem at avdelingen de ansatte jobber på kan ha en påvirkning på hvilken innsikt de har til risikoen og dens konsekvenser.

Spørreundersøkelsen viste at flere ansatte både har fått innsikt i risikoen og hva nettselskapet forventer av dem. Det kommer også frem at mange av de ansatte ikke tillater seg å gjøre ting som ikke er anbefalt gjennom opplæringen. Spørreundersøkelsen viser dermed stor enighet hos

de ansatte, men samtidig en viss spredning. Særlig gjelder dette spørsmålet om de kan forårsake en sikkerhetstruende hendelse på tross av opplæring.

4.4.4 Interesse

Gjennom intervjuene kom det frem at utbyttet av den digitale opplæringen henger sammen med interessen man har for temaet før man gjennomfører opplæringen. To superbrukere og en fra ledelsen mente at interesse for temaet gjør at man tilegner seg stoffet lettere. Videre beskrev en av dem at interessen også påvirker viljen til å gjennomføre kursene. Dette samsvarer med L1:

> *"Vi inviterte en kar fra NSM som holdt et foredrag. Alle fikk jo invitasjon, men det var bare ca. halvparten som deltok"* (S1)
> *"Så da er det denne interessen som påvirker oppmøte da?"* (Intervjuer)
>
> *"Ja.. og så er det klart at det er helst de som ikke deltok, vi skulle hatt på foredraget"* (S1)

Samtlige av informantene mente at digitale angrep er en trussel både på jobb og privat, og dermed skaper det større interesse. Denne interessen gjør dem mer mottagelig for opplæringen de får på jobb.

Når det kommer til om opplæringen skaper interesse innen temaet digital sikkerhet, viste intervjuene nyanserte svar. En superbruker og to fra ledelsen mente at de ansatte blir mer motivert til å lære om temaet etter opplæringen. Videre beskrev en fra ledelsen at ansatte har oppsøkt mer informasjon om cybersikkerhet på de interne nettsidene til nettselskapet, etter gjennomført opplæring. En superbruker fortalte at det alltid blir litt diskusjon hos de ansatte etter opplæringen. Dette kommer også frem gjennom tekstsvarene i spørreundersøkelsen, hvor en av respondentene skrev: *"I etterkant av utsendt opplæring blir det naturlig med diskusjoner internt i avdelingen, dette fører til mer bevissthet rundt tema"* (Respondent fra ansatte).

Enkelte fra ledelsen mente at det er stort fokus og interesse hos de som jobber med IT og i SCADA-avdelingen, men at det trolig er varierende i resten av bedriften. En annen informant fra ledelsen skilte ikke på arbeidsområde, men uttalte at omtrent 30% av de ansatte har

egeninteresse for temaet. På spørsmål om interesse, mente derimot to superbrukere at opplæringen trolig ikke skaper interesse, men heller at de ansatte får et positivt forhold til det og får økt bevissthet knyttet til temaet.

> *"Jeg mener jo det er en interesse hvis man får folk til å tenke seg om et par ganger før man gjør noe, da har man jo automatisk en bevissthet som har festet seg inni deg.. Så lenge det er der, så er det jo nok"* (S4)

Dette kan ses i sammenheng med beskrivelsene til L4:

> "*En trenger ikke noe mer interesse enn at folk tenker seg om et par ganger før de gjør noe"* (L4)

Videre kom det frem gjennom intervjuene at en av superbrukerne og en fra ledelsen mente at det er vanskelig å skille om det er opplæringen som skaper interesse til å lære mer, eller om det er mediefokus og nærhet til risikoen gjennom andre kanaler. Dette samsvarer med L2 sitt svar på om opplæring motiverer de ansatte til å lære mer:

> *"Det klarer jeg ikke å svare på, for det vet vi ikke. Men det er jo en opplæring med det som kommer ut i aviser"* (L2)

Funnene fra intervjuene samsvarer i stor grad med svarene i spørreundersøkelsen. Svarene i spørreundersøkelsen viser at de ansatte i moderat grad blir motivert av opplæringen, og på spørsmål om de ønsker å lære mer om temaet, ligger svarene på omtrent samme nivå. Det er også en stor del som svarer «hverken eller» på disse spørsmålene.

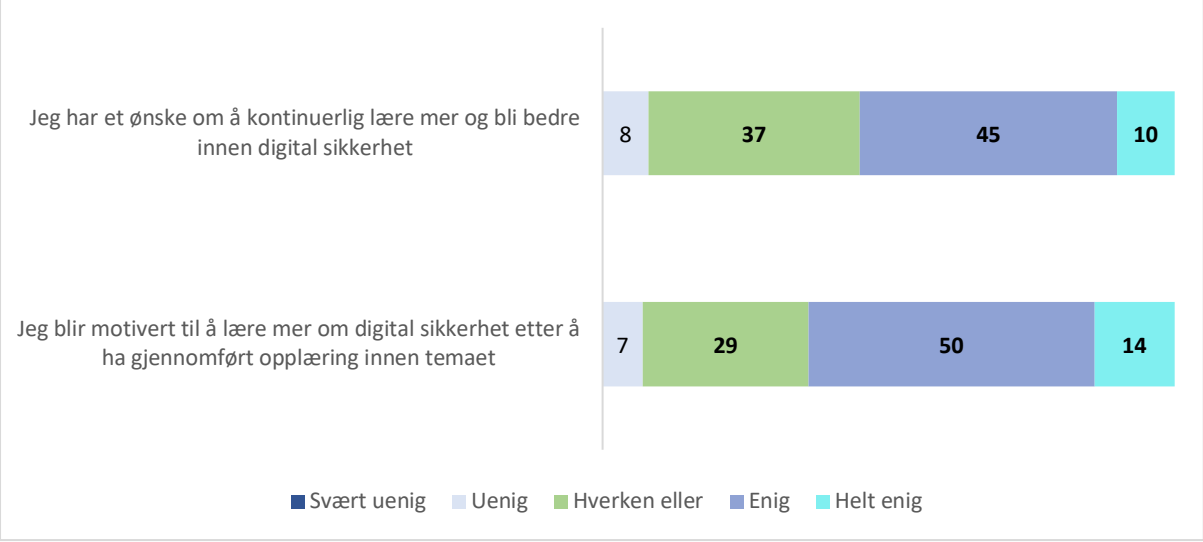


Diagram 14: Interesse - Svarene oppgitt i prosent (%)

Ingen av informantene fra ledelsen og superbrukerne mente de hadde fått tilbakemelding fra ansatte om den digitale opplæringen. Resultatene i spørreundersøkelsen viste derimot at enkelte ansatte har vist interesse ved å komme med innspill til innholdet og de digitale opplæringsmetodene.

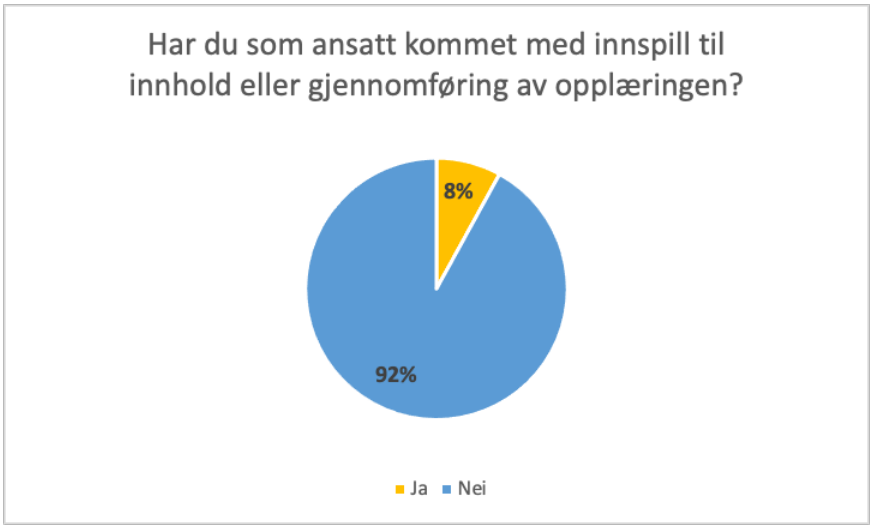


Diagram 15: Innspill til opplæringen

Oppsummering:

Ledelsen beskriver at det er mange som ikke har genuin egeninteresse for temaet, men at det heller ikke er nødvendig så lenge de er bevisst nok. Ledelsen synes det er vanskelig å vurdere om det er fokuset på temaet generelt i samfunnet som øker interessen, eller om det er opplæringen. Uansett hva interessen kommer av, vurderer ledelsen at den hjelper med å gjøre effekten av opplæringen bedre.

Svarene fra spørreundersøkelsen ser ut til å samsvare med det som fremkom i intervjuene. Den digitale opplæringen skaper interesse hos mange ansatte, men det er også flere som svarer hverken eller, og noen uenig. Enkelte ansatte viser interesse for temaet ved å gi tilbakemelding på nettselskapets opplæring om temaet.

4.5 Bivariat analyse av alder og arbeidsform

Som analyseresultatene viser over, gav enkelte informanter uttrykk for at digital opplæring ikke er tilrettelagt og kunne dermed påvirke utbyttet hos enkelte grupper. Disse gruppene var eldre og de som jobber ute. På bakgrunn av disse uttalelsene, valgte vi å gjennomføre en uavhengig to-halet t-test for å undersøke om det var statistisk signifikans mellom variablene.

Vi utarbeidet nullhypoteser for hver av effektvariablene: kompetanse, atferd, risikopersepsjon og interesse. Hver nullhypotese tok utgangspunkt i at det ikke foreligger en sammenheng mellom henholdsvis alder og arbeidsform, og effektutbytte etter digital opplæring. Vi gjør oppmerksom på at kategoriene kombinasjonsarbeid inne og ute, og utearbeid ble slått sammen grunnet for lav svarprosent i hver av dem.

		Alder		**Arbeidsform**	
		Under 50 år	Over 50 år	Kontor	Kombinasjon kontor og ute, eller ute
Kompetanse	Gjennomsnitt:	3,83	3,54	3,81	3,61
	Varians:	0,28	0,52	0,35	0,48
	Standardavvik:	0,53	0,72	0,59	0,69
	N:	30	24	32	26
	P-verdi:		0,105		0,257
Atferd	Gjennomsnitt:	3,81	3,82	3,78	3,88
	Varians:	0,29	0,33	0,24	0,36
	Standardavvik:	0,54	0,57	0,49	0,60
	N:	32	23	32	25
	P-verdi:		0,929		0,508
Risiko-persepsjon	Gjennomsnitt:	3,78	3,95	3,9	3,8
	Varians:	0,24	0,33	0,35	0,23
	Standardavvik:	0,49	0,57	0,59	0,48
	N:	32	22	32	27
	P-verdi:		0,256		0,514
Interesse	Gjennomsnitt:	3,55	3,87	3,9	3,5
	Varians:	0,79	0,39	0,54	0,66
	Standardavvik:	0,89	0,62	0,73	0,81
	N:	31	26	32	26
	P-verdi:		0,125		0,0534

Tabell 8: Bivariat analyse

Gjennomsnittsverdien er basert på de fem Likert skala-verdiene vi benyttet i spørreundersøkelsen. 1 tilsvarer "svært uenig", mens 5 er "helt enig". De fleste

gjennomsnittsverdiene ligger et sted mellom 3 og 4, noe som tilsvarer kategoriene “hverken eller” og “enig”.

I t-testen er det benyttet et konfidensintervall 95%, og p-verdi på 0,05. Ingen av p-verdiene er under 0,05, og nullhypotesene blir dermed stående. Analysen viser dermed ingen statistisk signifikans mellom variablene alder og arbeidsform, når det kommer til effektutbyttet etter digital opplæring.

5.0 Diskusjon

Hittil har vi redegjort for problemstillingen og dens aktualitet, teorier som anses som relevante, hvordan vi har valgt å operasjonalisere problemstillingen, og den gjennomførte analysen. Dette har bygd opp til diskusjon av oppgavens problemstilling: *Hvordan påvirker digital opplæring om cybersikkerhet den digitale sikkerhetskulturen i et nettselskap?*

Diskusjonskapittelet er bygd opp ved bruk av teorier fra kapittel 2, og funn fra analysen i kapittel 4. Kapittelet er delt opp i tre, hvor hvert forskningsspørsmål utgjør hver sin del. Rekkefølgen på forskningsspørsmålene er strukturert på en måte som samsvarer med rekkefølgen i problemstillingen. Dette vil si at vi først diskuterer digital opplæring i nettselskapet, for så å gå inn på digital opplæring i relasjon til nettselskapets digitale sikkerhetskultur. Dette skal til sammen kunne svare på problemstillingen.

I diskusjonskapittelet vil vi omtale ledelsen og superbrukere som "ledelsen". Dette gjør vi på bakgrunn av at begge grupper er involvert i opplæringsarbeidet, og at analysefunnene fra de to gruppene ikke ser ut til å skille seg nevneverdig fra hverandre. Det blir dermed bare skilt mellom ledelse og ansatte videre i oppgaven.

F1: Hvordan fungerer nettselskapets digitale opplæring om cybersikkerhet for å fremme læring?

Teori om sikkerhetsstyring viser til at opplæring er et virkemiddel for å styre sikkerheten i virksomheter, og er et tiltak som nettselskapet har benyttet seg av for å nå målet om cybersikkerhet i samsvarer med lovverket (Njå et al, 2020; Energiloven, 1990; Kraftberedskapsforskriften, 2012). Flere forskere vektlegger verdien av opplæring for å bedre sikkerhetskulturen (Malmedal, 2020; Sas et al., 2021; Parsons et al., 2015; Wiley et al., 2020; Daler et al, 2019; LaFrancé, 2004 referert i Talbot & Jakeman, 2009; Reason, 1997). Før vi kan gå nærmere inn på om den digitale opplæringen i nettselskapet har påvirket den digitale sikkerhetskulturen, er det nyttig å studere hvilken type digital opplæring de benytter. Videre skal dette ses i lys av ledelsens tanker bak opplæringen, og om det samsvarer med de ansattes preferanser innen læring. Dette ser vi som sentralt å diskutere, da en opplæringsmetode som

ikke samsvarer med ansattes preferanser innen læring, trolig vil ha begrenset effekt på sikkerhetskulturen. På bakgrunn av dette, skal det diskuteres hvordan digital opplæring fungerer for å lære de ansatte om cybersikkerhet.

Ifølge Roer (2015) vil læringsformer som er tilrettelagt for de ansatte, legge et godt grunnlag for læring. Funnene fra analysen viser at deler av den digitale opplæringen nettselskapet benytter er godt tilrettelagt for læring basert på de ansattes preferanser. Fordelene med digital opplæring som både ansatte og ledelsen løfter frem, viser seg å være fleksibilitet, tidseffektivitet, god bruk av ressurser, at det skaper en rolig læringssituasjon og gir mulighet for å nå ut til mange ansatte. I tillegg trekkes det frem at korte kurs om temaet fungerer godt for nærmest samtlige av respondentene. Dette samsvarer med fordeler som tidseffektivitet, fleksibilitet og uavhengighet fra tid og rom som flere forskere trekker frem (Katz, 2000; Horton, 2000; Welsh, 2022). Et annet eksempel på at nettselskapet tilrettelegger for at ansatte har ulike læringspreferanser, kan knyttes til funnene som viser at de benytter ulike digitale plattformer som eksempelvis e-læringskurs, e-post og webinar. I tillegg benyttes det både asynkrone og synkrone opplæringsformer (Hrastinski, 2008; Rosenberg, 2001; Hall, 1997). Det kan tenkes at en bredspektret bruk av plattformer kan være med på å treffe de ansattes ulike preferanser for å lære. Eksempelvis kan enkelte ansatte lære bedre ved bruk av video, mens andre foretrekker tekst. Ved å benytte ulike plattformer, kan informasjonen også nå ut til flere ansatte. Det fremkommer gjennom analysen at de ansatte verdsetter ulike former for plattformer, noe som underbygger påstanden om at nettselskapet benytter digital opplæring på en måte som samsvarer med de ansattes preferanser (Roer, 2015).

Jacobsen & Thorsvik (2016) sier at en virksomhet må sørge for at ansatte oppnår felles læring. Dette skjer ikke før ansatte formidler den lærte informasjonen til andre i virksomheten og de i fellesskap etablerer en forståelse for hvordan det skal gjøres. Funnene fra analysen viser at det ved enkelte tilfeller oppstår diskusjoner etter gjennomført opplæring. På bakgrunn av dette, kan vi argumentere for at digital opplæring har potensial for å fremme felles læring. Det er imidlertid relativt få funn som indikerer dette, og det er dermed usikkert hvor store deler av nettselskapet dette gjelder for.

Den asynkrone læringsformen har potensial for å fremme læring med bedre tid til refleksjon, ifølge Hrastinski (2008). Dette kan ses i sammenheng med Filstad (2016) og Olsen (2016) sin beskrivelse av at læring som har innslag av selvstendig utførelse, er en optimal læringsmetodikk. Både ledelsen og ansatte rapporterer at de bidrar aktivt ved e-læringskurs med quiz, og at det er mulighet for interaksjon under digitale allmøter. Funnene viser at ansatte liker e-læringskurs med quiz der det skapes aktiv deltagelse og refleksjon. Basert på funnene som viser at nettselskapet benytter aktiv deltagelse, fremstår det som den digitale opplæringen er utformet på en måte som fremmer læring hos ansatte. Dette støttes av funn fra tidligere forskning som viser at opplæring som skaper interaksjon blir godt likt og huskes i lengre tid (Skotnes, 2014).

På tross av fordeler ved å benytte aktiv deltagelse, finner vi at nettselskapet benytter flere digitale opplæringsmetoder uten aktiv deltagelse. Funnene fra de ansatte viser at opplæringsmetodene uten aktiv deltagelse, er de som skaper minst refleksjon. Aktiv deltagelse er ikke en nødvendighet i all opplæring, men trekkes frem som en styrke for å øke refleksjon, slik at informasjonen blir tatt imot og huskes (Filstad, 2016; Olsen 2016; Skotnes, 2014). På bakgrunn av dette, argumenterer vi for at enkelte av de digitale opplæringsmetodene nettselskapet benytter, potensielt ikke skaper ønskelig refleksjon under læring. Dette kan dermed virke negativt på læringseffekten. Imidlertid viser det seg at omtrent halvparten av både ansatte og ledelsen ikke ønsker mer aktiv deltagelse. Hvorvidt dette tyder på at metodene skaper nok læring uten aktiv deltagelse, eller om de ikke ønsker økt deltagelse, er usikkert. En mulig årsak til at ansatte og ledelsen ikke ønsker mer aktiv deltagelse, kan være at det krever mer tid og ressurser i gjennomføring av opplæringen. Hvis dette er tilfellet, kan det være nyttig for nettselskapet å benytte aktiv deltagelse på andre måter enn de gjør i dag. Dette fremstår spesielt viktig da spørreundersøkelsen viser at aktiv deltagelse er det verktøyet som skaper mest refleksjon, og dermed potensielt større læringsutbytte. Det fremstår som ledelsen anerkjenner behovet for økt aktiv deltagelse ettersom en større prosentandel svarer at det ikke benyttes nok i dag.

Analysen viser at den digitale opplæringen blir gjentatt for sjeldent, at innholdet er for generelt, og til tider benytter de seg av interaksjon som ikke passer med ansattes preferanser. Som nevnt vektlegger Roer (2015) og Filstad (2010) hvor viktig det er å tilpasse opplæringen etter de

ansattes behov. I tillegg argumenterer Tennant (1999) og Bednall & Sanders (2016) for at generell informasjon kan være utfordrende å overføre til praktiske hendelser. I lys av disse teoriene, kan en argumentere for at nettselskapet ikke i tilstrekkelig grad har tilpasset den digitale opplæringen til de ansattes preferanser og behov, for å kunne overføre informasjonen til praksis. En potensiell forklaring på det, er funnene som viser at ledelsen har problem med å vurdere hvilken effekt opplæringen har på de ansatte. Hvis ledelsen opplever problem med å vurdere effekten, kan det tenkes at de har manglende innsikt i hvilken opplæringsform de ansatte mener har best effekt. Denne antagelsen underbygges av analysen som viser at enkelte ansatte har gitt tilbakemelding om opplæringen, men at ledelsen ikke har innsikt i at det har skjedd. Dette kan ses i sammenheng med Roers (2015) teori som sier at opplæringen bare oppnår første trinn i firetrinns-kognitiv prosess (tabell 2), dersom læringen ikke er tilpasset de ansattes preferanser. Læring som stopper på dette nivået, vil også ha lite mulighet for å påvirke den digitale sikkerhetskulturen (Roer, 2015).

Det kan tenkes at nettselskapet har mulighet til å forbedre den digitale opplæringen for å redusere disse svakhetene, men basert på funnene ser det ikke ut til at de har gjort det til nå. Årsakene til dette kan være flere, men vi ønsker å trekke enkelte som fremkom fra analysen. Det at nettselskapet benytter generell opplæring og at kursene gjennomføres sjeldnere enn ønsket, kan ses i sammenheng med ledelsens argument om at digital opplæring er ressursbesparende. Om opplæringen skulle bestått av spesifikt innhold og blitt gjentatt ofte nok, hadde metoden krevd mer ressurser. Dette kunne ha svekket fordelen om at digital opplæring er en ressursbesparende opplæringsform (Welsh, 2022). En annen årsak kan ses i sammenheng med Hrastinski (2008) som viser til at både asynkron og synkron digital opplæring har potensial for å skape læring med et mangfoldig innhold. Dette kunne eksempelvis ført til bruk av aktiv deltagelse som samsvarer bedre med ansattes preferanser. Funnene som viser at klasseromsundervisning skaper større rom for aktiv deltagelse enn digital opplæring gjør, kunne potensielt vært mindre fremtredende hvis nettselskapet hadde tilrettelagt bedre for interaksjon i de digitale opplæringsmetodene. På bakgrunn av dette, argumenterer vi for at nettselskapet ikke har utnyttet digitale opplæringsmetoders fulle potensial for å skape best mulig læring hos de ansatte.

Ut fra teori om HRO må alle i virksomheten drive kontinuerlig læring for å ha kompetanse til å oppdage og være årvåkne på risiko (La Porte, 1996; Weick & Sutcliffe, 2007). Manglende kompetanse i deler av virksomheten, øker potensialet for at en angriper kan trenge seg inn i systemet uten å bli oppdaget ved et eventuelt cyberangrep (Bergsjø, 2020). Gjennom intervjuene med ledelsen fremkommer det at digital opplæring ikke er like godt tilrettelagt for de som jobber ute. Basert på dette funnet, kan en argumentere for at nettselskapet har valgt en opplæringsmetode som ikke er like godt egnet i alle områder av virksomheten. Basert på Roers (2015) teori om opplæring, kan det argumenteres for at det hindrer det første trinnet i firetrinns-kognitiv prosess (tabell 2) fra å bli oppnådd. Hvis de ansatte som jobber ute har dårligere utgangspunkt for å gjennomføre den digitale opplæringen, kan dette potensielt føre til at nettselskapet mangler nødvendig kompetanse om cybersikkerhet i enkelte deler av virksomheten. Det at deler av nettselskapet ikke besitter samme kompetanse om cybersikkerhet, kan potensielt øke sannsynligheten for å bli utsatt for cyberangrep (Njå et al, 2020; Malmedal, 2020). På en annen side viser analysen at de ansatte selv i stor grad opplever at arbeidsplassen legger til rette for at den digitale opplæringen kan gjennomføres. Dette svekker argumentet om at deler av virksomheten ikke får gjennomført opplæringen, og gir tro på at digital opplæring fungerer for å lære ansatte i hele nettselskapet.

Roer (2015) vektlegger at ansatte må forstå temaets relevans for å oppnå effekt av opplæringen. Til tross for fordeler og ulemper med den digitale opplæringen nettselskapet benytter i dag, fremstår det som at ansatte og ledelsen forstår alvoret knyttet til cyberangrep, og mange gir uttrykk for et ønske om å kontinuerlig lære mer. Dette underbygges av at de ansatte gjennomfører opplæringen på tross av uklare krav og manglende repetisjon av kursene. Basert på de overnevnte funnene, kan det virke som at de ansatte prioriterer cybersikkerhet, men at mangelen på kompetanse hovedsakelig kan knyttes til den digitale opplæringen. Dette underbygges av funn som viser at de ansatte gjerne skulle hatt mer kunnskap om cybersikkerhet for å utføre sitt arbeid på en trygg måte. Om den manglende kompetansen kan relateres direkte til digital opplæring som metode, eller om det handler om selskapets opplæringsstrategi, har i denne oppgaven vært utfordrende å få svar på. Gjennom diskusjonen argumenterer vi likevel for at sikkerhetsstyring ved bruk av digital opplæring har potensialet for å fremme læring hos ansatte i nettselskapet (Reason, 1997; Njå et al, 2020). Nettselskapet er dog avhengig av å optimalisere den digitale opplæringen ved å benytte de positive sidene ved læringsmetoden

ytterligere. Dette kan tenkes å skape bedre læringseffekt, sammenlignet med det som er tilfellet i dag.

Oppsummering:

Basert på funnene og teorien presentert over, kan man oppsummere F1 med at måten nettselskapet benytter digital opplæring på, delvis utnytter opplæringsmetodens potensial. I tillegg viser funnene at digital opplæring har potensial for å fremme felles læring i virksomheten. Det fremkommer likevel svakheter ved nettselskapets utnyttelse av digital opplæring, og vi argumenterer for at dette kan påvirke muligheten for å fremme læring hos ansatte. Måten nettselskapet tilrettelegger for digital opplæring, bør ta høyde for ansattes individuelle tilpasninger og ønsker for å optimalisere læringsutbyttet. Måten opplæringen blir gjennomført på, kan ha direkte påvirkning på læringsutbyttet, som igjen kan ha effekt på den digitale sikkerhetskulturen. Dette vil diskuteres videre i forskningsspørsmål 2.

F2: Hvordan påvirkes de digitale sikkerhetskultursmomentene kompetanse, atferd, risikopersepsjon og interesse av den digitale opplæringen?

Teori om digital sikkerhetskultur viser til at læring kan påvirke momentene kompetanse, atferd, risikopersepsjon og interesse (NorSIS, 2019). Dette har vi lagt til grunn i denne oppgaven, men vi vil også benytte annen sikkerhetskulturs-teori som er relevant for læring. Det at kompetanse og atferd er sentralt innen sikkerhetskultur, fremkommer også i James Reasons definisjon (1997). Reason vektlegger at momentene er sentrale både på individ og gruppenivå. På bakgrunn av dette skal forskningsspørsmål 2 løfte frem hvordan faktorer innen digital sikkerhetskultur blir påvirket av digital opplæring på et individuelt nivå, mens forskningsspørsmål 3 retter seg mot opplæringens effekt på gruppers *felles* digitale sikkerhetskultur. Diskusjonen i begge forskningsspørsmålene retter seg mot digital sikkerhetskultur på individ og gruppenivå hos *ansatte* (som beskrevet i 3.2 Forskningsmetode).

Før vi går inn på hvorvidt digital opplæring påvirker de utvalgte momentene innen digital sikkerhetskultur, ønsker vi å diskutere hvorvidt denne oppgaven kan si noe om sikkerhetskultur. Som presentert i teorikapittelet er sikkerhetskultur et komplekst fenomen å

studere (Engen et al, 2021; Schein, 2010). Ut fra at denne studien er basert på spørreundersøkelse og intervju, får vi frem de ansatte og ledelsens verdier og holdninger. Schein (2010) argumenterer for at dette ikke sier noe om kulturen i sin helhet, og en kan dermed diskutere om denne oppgaven heller studerer sikkerhetsklima. Ifølge Reichers & Schneider (1990) kan en trekke linjer mellom sikkerhetsklima og sikkerhetskultur. Dette underbygges av Teo & Feng (2008) som sier at særlig sikkerhetskulturmomentet atferd kan studeres gjennom sikkerhetsklima. Atferd anses som et sentralt mål innen cybersikkerhetsopplæring da ønsket er å gi de ansatte et handlingsmønster som fremmer rapportering, årvåkenhet og bevissthet (Bergsjø, 2020; NorSIS, 2019). Det kan diskuteres hvorvidt oppgaven sier noe om sikkerhetskultur eller klima, men basert på teorien presentert over, kan det argumenteres for at sikkerhetsklima kan si noe om den faktiske digitale sikkerhetskulturen i nettselskapet. Det fremstår likevel som en begrensning at studien er basert på et øyeblikksbilde, da kulturer er i stadig endring og gjerne krever en studie som strekker seg over lengre tid (Flin et al, 2000; Roer, 2015).

Digital opplærings påvirkning på digital sikkerhetskultur

Ettersom flere forskere viser til at opplæring har potensiale for å påvirke sikkerhetskultur, har vi i denne oppgaven lagt til grunn at en velfungerende opplæring har potensial for å styrke den digitale sikkerhetskulturen (Parsons et al, 2015; Wiley et al, 2020; Cheng & Wang 2022; Roer, 2015). Vi ønsker her å diskutere i dybden hvilken måte den digitale sikkerhetskulturen påvirkes av nettselskapets digitale opplæring. For å besvare dette spørsmålet, skal vi nå diskutere hvordan digital opplæring har påvirket NorSIS (2019) fire momenter som er relevant for læring.

Kompetanse og atferd

I lys av teoretiske grunnlaget som viser til at kunnskap som fører til kompetanse, også vil påvirke handling- og atferd (Filstad, 2016; Lai, 2013; Roer, 2015). På bakgrunn av dette velger vi å presentere kompetanse og atferd sammen.

Ifølge Bergsjø (2020) er virksomheters cybersikkerhetsarbeid avhengig av at de ansatte har en atferd preget av årvåkenhet, og rapporterer inn hendelser som fremstår mistenksomme. Enkelte informanter fra ledelsen trekker frem at opplæringen har vært avgjørende for å hindre ondsinnede aktører fra vellykkede cyberangrep. I tillegg har opplæringen ført til at ansatte viser

økt skepsis og årvåken holdning. Dette samsvarer med spørreundersøkelsen til de ansatte hvor mange rapporterer at de har fått både økt kompetanse og tryggere atferd etter den digitale opplæringen. Det at ansatte reproduserer den lærte kunnskapen til atferd, kan ses i lys av "Reproduksjonstrinnet" (Roer, 2015). Dette taler for at den digitale opplæringen nettselskapet benytter seg av, fungerer for å endre kompetansen og resulterer i atferd hvor økt årvåkenhet og rapportering oppnås (Filstad, 2016; Roer, 2015; Hopkins, 2002; Borys et al, 2009; Lai, 2013). Dette samsvarer med funn fra Hagen & Albrechtsen (2009) som viser at ansatte opplevde økt kunnskap, holdninger og atferd etter digital opplæring.

For å måle om opplæringen har ført til endret kompetanse og atferd, kan en benytte tester (Roer, 2015). Ettersom analysen utelukkende er basert på ansattes egenvurderinger, og ledelsen uttrykker stor usikkerhet knyttet til vurdering av effekt etter opplæring, kan det være utfordrende å si noe sikkert om kompetanseutbyttet og atferdsendringer. I analysen kommer det frem at nettselskapet gjennomførte en phisingtest før og etter opplæring, og dette kan dermed fremstå som en sikrere måte å måle effekten på. Til tross for at mange ansatte opplever en bedret atferd etter opplæring, viste phisingtesten at mange ansatte utførte en annen atferd enn det de er lært opp til. Atferden etter digital opplæring samsvarer dermed ikke med det som faktisk kreves for å hindre cyberangrep. Imidlertid viser analysen at ansattes utførelse av rapportering faktisk har hindret nettselskapet fra å bli utsatt for cyberangrep. Dette taler for at den digitale opplæringen har hatt effekt på de ansattes atferd og kompetanse, men på bakgrunn av resultatet fra phishingtesten argumenterer vi for at nettselskapet fremdeles har en vei å gå for å forbedre utbyttet av opplæringen.

Opplæringen innen cybersikkerhet oppfordrer til rapporterende atferd (Bergsjø, 2020). Gjennom analysen finner vi at flere opplever sin atferd som tryggere etter opplæring, men en større andel svarer at de er usikre på når og hvem de skal rapportere til. Ettersom rapportering er en sentral atferd innen cybersikkerhetsarbeid, kan en stille seg spørrende til hvorvidt de ansatte har fått en tryggere atferd etter opplæringen, da flere uttrykker usikkerhet rundt rapportering. Dette kan relateres til den digitale opplæringen, men også til nettselskapets tilrettelegging for rapportering (Roer, 2015; Reason, 1997). Da denne oppgaven setter søkelys på digital opplæring, er det dette som diskuteres videre. Hvis det er relatert til den digitale opplæringen, kan det fremstå som de ansatte har problem med å overføre informasjon som

kommer frem i opplæringen til praktisk arbeid. Mulige årsaker til dette kan være at informasjonen i opplæringen blir for generell eller at opplæringssituasjonen er for ulik praksis for rapportering (Tennant, 1999; Bednall & Sanders, 2016). Gjennom analysen kommer det frem at de ansatte savner spesifikk informasjon i opplæringen. Det kan dermed tenkes at økt bruk av spesifikke eksempler i opplæringen, kunne gjort det lettere å overføre informasjonen om rapportering ut i praksis.

Risikopersepsjon

Ifølge teori om HRO er en avhengig av at samtlige ansatte prioriterer sikkerhet, og forstår sitt ansvar for å forhindre risikoen. Det skaper en mulighet for tidlig oppdagelse av eventuelle trusler (La Porte 1996; Weick et al., 1999). Dette kan ses i sammenheng med Mearns og Flins (1995) argument om at økt risikopersepsjon fører til økt oppmerksomhet og årvåkenhet til å oppdage risikoer. Økt risikoforståelse hos ansatte er dermed et nøkkelelement for å oppdage eventuelle cybertrusler. Analysen viser at både ledelsen og ansatte anerkjenner at det er viktig at samtlige har en risikoforståelse, og flere ser en økning hos ansattes forståelse etter opplæring. I tillegg tyder flere tekstsvar fra de ansattes spørreundersøkelsen på at de forstår risikoen og innser at deres rolle er sentral for å hindre cyberangrep. Dette styrker troen på at den digitale opplæringen gir de ansatte en forståelse som påvirker deres evne til å være årvåkne og oppdage eventuelle trusler. Dette samsvarer med LaFrancé (2004) sitt synspunkt på opplærings mulighet for å styrke sikkerhetskulturen (referert i Talbot & Jakeman, 2009).

På en annen side trekker en informant fra ledelsen frem at det foreligger en usikkerhet om hvorvidt de ansatte har kjennskap til konsekvensene. Dette kan sees i sammenheng med at enkelte ansatte svarer at de tillater seg å gjennomføre handlinger som strider imot hva opplæringen sier. Ettersom cyberangrep kan føre til store konsekvenser for driften av nettselskapet, kan man stille seg spørrende til om den digitale opplæringen egentlig gir de ansatte en tilstrekkelig risikoforståelse (NOU 2015:15). En alternativ forklaring på dette funnet kan relateres til at informanten fra ledelsen har stor innsikt og forståelse for temaet. Basert på at informanten jobber med opplæring innen cybersikkerhet, kan det tenkes at det påvirker risikopersepsjonen på en annen måte enn det ansatte ellers får gjennom opplæringen. Dette kan underbygges av teori som viser at økt kunnskap fører til økt risikopersepsjon (Mearns & Flin,

1995).

Informasjon må oppdateres etter hvert som trusselbildet er i endring for å gi de ansatte en risikoforståelse som samsvarer med trusselbildet (NorSIS, 2019; Roer, 2015). Gjennom analysen fremkommer det at nettselskapet mangler repetisjon på kursene, men oppdaterer e-post- og intranettsidene i takt med trusselbildet. Der informeres det blant annet om angrep på andre selskap og trusselbildet generelt. Dette viser forsøk på å holde de ansatte oppdatert på risikoen og holde fokuset oppe, på tross av at de selv ikke har blitt utsatt for angrep (Reason, 1997). Imidlertid viser analysen at disse læringsplattformene er de minst likte for å skape refleksjon. Dette er funn som samsvarer med Skotnes (2014) hvor opplæring ved bruk av enveis-kommunikasjons-verktøy fører til vansker med å holde ved like kunnskapen. Dermed kan en stille seg spørrende til om de kontinuerlige oppdateringene gir samtlige ansatte en tilstrekkelig risikoforståelse, eller om de bare når ut til dem som liker plattformene. Sett i lys av teori som viser at ansatte har individuelle preferanser innen læringsmetodikk, kan det dermed konkluderes med at oppdatering av et begrenset utvalg læringsplattformer, gir redusert mulighet for å skape tilstrekkelig risikoforståelse hos de ansatte (Roer, 2015).

Interesse

NorSIS (2019) trekker frem at interesse er et nøkkelelement innen all læring. Funnene fra både ansatte og ledelsen viser at digital opplæring delvis skaper interesse. Hvorvidt det har noe med den digitale opplæringen å gjøre, eller temaet generelt, er utfordrende å få tak på gjennom analysen. Imidlertid trekker informanter fra ledelsen frem at målet er å skape bevissthet, og ikke nødvendigvis egeninteresse. Ettersom ledelsen er involvert i opplæringsarbeidet, kan det dermed tenkes at opplæringen bærer preg av et mål om å skape bevissthet. På bakgrunn av dette, kan det tenkes at opplæringen ikke er optimalisert til et nivå hvor det skaper tilstrekkelig interesse hos de ansatte. Hvorvidt det er godt nok med bevissthet for å beskytte seg mot cyberhendelser kan diskuteres ettersom NorSIS trekker frem at interesse er sentralt i all læring. Funn som derimot kan tale for at bevissthet er tilstrekkelig for å verne seg mot cyberhendelser, er at nettselskapet hittil ikke har blitt utsatt for vellykkede cyberangrep. En må imidlertid ta høyde for at det er utfordrende å vurdere kvaliteten på sikkerhetsarbeid, da arbeidet heller er synlig gjennom sitt fravær enn tilstedeværelse (Reason, 1997). Dermed kan vi argumentere for

at selv om nettselskapet ikke har blitt utsatt for vellykkede cyberangrep hittil, er det ikke et bevis på at bevissthet er nok for å verne nettselskapet fra cyberangrep i tiden fremover.

Opplæring handler ikke bare om opplæringsmetoden, men også hvorvidt de ansatte er mottakelig og motivert (Filstad, 2016; Roer, 2015; Reason, 1997). På bakgrunn av dette hjelper det ikke å skape en god opplæring, om ikke interesse eller fokus fra de ansatte er til stede. Analysen viser at det er mange ansatte som er interessert i å lære om temaet, men også at det er mange som ikke deler samme engasjement. Dette kan påvirke det eventuelle utbyttet de får av opplæringen (NorSIS, 2019). Selv om nettselskapet skulle hatt optimal digital opplæring, vil de med manglende interesse for temaet trolig få et mindre læringsutbytte. Imidlertid viser diskusjonen i forskningsspørsmål 1 at nettselskapets digitale opplæring trolig innehar mangler. Dette styrker troen på at det ikke bare handler om ansattes interesse og fokus under opplæringen, men også metoden i seg selv. Dermed kan vi konkludere med at effekten etter digital opplærings vil avhenge av både de ansattes innstilling og optimalisering av opplæringen.

Oppsummering:
Diskusjonen viser i korte trekk at digital opplæring har hatt påvirkning på ansattes kompetanse, atferd, risikopersepsjon og interesse knyttet til cybersikkerhet. Den digitale opplæringen har hatt positiv påvirkning på momentene, men analysen viser også at opplæringseffekten har sine begrensninger. Blant de positive sidene finner vi at opplæringen har ført til økt risikoperspesjon, kompetanse og endret atferd til et nivå hvor økt årvåkenhet, rapportering og bevissthet oppnås hos mange ansatte. Det er likevel begrensninger ved den digitale opplæringen som særlig påvirker risikopersepsjon og interesse. Momenter som trekkes frem som årsaker, er at den digitale opplæringen ikke er tilstrekkelig optimalisert i forhold til de ansattes preferanser, samt at den skaper bevissthet heller enn interesse. Det er viktig å trekke frem at det ikke alltid utelukkende handler om metoden, men også ansattes fokus og motivasjon til å lære.

F3: I hvilken grad skaper digital opplæring felles digital sikkerhetskultur i nettselskapet, og hvilke faktorer påvirker evnen til å gjøre det?

Som beskrevet i forskningsspørsmål 2 handler sikkerhetskultur om både individuelle og gruppers verdier, holdninger, kompetanse og atferd (Reason, 1997). At kultur er noe som eksisterer i fellesskap er noe som blir vektlagt i teori om organisasjonskultur, sikkerhetskultur og digital sikkerhetskultur (Reason, 1997; Schein, 1985; Malmedal, 2020). For å fremme sikkerhet i virksomheten må alle være bevisstgjort og ha nødvendig kompetanse (La Porte, 1996). Formell læring, eksempelvis gjennom digital opplæring, kan disponere til lik handling og atferd hos de ansatte, og kan på den måten ses i relasjon til fellesskapet (Filstad, 2010). Gjennom diskusjonen av forskningsspørsmål 2 fremkommer det at mange ansatte har fått en forsterket kompetanse, atferd, risikopersepsjon og interesse etter digital opplæring. Funnene viser derimot også sprik i svarene fra de ansatte innen samtlige momenter, og at ledelsen er usikre på om alle i virksomheten har effekt av opplæringen. Dette har ledet til spørsmål om hvorvidt den digitale opplæringen fungerer for å bygge felles digital sikkerhetskultur, og hvilke faktorer som påvirker evnen til å gjøre det.

I analysen trekker ledelsen frem at enkelte grupper har stort fokus og prioriterer cybersikkerhet. Her blir spesifikt IT- og SCADA-avdelingen trukket frem. På bakgrunn av dette kan en argumentere for at den digitale opplæringen har påvirket gruppers felles digitale sikkerhetskultur. På en annen side er det funn som viser at ledelsen er usikre på om det gjelder alle avdelinger. Funn fra spørreundersøkelsen underbygger at ikke alle ansatte opplever like god effekt av den digitale opplæringen. Hvis det er tilfelle at felles kultur bare er oppnådd i enkelte grupper, kan en stille seg spørrende til om dette er tilstrekkelig i cybersikkerhetsarbeidet til nettselskapet. Med tanke på at en cyberangriper gjerne benytter seg av menneskelige sårbarheter ved cyberangrep, kan en argumentere for at det er viktig at alle i virksomheten er bevisstgjort for å opprettholde sikkerheten (Martin, 2019; NOU 2015:13; La Porte, 1996). Basert på Malmedal (2020) sitt argument om at det er nødvendig å skape en felles kultur innen cybersikkerhet, fremstår det som om nettselskapet ikke har oppnådd en felles helhetlig digital sikkerhetskultur på virksomhetsnivå. Med andre ord viser funnene at den digitale opplæringen har ført til at enkelte grupper opplever en felles digital sikkerhetskultur, men at dette ikke gjelder for nettselskapet som helhet.

Når det kommer til hvilke faktorer som kan påvirke nettselskapets evne til å skape felles digital sikkerhetskultur, anses det å være flere som kan knyttes til digital opplæring. I det følgende skal vi diskutere noen av dem. Nettselskapet bedriver digital opplæring som et sikkerhetsstyringstiltak, med mål om økt bevissthet, årvåkenhet og rapporterende atferd hos de ansatte. Dette vil si at nettselskapet driver formell opplæring hvor læring skal føre til felles handling og atferd (Filstad, 2010). Det å forvente at et sikkerhetsstyringstiltak som digital opplæring skal føre til felles handlinger og atferd, velger vi å se i sammenheng med teori om hvorvidt en kultur kan styres. Det fremstår som at nettselskapet har en funksjonalistisk tilnærming til kultur, hvor det foreligger en forventning om at innholdet i den digitale opplæringen skal bli mottatt og implementert (Huang et al., 2007; Lee & Harrison, 2000; Nævestad, 2009; Alvesson, 2002; Smiricich, 1983; Reason, 1997). Derimot viser analysen at ikke alle ansatte oppnår samme effekt av opplæringen. En kan dermed diskutere hvorvidt nettselskapets digitale opplæring fungerer for å skape felles digital sikkerhetskultur.

En mulig faktor til at den digitale opplæringen ikke oppnår felles digital sikkerhetskultur, kan knyttes til hvorvidt en har en funksjonalistisk eller fortolkende tilnærming til kulturbegrepet. Ut fra den fortolkende forståelsen av kultur, vil et styringstiltak som digital opplæring ikke fungere for å endre den digitale sikkerhetskulturen (Alvesson, 2002; Haukelid, 2008). Det kan tenkes at det allerede eksisterer kulturer i nettselskapet som påvirker den digitale opplæringens effekt. Dette underbygger en oppfatning om at et sikkerhetsstyringstiltak som digital opplæring ikke nødvendigvis fører til en felles digital sikkerhetskultur, hvor samtlige i like stor grad blir bevisstgjort. Den fortolkende tilnærmingen kan også ses i relasjon med teori om at det kan eksistere subkulturer i en organisasjon (Kaufmann & Kaufmann, 1996; Bang, 1995; Schein, 1984). Funn fra analysen viser at eldre og de som jobber ute potensielt kan oppfattes som en subkultur der den digitale opplæringsformen ikke passer like godt og dermed påvirker effekten. Derimot viste ikke den gjennomførte t-testen noen statistisk sammenheng (Tabell 8: Bivariat analyse). Funnene kunne dermed ikke være med på å underbygge teorien om at det eksisterer subkulturer i nettselskapet, og at dette har påvirket den felles digitale sikkerhetskulturen. Det kan likevel ikke utelukkes at det eksisterer andre subkulturer i nettselskapet enn de som ble undersøkt i denne studien. I en subkultur kan det oppstå krefter som kan motarbeide ledelsens styringstiltak, og kan dermed begrense nettselskapet mulighet for å oppnå en felles digital sikkerhetskultur (Haukelid, 2001). Det kan tenkes at eventuelle andre subkulturer kan påvirke

digital opplærings effekt på den felles digitale sikkerhetskulturen, men dette har ikke denne studien tilstrekkelig empirisk grunnlag for å si noe om.

En annen mulig forklaring på hvorfor digital opplæring ikke har skapt en felles digital sikkerhetskultur på virksomhetsnivå, kan diskuteres ved å trekke inn Jacobsen og Thorsviks (2016) teori om felles læring, igjen. De sier at virksomheter må sørge for at læring ikke stopper med individuell læring, og må jobbe for en felles læring. Det at funnene fra analysen viser at den digitale opplæringen har ulik læringseffekt hos de ansatte, kan tyde på at den digitale opplæringen ikke skaper felles læring i tilstrekkelig grad. Det kan være flere grunner til at ansatte oppnår ulik læringseffekt. Som presentert i forskningsspørsmål 1, kan en årsak være at den digitale opplæringen bare delvis treffer de ansattes preferanser innen læring. Det kan dermed ikke utelukkes at optimalisering av nettselskapets digitale opplæring kunne ført til felles digital sikkerhetskultur i større grad.

En annen årsak til at nettselskapet ikke oppnår felles digital sikkerhetskultur, kan ses i lys av Filstads (2010) beskrivelse av at det eksisterer både uformell og formell læring. Utfordringen med uformell læring er at det kan påvirke den felles digitale sikkerhetskulturen i nettselskapet, ettersom ulike informasjonskilder kan gi motstridende eller upålitelig informasjon (Bergsjø et al, 2020). Uformelle læringsplattformer som fremkommer i analysen er informasjon fra media og samfunnet, og diskusjon med kollegaer. Dermed kan det tyde på at den digitale opplæringen, altså den formelle opplæringsformen, ikke er den eneste læringsformen som påvirker den digitale sikkerhetskulturen. På bakgrunn av dette, argumenterer vi for at både mangel på optimalisering av digital opplæring, og påvirkning av uformell læring, er faktorer som påvirker digital opplærings evne til å skape en felles digital sikkerhetskultur på virksomhetsnivå.

Oppsummering:

Gjennom diskusjonen i F3 fremkommer det at den digitale opplæringen har evne til å skape felles digital sikkerhetskultur i enkelte deler av nettselskapet. Videre fremkommer det at det også er andre elementer som påvirker den digitale sikkerhetskulturen, noe som begrenser den digitale opplæringens evne til å påvirke kulturen alene. De identifiserte momentene er hvorvidt en kultur kan styres, svakheter i opplæringsmetoden som begrenser evnen til å skape felles

læring, samt påvirkning av uformell læring. Vi konkluderer dermed med at den digitale opplæringen har evne til å påvirke deler av nettselskapets digitale sikkerhetskultur, men ikke til å skape en felles digital sikkerhetskultur i hele virksomheten.

6.0 Konklusjon

Formålet med denne oppgaven har vært å studere hvordan digital opplæring om cybersikkerhet påvirker den digitale sikkerhetskulturen i et nettselskap. På bakgrunn av dette ble følgende problemstilling formulert: *Hvordan påvirker digital opplæring om cybersikkerhet den digitale sikkerhetskulturen i et nettselskap?*

Det første forskningsspørsmålet tar for seg hvordan nettselskapets digitale opplæring fungerer for å fremme læring. Her trekkes det frem både fordeler og ulemper ved nettselskapets opplæring. Påvirkende faktorer anses å være knyttet til at nettselskapet til en viss grad benytter fordeler ved digital opplæring som fremmer læring hos ansatte. Likevel konkluderes det med at nettselskapet ikke utnytter digital opplærings fulle potensial, og dermed ikke har optimalisert opplæringen på en måte som virkelig fremmer læring hos ansatte. Vi argumenterer for at optimalisering av den digitale opplæringen kunne fremmet læring ytterligere, og dermed påvirket den digitale sikkerhetskulturen i større grad.

Det andre forskningsspørsmålet tar for seg hvordan de digitale sikkerhetskulturmomentene kompetanse, atferd, risikopersepsjon og interesse, påvirkes av digital opplæring. Basert på at digital opplæring delvis har hatt effekt på momentene, viser det seg at digital opplæring har påvirket den digitale sikkerhetskulturen. Fordelene ved den digitale opplæringsmetoden knyttes til at den skaper økt årvåkenhet og risikoforståelse hos de ansatte. Dette viser at atferden og kompetansen er forbedret, men det er likevel usikkerhet knyttet til om det er godt nok for å verne nettselskapet mot cyberangrep. Det eksisterer også svakheter ved metoden som særlig knyttes til at den skaper for lite interesse og ikke påvirker sikkerhetskulturmomentene i tilstrekkelig grad hos samtlige ansatte. Det må også bemerkes at utbyttet de ansatte får av den digitale opplæringen alltid vil bli påvirket av deres innstilling til å lære.

Det tredje forskningsspørsmålet tar for seg i hvilken grad digital opplæring skaper en felles digital sikkerhetskultur i nettselskapet, og hvilke faktorer som påvirker evnen til å gjøre det. Basert på funnene som viser at digital opplæring har ført til felles digital sikkerhetskultur på gruppenivå, mener vi at opplæringsmetoden har potensial for å påvirke en felles kultur. Likevel vil det være faktorer som begrenser muligheten for at digital opplæring alene skaper en felles digital sikkerhetskultur på virksomhetsnivå. Det konkluderes med at påvirkende faktorer er hvorvidt en kultur kan styres, uformelle læringsmetoder, og svakheter ved nettselskapets digitale opplæring.

I lys av de empiriske funn og diskusjonen rundt disse, kan vi konkludere med at med at nettselskapets digitale opplæring innen cybersikkerhet til en viss grad påvirker den digitale sikkerhetskulturen. Den digitale opplæringen ser ut til å påvirke digital sikkerhetskultur hos både individ og grupper, men ikke til et nivå hvor nettselskapet som helhet får en felles digital sikkerhetskultur. Dette blir ansett som en svakhet ettersom en felles digital sikkerhetskultur kan redusere risikoen for å bli rammet av cyberangrep. Det vil likevel trekkes frem at digital opplæring har en sentral påvirkning på den digitale sikkerhetskulturen og har en tydelig effekt på bevisstgjøring innen cybersikkerhet.

6.1 Forslag til videre forskning

Som nevnt tidligere i oppgaven krever kulturstudier gjerne andre datainnsamlingsmetoder og gjerne over lengre tid. På bakgrunn av dette ville det vært interessant å forske videre på temaet ved bruk av en annen metodetilnærming. Studiet kunne for eksempel brukt observasjon eller intervju med både ansatte, ledelsen og andre relevante aktører. En slik tilnærming kunne gitt ytterligere innblikk og dypere forståelse i temaet. Det kunne også vært aktuelt å studere digital sikkerhetskultur ved bruk av en longitudinell studie, hvor en eksempelvis vurderer sikkerhetskulturen før og etter digital opplæring.

En annen interessant vinkling kunne være å studere to eller flere nettselskap hvor det benyttes digital opplæring, og sammenlignet de ulike digitale opplæringsmetodenes effekt på digital sikkerhetskultur. Ettersom enkelte ansatte rapporterer at de savner fysiske kurs, kunne det også vært hensiktsmessig å sammenligne effekt av digital opplæring med fysisk opplæring. Videre kunne det også vært av interesse å studere om det eksisterer flere subkulturer, eller andre moment som anses som relevant for den fortolkende tilnærmingen til kultur, og dens eventuelle påvirkning på effekten av et sikkerhetsstyringstiltak som digital opplæring.

I denne oppgaven har vi utelukkende undersøkt momenter innen digital sikkerhetskultur som er relevant for læring, og dermed kunne det vært aktuelt å studere om digital opplæring også har effekt på andre digitale sikkerhetskulturmoment, som eksempelvis vilje til digitalisering og tillit.

7.0 Litteraturliste

Alnatheer, M., Chan, T., & Nelson, K., (2012) *Understanding and Measuring Information Security Culture.* Doktorgradsavhandling. Queensland University of Technology. https://core.ac.uk/download/pdf/18312508.pdf

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*(10), 1-10. https://doi.org/10.1016/j.cose.2020.102003

Alvesson, M. (2002). *Organisasjonskultur og ledelse.* Oslo: Abstrakt forlag

Antonsen, S. (2009a) *Safety culture: Theory method and improvement.* Farnham: Ashgate.

Antonsen, S. (2009b). *Safety culture and the issue of power.* Safety Science, 47, 183–191. https://doi.org/10.1016/j.ssci.2008.02.004

Bandura, A., & Walters, R.H. (1963). *Social learning and personality development.* Holt Rinehart and Winston: New York.

Bang, H. (1995). *Organisasjonskultur.* Tano Aschehoug.

Bang, H. (2011). *Organisasjonskultur.* Universitetsforlaget.

Basak, S.K., Wotto, M., Bélanger, P. (2018) *E-learning, M-learning and D-learning: Conceptual definition and comparative analysis*. 15 (4) s.191-216. DOI: 10.1177/2042753018785180

Bednall, T.C. & Sanders, K. (2016). *Do Opportunities for Formal Learning Stimulate Follow-Up Participation in Informal Learning? A Three-Wave Study.* Human Resource Management, *56*(5), s.803-820. https://doi.org/10.1002/hrm.21800

Bergsjø, H. (2020). Hendelseshåndtering og opprydding. I H. Bergsjø, R. Windvik & L. Øverlier (Red.), *Digital sikkerhet* (s. 267-278). Universitetsforlaget.

Blaikie, N. (2010). *Designing Social Research: The Logic of Anticipation*. (2.utg.). Cambridge: Polity Press

Blaike, J. & Priest, N. (2019). *Designing Social Research* (3. utg.). Polity Books.

Borys, D., Else, D. & Leggett, S. (2009). *The fifth age of safety: The adaptive age. Journal* of Health & Safety Research and Practice, *1*(1), 19-27. https://www.researchgate.net/publication/287564530_The_fifth_age_of_safety_The_adaptive_age

Brinkmann, S. & Tanggaard, L. (2012). Intervjuet. I S. Brinkmann & L. Tanggaard (Red.), *Kvalitative metoder* (s. 17-45). Gyldendal akademisk.

Cheng, E. C. K. & Wang, T. (2022). I*nstitutional Strategies for Cybersecurity in Higher Education Institutions.* Information, 13(4), 192. https://doi.org/10.3390/info13040192

Cooper, M. D. (2016). *Navigating the safety culture construct: A review of the evidence.* International Conference on Safety Culture.

Cox, S. & Cox, T. (1991). *The structure of employee attitudes to safety: A European example.* Work and Stress, 5(2), 93–106. https://doi.org/10.1080/02678379108257007

Cox, S. & Flin, R. (1998). *Safety culture: Philosopher's stone or man of straw?* Work and Stress, 12(3), 189–201. https://doi.org/10.1080/02678379808256861

Daler, T., Gulbrandsen, R., Høie, T. A. & Sjølstad, T. (2019). *Håndbok i datasikkerhet – informasjonsteknologi og risikostyring* (4. utg.). Bergen: Fagbokforlaget

D'Arcy, J. & Greene, G. (2014). *Security culture and the employment relationship as drivers of employees' security compliance*. Information Management Computer Security, 22(5), 474-489. DOI:10.1108/IMCS-08-2013-0057

DeCuir-Gunby, J. T. (2008). Mixed methods Research in the Social Sciences IJ. W. Osborne (Red.), *Best Practices in Quantitative Methods* (s. 125-134). Sage Publication.

Digitaliseringsdirektoratet (u.å) *Veileder for kartlegging av digital sikkerhetskultur*. Digdir.no https://www.digdir.no/informasjonssikkerhet/veileder-kartlegging-av-digital-sikkerhetskultur/2142

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

Edwards, J. R. D., Davey, J., & Armstrong, K. (2013). Returning to the roots of culture: A review and re-conceptualisation of safety culture. Safety Science, 55, 70–80. https://doi.org/10.1016/j.ssci.2013.01.004

Energiloven. (1990). *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.* (LOV-1990-06-29-50). Lovdata. https://lovdata.no/dokument/NL/lov/1990-06-29-50?q=energiloven

Engen, O. A. H., Gould, K. A. P., Kruke, B. I., Lindøe, P. H., Olsen, K. H. & Olsen, O. E. (2021). *Perspektiver på samfunnssikkerhet*. Cappelen Damm akademisk.

Filstad, C. (2010). Organisasjonslæring – fra kunnskap til kompetanse. Bergen: Fagbokforlaget

Filstad, C. (2016). *Organisasjonslæring – fra kunnskap til kompetanse* (2. utg.). Bergen: Fagbokforlaget

Flin, R., Mearns, K., O´Connor, P., Bryden, R. (2000) *Measuring safety climate: identifying the common features.* Safety Science. 34 (1-3) s. 177-192. https://doi.org/10.1016/S0925-7535(00)00012-6

Furnham, A., & Gunter, B. (2015). *Corporate Assessment – Auditing a company's personality*. Routledge.

Guldenmund, F. (2018). Understanding safety culture through models and metaphors. Gilbert, C., Journe, B., Laroche, H., Bieder, C. (Red) *Safety cultures, Safety models: Taking stock and moving forward* (s. 21–34). Springer Publishing.

Gripsrud, G., Olsson, U.H., Silkoset, R. (2021) *Metode, dataanalyse og innsikt*. (4 utg). Oslo: Cappelen Damm

Grønmo, S. (2016). *Samfunnsvitenskapelige metoder*. Fagbokforlaget.

Hagen, J., Albrechtsen, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377-397. https://doi.org/10.1108/09685220810908796

Hagen, J. & Albrechtsen, E. (2009). Effects on employees´ information security abilities by e-learning. *Information Management & Computer Security*, *17*(5), 388-407. https://doi.org/10.1108/09685220911006687

Hall, B. (1997), Web-based Training Cookbook. New York: John Wiley and Sons

Harvey, J., Erdos, G., Bolam, H., Cox, M. A. A., Kennedy, J. N. P., & Gregory, D. T. (2002). An Analysis of Safety Culture Attitudes in a Highly Regulated Environment. Work and Stress, 16(1), 18–36. DOI:10.1080/02678370110113226

Haukelid, K. (2001). *Oljekultur og sikkerhetskultur.* Oslo: Universitetet i Oslo.

Haukelid, K. (2008). Theories of (safety) culture revisited—An anthropological approach. Safety Science, 46, 413–426 https://doi.org/10.1016/j.ssci.2007.05.014

Henriqson, E., Schuler, B., Van Winsen, R., & Dekker, S. W. A. (2014). The constitution and effects of safety culture as an object in the discourse of accident prevention: A Foucauldian approach. Safety Science, 70, 465–476. DOI: 10.1016/j.ssci.2014.07.004

Hopkins, A. (2002). *Safety Culture, Mindfulness and Safe Behaviour: Converging Ideas?* Working Paper 7. https://neuro.bstu.by/ai/To-dom/My_research/Review-DONE/Cisim-2009/Safety-culture/wp%25207%2520-%2520Hopkins.pdf

Hopkins, A., (2016). Quiet Outrage: The way of a sociologist. Wolters Kluwers. https://doi.org/10.1111/1468-5973.12158

Horton, W. (2000), Designing Web-based Training. New York: John Wiley and Sons.

Huang, D. T., Clermont, G., Sexton, J. B., Karlo, C. A., Miller, R. G., Weissfeld, L. A., Rowan, K. M., & Angus, D. C. (2007). Perceptions of safety culture vary across the intensive care units of a single institution. Critical Care Medicine, 35, 165–176. DOI: 10.1097/01.CCM.0000251505.76026.CF

Hrastinski, S. (2008) *Asynchronous and synchronous e-learning*. https://www.researchgate.net/publication/238767486_Asynchronous_and_synchronous_e-learning

Jaatun, M. G., Moe, M. E. G., Nordbø, P. E. (2017). Sikkerhetsbetraktninger rundt selvhelende distribusjonsnett. (NEF-2017). SINTEF. Hentet fra https://docplayer.me/47710028-Sikkerhetsbetraktninger-rundt-selv-helendedistribusjonsnett.html

Jacobsen, D. I., (2005) *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode.* (2.utg) Høyskoleforlaget.

Jacobsen, D. I., & Thorsvik, J. (2016). *Hvordan organisasjoner fungerer.* Bergen: Fagbokforlaget.

Johannessen, A., Tufte, P. A. & Christoffersen, L. (2016). *Samfunnsvitenskapelig metode* Abstrakt forlag.

Johnson, E. C. (2006). *Security awareness: switch to a better programme.* Network Security, (2), 15-18. https://doi.org/10.1016/S1353-4858(06)70337-3

Jore, S. (2017) *The Conceptual and Scientific Demarcation of Security in Contrast to Safety.* European Journal for Security Research.4, s.157-174. https://doi.org/10.1007/s41125-017-0021-9

Jore, S. (2020). Safety and Security Culture - Dual or distinct Phenomena? I C. Bieder & K. A. P. Gould (Red.), *The Coupling of Safety and Security - Exploring Interrelations in Theory and Practice* (s. 43-51). Springer Open. https://library.oapen.org/bitstream/handle/20.500.12657/41716/978-3-030-47229-0.pdf?sequence=1 - page=49

Kaufmann, G., & Kaufmann, A. (1996). *Psykologi i organisasjon og ledelse.* Fagbokforlaget.

Katz, Y. J. (2000). *The comparative suitability of three ICT distance learning methodologies for college level instruction*. Educational Media International, 37(1), 25–30. https://doi.org/10.1080/095239800361482

Kono, T. (1990). Corporate culture and long-range planning. Long Range Planning, 23(4), 9–19. https://doi.org/10.1016/0024-6301(90)90148-W

Kraftberedskapsforskriften. (2012). *Forskrift om sikkerhet og beredskap i kraftforsyningen* (FOR-2012-12-07-1157). Lovdata. https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M. & Halgand, Y. (2015). *A survey of approaches combining safety and security for industrial control systems.* Reliability engineering & system safety, 139, 156-178. https://doi.org/10.1016/j.ress.2015.02.008

Krumsvik, (2014)

Kvale, S. & Brinkmann, S. (2015). *Det kvalitative forskningsintervju* (3. utg.). Gyldendal akademisk.

Lai, L. (2013). *Strategisk kompetanseledelse* (3.utg). Bergen: Fagbokforlaget

La Porte, T. R. (1996). High Reliability Organizations: Unlikely, Demanding and At Risk. *Journal of Contingencies and Crisis Management*, *4*(2), 60-71. https://doi.org/10.1111/j.1468-5973.1996.tb00078.x

Le Coze, J. C. (2019). *How can safety culture can make us think*. Safety Science, 118, 221–229 DOI:10.1016/j.ssci.2019.05.026

Lee, T., & Harrison, K. (2000). Assessing Safety Culture in Nuclear Power Stations. Safety Science, 34(1–3), 61–97. https://doi.org/10.1016/S0925-7535(00)00007-2

Liang, G., Weller, S. R., Zhao, J., Lou, F., Dong, Z. Y. (2016) The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. Transactions on Power Systems. 32 (4) s.3317-3318. Doi: 10.1109/TPWRS.2016.2631891

Lundberg, C. C. (1990). Surfacing organizational culture. Journal of Managerial Psychology, 5(4), 19–26 https://doi.org/10.1177/105256299602000102

Malcolmson, J. (2009). *What is Security Culture? Does it differ in content from general Organisational Culture?* Security Technology. Doi: 10.1109/CCST.2009.5335511

Malmedal, B. (2020). Sikkerhetskultur. I H. Bergsjø, R. Windvik & L. Øverlier (Red.), *Digital sikkerhet* (s. 33-46). Universitetsforlaget.

Malterud, K. (2017). *Kvalitative forskningsmetoder for medisin og helsefag* (4.utg.). Universitetsforlaget

Martin, P. (2019). *The rules of security: staying safe in a risky world*. Oxford University Press.

Mearns, K., & Flin, R. (1995). *Risk perception and attitudes to safety by personnel in the offshore oil and gas industry: a review.* Journal of Loss Prevention in the Process Industries, s. 299-305. https://doi.org/10.1016/0950-4230(95)00032-V

Njå, O., Sommer, M., Rake, E.L., Braut, G.S., (2020) *Samfunnssikkerhet - Analyse, styring og evaluering*. Universitetsforlaget

Norges vassdrags- og energidirektorat (2015). Økonomisk regulering av nettselskap. NVE. https://www.nve.no/reguleringsmyndigheten/regulering/nettvirksomhet/oekonomisk-regulering-av-nettselskap/

Norges vassdrags- og energidirektorat NVE (2017). Regulering av IKT-sikkerhet. (26- 2017). http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

Noregs vassdrags- og energidirektorat NVE (2020). *Veiledning i kraftberedskapsforskriften*. NVE. https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/veiledning-til-kraftberedskapsforskriften/

Norges vassdrag- og energidirektorat NVE (2021). *IKT-sikkerhetstilstanden i kraftforsyningen 2021.* Ekstern rapport nr. 19/2021. NVE. https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_19.pdf

Norges vassdrag- og energidirektorat NVE (u.å) Nettvirksomhet. https://www.nve.no/reguleringsmyndigheten/regulering/nettvirksomhet/

NorSIS. (2019). *Nordmenn og digital sikkerhetskultur*. Norsk Senter for Informasjonssikring. https://norsis.no/content/uploads/2022/05/kulturrapport_2019_web_komprimert.pdf

NorSIS. (2021). *Trusler og trender 2021*. NorSIS. https://norsis.no/content/uploads/2022/05/NorSIS_Trusler_Trender_2021_Digital.pdf

NOU 2015:13. (2015). *Digital sårbarhet - sikkert samfunn*. Departementenes sikkerhets-og serciceorganisasjon. https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NSM (2022). *Risiko 2022.* Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

NSR – Næringslivets sikkerhetsråd (2020). Mørketallsundersøkelsen 2020. Næringslivets sikkerhetsråd. https://www.nsr-org.no/aktuelt/m%C3%B8rketallsunders%C3%B8kelsen-2020

NSR – Næringslivets sikkerhetsråd (2022). *Mørketallsundersøkelsen.* https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen

Nævestad, T.-O. (2009). *Mapping Research on culture and Safety in High-Risk Organizations: Arguments for a Sociotechnical Understanding of Safety Culture.*

Journal of Contingencies and Crisis Management, 7(2), s. 126–136. https://doi.org/10.1111/j.1468-5973.2009.00573.x

Olsen, T. H. (2016). *Kompetanseutvikling.* I A. Mikkelsen & T. Laudal (Red.), Strategisk HRM 2: HMS, etikk og internasjonale perspektiver (2. utg., s. 238-276). Oslo: Cappelen Damm

Pallant, J. (2010). *SPSS Survival Manual. A step by step guide to data analysis using SPSS* (4 utg.pall). Maidenhead: Open University Press, McGraw-Hill Education.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R. & Jerram, C. (2015). *The Influence of Organizational Information Security Culture on Information Security Decision Making.* Cognitive Engineering and Decision Making, 9(2), 117-129. DOI:10.1177/1555343415575152

Pidgeon, N. (1998) *Risk assessment, risk values and the social science programme: Why we do need Risk Perception Research.* Reliability Engineering & System Safety, 59 (1) s. 5-15. https://doi.org/10.1016/S0951-8320(97)00114-2

Reason, J. (1997) *Managing the risk of organizational accidents.* Ashgate Publishing Limited.

Reichers, A. E., & Schneider, B. (1990). Climate and culture: An evolution of constructs. I Schneider, B. (Red), *Organizational climate and culture* (s. 5-39). San Francisco: Jossey-Bass.

Renn, O. (2008). *Risk Governance – Copin with Uncertainty in a Complex World.* Earthscan Ltd.

Rochlin, G.I. (1993). Defining "High Reliability" organizations in practice: A taxonomic prologue. I Roberts K., H. (Red.), *New challenges to understanding organizations* (s. 11– 32). New York: Macmillan.

Roer, K., 2015. *Build a security culture*. Cambridgeshire: IT Governance Publishing.

Rosenberg, M. J. (2001), *E-learning: Strategies for delivering knowledge in the digital age.* New York: McGraw-Hill.

Sas, M., Reniers, G., Ponnet, K. & Hardyns, W. (2021). The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour. *Safety Science*, *144*. https://doi.org/10.1016/j.ssci.2021.105447

Schein, E. H. (1984). Culture as an environmental context for careers. *Journal of Organizational Behavior*, 5 (1) s. 71-81. https://doi.org/10.1002/job.4030050107

Schein, E. H. (1985). *Organizational Culture and Leadership.* Jossey-Bass Publishers.

Schein, E. H. (2010). *Organizational Culture and Leadership* (4 utg.) San Francisco: Jossey-Bass

Schultz, M. (2004). *Kultur i Organisationer - Funktion eller symbol* (1 utg.). Kjøbenhavn: Handelshøjskolens Forlag.

Sintef (2021) *Cybersikkerhet og barrierestyring.* Hentet fra https://www.sintef.no/prosjekter/2021/cybersikkerhet-og-barrierestyring/

Skotnes, R. Ø. (2014). Management commitment and awareness creation – ICT safety and security in electric power supply network companies. *Information & Computer Security*, *23*(3), 302-316. https://doi.org/10.1108/ICS-02-2014-0017

Skotnes, R. Ø. (2015). Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector. Doktoravhandling, Universitetet i Stavanger. https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/2374441/Ruth_Skotnes.pdf?sequence=1&isAllowed=y

Smircich, H. (1983). Concepts of Culture and Organizational Analysis. *Administrative Science Quarterly, 28*, 339-358. doi: 10.2307/2392246

Tashakkori, A., Teddlie, C. (2010) *Handbook of mixed methods in social & behavioral research.* Thousand Oaks: SAGE

Talbot, J. & Jakeman, M. (2009) *Security Risk Management: Body of Knowledge*. John Wiley Sons Inc.

Tennant, M. (1999) *Understanding and learning to work.* I Boud, D. & Garrick, J (red.). London: Routledge.

Teo, E.A., & Feng, Y. (2008) *The Role of Safety Climate in Predicting Safety Culture on Construction Sites.* Architectual Science Review. 52 (1) s.5-16. https://doi.org/10.3763/asre.2008.0037

Tjora, A., (2018). *Viten skapt: Kvalitativ analyse og teoriutvikling*. Cappelen Damm Akademisk

Thaagard, T. (2018) *Systematikk og innlevelse – en innføring i kvalitativ metode.* (5 utg.). Fagbokforlaget.

UiO (26.09.2017) *Nettskjema-diktafon mobil.* Universitetet i Oslo. https://www.uio.no/tjenester/it/adm-app/nettskjema/hjelp/diktafon.html

van Niekerk, J. & von Solms, R. (2005). *A holistic framework for the fostering of an information security sub-culture in organizations*. Centre for Information Security Studies, South Africa. https://digifors.cs.up.ac.za/issa/2005/Proceedings/Full/041_Article.pdf

Veccio-Sudus, A., & Griffiths, S. (2004). Marketing strategies for enhancing safety culture. *Safety Science*, 42(7), s. 601-619, DOI:10.1016/j.ssci.2003.11.001

Vierendeels, G., Reiniers, G., Nunen, K. & Ponnet, K. (2018). *An integrative conceptual framework for safety culture:* The Egg Aggregated Model (TEAM) of safety culture. Safety Science, 103, 323-339. https://doi.org/https://doi.org/10.1016/j.ssci.2017.12.021

Weick, K.E., Sutcliffe, K. & Obstfeld, D. (1999). Organizing for High Reliability: Process of Collective Mindfulness. I Sutton, R., S. & Staw, B., M. (Red.), *Research in Organizational Behavior*, Vol. 21. (s. 81–123). Stanford: Jai Press.

Weick, K.E. & Sutcliffe, K.M. (2007). *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. San Fransisco, California: Jossey-Bass.

Welsh, E. T., Wandberg, C. R., Brown, K. G., Simmering, M. J., (2022) *E-learning: emerging uses, empirical results and future directions*. Training and Development. 7 (4) 228-320 DOI:10.1046/j.1360-3736.2003.00184.x

Wiley, A., McCormac, A. & Dragana, C. (2020). *More than the individual: Examining the relationship between culture and Information Security Awareness*. Computers & Security, 88. DOI:10.1016/j.cose.2019.101640

Wæhle, E., Dahlum, S., Grønmo S., (2020, 14.mai) *Case-studie*. Store norske leksikon. https://snl.no/case-studie

Yin, R., K. (2014) *Case study research design and methods* (5 utg.). Sage: Thounsand Oaks

8.0 Vedlegg

8.1 Intervjuguide

Bakgrunn:

- Hva er din stillingstittel?
- Kan du fortelle litt om hvordan dere jobber med cybersikkerhet?
- Hvem har ansvaret for kursing innen cybersikkerhet hos dere?
- Hvordan er du involvert i cybersikkehetsarbeidet?

Opplæringsmetoder i nettselskapet:

- Hvilke digitale opplæringsmetoder benytter nettselskapet for å styrke kompetanse knyttet til cybersikkerhet hos de ansatte?
- Hvilken form for digitale opplæringsmetoder benytter dere?
  - Kan du beskrive om det kreves interaksjon fra de ansatte i de digitale opplæringsmetodene, og hvordan det utføres?
- Er det krav til hvor ofte ansatte må gjennomføre digitale opplæringskurs knyttet til cybersikkerhet? I så tilfelle hvor ofte?
  - Hvis ja: Hvordan opplever du at de ansatte forholder seg til disse kravene?
  - Hvis nei: opplever du at de ansatte gjennomfører opplæring selv om det ikke eksisterer krav?

Ditt syn på digitale opplæringsverktøy:

- Opplever du at den digitale opplæringen selskapet gjennomfører bidrar til at menneskene som jobber her blir mer bevisst på temaet cybersikkerhet? Utdyp gjerne.
- Kan du beskrive hvordan de ansatte tar i bruk informasjonen de tilegner seg gjennom opplæring?
- Har du sett økt årvåkenhet/rapportering hos de ansatte etter hvert som den digitale opplæringen har blitt gjennomført?
  - Utdyp gjerne
- Hvordan opplever du at den digitale opplæringen påvirker de ansattes syn på cyberhendelser som en risiko?
  - Opplever du at de ansatte tar cybersikkerhet alvorlig, og ser du tegn til atferd som samsvarer med det?
- Hvilken form for digitale opplæringsmetoder opplever du at fungerer best for å øke de ansattes kompetanse? Utdyp gjerne hvorfor.
- Opplever du at digital opplæring er tilstrekkelig for at de ansatte får en atferd som samsvarer med det nettselskapets forventninger relatert til cybersikkerhet?
- Opplever du at digital opplæring motiverer de ansatte til å lære mer om temaet digital sikkerhet?
  - Hvis ja: Tilpasser nettselskapet ønsket om å lære mer, eller må de ansatte oppsøke andre kilder til informasjon på egenhånd?
- Får de ansatte en mulighet til påvirke hva som vektlegges i opplæringen?
- Får de ansatte en mulighet til å påvirke hvilke opplæringsmetoder som benyttes?
  - Hvis ja: Opplever du at sikkerhetsarbeidet blir forbedret etter involvering fra andre ansatte?
- Opplever du at digital opplæring alene er tilstrekkelig for å bygge kompetanse om digital sikkerhet?
- Opplever du at digital opplæring fungerer bedre på noen ansatte/deler av virksomheten enn hos andre?

Selskapets digitale opplæringsverktøy innen cybersikkerhet:

- Kan du utdype hvordan selskapet har benyttet digital opplæring de siste årene?
    - Opplever du endring i opplæringsmetodene/innholdet i opplæringen?
- Kan du beskrive hvordan nettselskapet prioriterer å holde seg oppdatert vedrørende digitalt trusselbilde?
    - Gjør de andre ansatte det samme?
- Opplever du at nettselskapet oppdaterer innholdet i de digitale læringskursene i en hastighet som samsvarer med endringene i trusselbildet?
- Er det faktorer som begrenser virksomheten i å gjennomføre optimale digitale opplæringsmetoder/opplæringsinnhold?
    - Hvis ja: Hvilke?
    - Hvis ja: Hvordan tror du manglende opplæringsmetoder påvirker sikkerheten i nettselskapet?

8.2 Spørreundersøkelsen til ansatte og ledelsen

Spørsmål	Svaralternativ
Hvilken form for arbeid består din hverdag av?	Kontorarbeid Ute i felt En kombinasjon av kontorarbeid og ute i felt Annet
Alder	16 – 20 år 21 – 30 år 31 – 40 år 41 – 50 år 51 – 60 år 61 eller eldre
Hvilke digitale kommunikasjonsverktøy benytter du i arbeidshverdagen?	PC Nettbrett Mobil Annet
Hvilke opplæringsmetoder tilbyr arbeidsplassen din innen temaet digital sikkerhet?	E-læringskurs med quiz E-læringskurs uten quiz Direktesendt seminar (webinar) Informasjonsplansjer på intranett Videokurs på interne nettsider Informasjon per e-post Ingen Annet
Hvilke opplæringsmetoder tilbyr arbeidsplassen din innen temaet digital sikkerhet? – Annet	(Tekstsvar)
Hvor ofte gjennomfører du opplæring om digital sikkerhet?	Oftere Fire ganger årlig To ganger årlig En gang årlig Annethvert år Hvert femte år Sjeldnere Aldri
Hvor ofte mener du en bør gjennomføre opplæring for å få tilstrekkelig kompetanse om digital sikkerhet?	Oftere Fire ganger årlig To ganger årlig En gang årlig Annethvert år Hvert femte år Sjeldnere
Hvor lenge foretrekker du at digitale kurs varer for å oppnå best læringsutbytte?	1-5 minutt 5-15 minutt 15-60 minutt Flere timers kurs Heldagskurs

Du opplever større læringsutbytte når du selv kan bestemme tidspunkt og hastighet underveis i opplæringen?	I svært liten grad I liten grad Middels I stor grad I svært stor grad
Jeg lærer gjennom å snakke med mine kollegaer om temaet digital sikkerhet?	Svært uenig Uenig Hverken eller Enig Helt enig
Hvilken type innhold i opplæring fungerer best for å øke din interesse innen temaet?	Generell informasjon Spesifikke eksempler fra hendelser som har skjedd Innhold som kan benyttes på flere arenaer enn jobb
Er aktiv deltakelse viktig å benytte i digital opplæring?	Svært uenig Uenig Hverken eller Enig Helt enig
Hvilken type opplæringsmetode fungerer best for å skape refleksjon underveis i opplæringen?	E-læringskurs med quiz E-læringskurs uten quiz Direktesendt seminar (webinar) Informasjonsplansjer på intranett Videokurs på interne nettsider Informasjon per e-post Ingen Annet (tekstsvar)
Hvilken form for aktiv deltagelse foretrekker du under opplæring?	Chat/kommunikasjon via tekst underveis i kurset Quiz i e-læringskurs Oppgaveløsning i diskusjon med andre Annet Foretrekker ingen form for aktiv deltagelse
Benytter din arbeidsplass nok aktiv deltagelse i opplæringen?	Ja Nei
Sett vekk fra digitale opplæringsmetoder, er det andre opplæringsmetoder du skulle sett mer av? (Eksempelvis fysisk foredrag)	Ja Nei
Hvis du svarte ja på forrige spørsmål, hvilke andre opplæringsmetoder ønsker du?	Fysiske foredrag Kurs med praktisk øvelse Annet

	Ønsker bare digitale opplæringsmetoder
Hvis du svarte ja på forrige spørsmål, hvilke andre opplæringsmetoder ønsker du? - Annet	(Tekstsvar)
Hvor lenge har du vært ansatt på din nåværende arbeidsplass	0-5 måneder 6 måneder - 1 år 1-3 år 3-5 år 5-10 år 10 år eller mer
Nettselskapet legger til rette for at du kan gjennomføre opplæring i din arbeidshverdag?	Helt enig Enig Hverken eller Uenig Svært uenig
Har du som ansatt kommet med innspill til hvordan opplæringen bør gjennomføres?	Ja Nei
Beskriv hvordan du mener at opplæring bidrar til å skape en kultur på arbeidsplassen med fokus på digital sikkerhet?	(Tekstsvar)
Kompetanse	
Jeg synes selskapet har nok opplæring innen digital sikkerhet	Helt enig Enig Hverken eller Uenig Svært uenig
Jeg får tilstrekkelig med kunnskap om digital sikkerhet gjennom opplæringen selskapet benytter	Helt enig Enig Hverken eller Uenig Svært uenig
Selskapet benytter opplæringsverktøy som øker de ansattes kompetanse om digital sikkerhet	Helt enig Enig Hverken eller Uenig Svært uenig
Opplæringen er med på å øke kompetansen knyttet til hva som kan true sikkerheten ved bruk av digitale tjenester	Helt enig Enig Hverken eller Uenig Svært uenig
Opplæringen jeg har fått i selskapet gjør meg rustet til å vurdere hva som er trygt ved bruk av digitale tjenester	Helt enig Enig Hverken eller Uenig Svært uenig
Interesse	
Jeg blir motivert til å lære om digital sikkerhet etter å ha gjennomført opplæring innen temaet	Helt enig Enig

	Hverken eller Uenig Svært uenig
Jeg har et ønske om å kontinuerlig lære mer og bli bedre innen digital sikkerhet	Helt enig Enig Hverken eller Uenig Svært uenig
Atferd	
Jeg kjenner meg trygg på hva jeg skal se etter for å gjenkjenne og hindre digitale angrep	Helt enig Enig Hverken eller Uenig Svært uenig
Jeg kjenner meg trygg på når jeg skal rapportere ved mistanke om digitale angrep	Helt enig Enig Hverken eller Uenig Svært uenig
Jeg kjenner meg trygg på hvem jeg skal rapportere til ved mistanke om digitale angrep	Helt enig Enig Hverken eller Uenig Svært uenig
Jeg opplever at min adferd ved bruk av digitale tjenester har blitt tryggere etter opplæringen	Helt enig Enig Hverken eller Uenig Svært uenig
Risikopersepsjon	
Opplæringen gjør meg og andre ansatte bevisst på hvilke hendelser som kan true digital sikkerhet	Helt enig Enig Hverken eller Uenig Svært uenig
Opplæringen gir deg innblikk i selskapets forventninger til deg for å forhindre digitale trusselhendelser	Helt enig Enig Hverken eller Uenig Svært uenig
Jeg tillater meg ikke å gjøre ting jeg vet strider mot hva jeg har lært om digital sikkerhet	Helt enig Enig Hverken eller Uenig Svært uenig
Jeg tror ikke jeg kan forårsake sikkerhetstruende hendelser siden jeg har fått opplæring om hva som er forventet av meg	Helt enig Enig Hverken eller Uenig

	Svært uenig
Kontrollspørsmål	
Jeg tror jeg kan forårsake en sikkerhetstruende hendelse selv om jeg har fått opplæring av hva som er forventet av meg	Helt enig Enig Hverken eller Uenig Svært uenig
Grunnet manglende opplæring på jobb, må jeg lese meg opp på temaet på egenhånd	Helt enig Enig Hverken eller Uenig Svært uenig

8.3 Informasjonsskriv

Vil du delta i forskningsprosjektet

«Bevisstgjøring om cybersikkerhet i nettselskap»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å få innsikt i nettselskaps opplæringsarbeid relatert til cybersikkerhet, og hvordan dette arbeidet påvirker sikkerhetskulturen. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

For å verne om kritiske infrastrukturer, som eksempelvis kraftsektoren, er det viktig med grundig bevisstgjøringsarbeid relatert til cybersikkerhet. Formålet med dette mastergradsprosjektet er å se på hvordan nettselskaper driver bevisstgjøringsarbeid rettet mot cybersikkerhet, og hvilke effekt bevisstgjøringsarbeidet faktisk har på de ansatte og den helhetlige sikkerhetskulturen i virksomheten. Vi ønsker også å identifisere om det er forskjeller i hvordan ledelsen, beredskapsavdelingen og andre ansatte ser på temaet.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Stavanger er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Du blir nå spurt om å ta del i prosjektet ettersom du passer inn i oppgavens formål. Vi ønsker intervju med personell som jobber med opplæring innen cybersikkerhet og ledelse i virksomheten. Vi ser for oss å intervjue til sammen om lag ti personer som passer innenfor disse stillingstitlene. I tillegg ønsker vi å gjennomføre en spørreundersøkelse hos andre ansatte.

Personer i ledelsen i din virksomhet har anbefalt oss å ta kontakt med deg ettersom du kan gi oss informasjon som er nyttig i vårt mastergradsprosjekt. Vi håper derfor at du vil dele din innsikt i temaet med oss!

Hva innebærer det for deg å delta?

Til personer som skal intervjues:

Ditt bidrag i prosjektet vil være å stille til *ett* intervju med varighet på omtrent 30 minutter til en times tid. Noe slingring i tid kan medregnes. Intervjuet vil foregå som en samtale hvor vi snakker om hvordan ditt inntrykk er av selskapets bevisstgjøringsarbeid relatert til cybersikkerhet, og hvordan du mener det påvirker sikkerhetskulturen.

Samtalen vil foregå med deg og to mastergradsstudenter. Det vil bli benyttet lydopptaker under intervjuet med hensikt om å kunne gjengi det som fremkommer i samtalen på en korrekt måte. Lydbandopptaket vil være tilgjengelig for de to prosjektlederne for masteren, og vil bli slettet kort tid etter intervjuet er gjennomført. Du vil bli anonymisert i den endelige oppgaven.

Til personer som skal gjennomføre spørreundersøkelse:

Hvis du velger å delta i prosjektet, innebærer det at du fyller ut et spørreskjema. Spørreskjemaet består av 28 spørsmål og har til hensikt å kartlegge hvordan du opplever effekten av ulike opplæringsmetoder, og hvordan det påvirker den totale sikkerhetskulturen i virksomheten. Spørreundersøkelsen vil ta omtrent 10-15 minutter å gjennomføre.

Resultatene fra intervjuene og spørreundersøkelsen vil benyttes i masteroppgaven for å belyse og drøfte formålet med studien. Ditt bidrag vil være med på å gi innsikt i nettselskapenes bevisstgjøringsarbeid og sikkerhetskultur, og kan bidra til forbedrings- og prioriteringsarbeid i tiden fremover.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Dersom du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi grunn. Alle dine personopplysninger og informasjon du har delt vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg relatert til prosjektet eller arbeidsplassen hvis du ikke ønsker å delta eller velger å trekke deg. Samtykket må trekkes før 01.05.23 grunnet innleveringsdato for masteroppgaven.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Universitetet i Stavanger er behandlingsansvarlig institusjon, og de to prosjektansvarlige vil være de eneste som har tilgang til dine opplysninger.

For å sikre trygg oppbevaring av intervjumateriale vil det benyttes godkjent lydbandopptaker for forskningsprosjekt, og lydopptaket vil slettes så snart intervjuet er skrevet om til tekst. Dette vil skje innen en uke etter gjennomført intervju. Intervjumateriale i tekstformat vil oppbevares på datamaskin med. Dine personopplysninger oppbevares innelåst, og vil bli erstattet med en kode som lagres på en navneliste adskilt dra øvrige data.

De eneste som vil ha tilgang til personrelatert informasjon og materiale fra intervju og spørreundersøkelse er de to ansvarlige for mastergradsprosjektet. Under prosjektarbeidet vil navn og kontaktopplysningene dine bli erstattet med en kode som lagres på egen navneliste som er adskilt fra øvrig datamateriale. Materialet vil bli innelåst i en safe hvor bare forfattere av masteroppgaven har tilgang. Både selskap og personopplysninger vil være anonymisert i den endelige oppgaven, og dermed ikke mulig å gjenkjenne.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Prosjektet vil etter planen avsluttes 15.06.23. Intervjumateriale vil bli tatt opp på lydopptak, og skrevet om til ordrett tekst. Materialet vil bare være tilgjengelig for forfattere av masteroppgaven. Lydopptak vil slettes så snart intervjuet er omgjort til skriftlig format. Skriftlig intervjumateriale vil bli slettet ved prosjektsslutt i juni 2023. Liste over informanter vil være innelåst underveis i prosjektet, og blir distribuert ved prosjektsslutt. Både navn på intervjupersonene og nettselskap vil bli anonymisert i masteroppgaven.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Stavanger har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

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

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

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

- Universitetet i Stavanger ved prosjektledere:
  - Mari Lekve Bjelle: E-post 264699@uis.no
  - Tonje Stamnes Lindbom: E-post 267522@uis.no
  - Veileder av prosjektet er Kenneth Arne Pettersen Gould: E-post kenneth.a.pettersen@uis.no
- Vårt personvernombud:
  - Rolf Jegervatn, E-post: personvernombud@uis.no

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

- Personverntjenester på epost (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Kenneth Arne Pettersen Gould — (Veileder)

Tonje Lindbom & Mari Lekve Bjelle — (Studenter/forfattere)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet "*Bevisstgjøring av cybersikkerhet i nettselskap"*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju
- å delta i spørreundersøkelse

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

---

(Signert av prosjektdeltaker, dato)

8.4 NSD godkjenning

Prosjekttittel

Masteroppgave i samfunnssikkerhet: Bevisstgjøring om cybersikkerhet i nettselskap

Behandlingsansvarlig institusjon

Universitetet i Stavanger / Det teknisk- naturvitenskapelige fakultet / Institutt for sikkerheit, økonomi og planlegging

Prosjektansvarlig

Kenneth Arne Pettersen Gould

Student

Mari Lekve Bjelle & Tonje Stamnes Lindbom

Prosjektperiode

01.01.2023 - 15.06.2023

Kategorier personopplysninger

- Alminnelige

Lovlig grunnlag

- Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 15.06.2023.

Kommentar

OM VURDERINGEN

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

FØLG DIN INSTITUSJONS RETNINGSLINJER

Vi har vurdert at du har lovlig grunnlag til å behandle personopplysningene, men husk at det er institusjonen du er ansatt/student ved som avgjør hvilke databehandlere du kan bruke og hvordan du må lagre og sikre data i ditt prosjekt. Husk å bruke leverandører som din institusjon har avtale med (f.eks. ved skylagring, nettspørreskjema, videosamtale el.) Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

MELD VESENTLIGE ENDRINGER

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

OPPFØLGING AV PROSJEKTET

Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!