UiT Norges arktiske universitet

Fakultet for naturvitenskap og teknologi

# Cybersikkerhetskultur – en studie av interne organisatoriske mekanismers påvirkning

Christer Thomassen Furøy

Masteroppgave i Samfunnssikkerhet, SVF-3920, juni 2023

Antall ord: 20 649

# Sammendrag

Som et av verdens mest digitaliserte land forvalter norske virksomheter store deler av sine verdier gjennom det digitale domenet. Digitalisering er viktig for både vekst og verdiskapning, men sikkerhetsutfordringene er også store, og de senere års nasjonale trusselvurderinger har hatt et økende fokus på den digitale trusselen. Derfor er cybersikkerhet som begrep blitt mer fremtredende de siste årene. Det er blitt en erkjennelse at mennesket blir sett på som det svakeste leddet i cybersikkerhetsarbeidet, hvor så mye som 80% av digitale angrep kan skyldes menneskelig feil. Den menneskelige faktoren i cybersikkerhetsarbeidet har derfor fått et økende fokus. For å styre de ansatte mot en sikker digital atferd blir en god cybersikkerhetskultur sett på som løsningen på mange av de digitale sikkerhetsutfordringene virksomheter står ovenfor.

Samfunnsområdet forskning og utvikling er et at områdene nasjonale trusselvurderinger peker på som spesielt utsatt for cyberangrep. Det har i denne studien blitt gjennomført en kvalitativ forskningsstudie hvor en virksomhet tilhørende samfunnsområdet forskning og utvikling har vært gjenstand for denne studiens formål og problemstilling.

Denne studien har søkt å øke forståelsen om hvordan interne organisatoriske mekanismer som ledelse, kommunikasjon, evaluering, ris og ros, trening, og læring, påvirker cybersikkerhetskultur i en virksomhet. Funnene fra studien viser at ledelse, kommunikasjon og trening er de tre mekanismer som utpeker seg til å ha størst effekt på cybersikkerhetskultur. De ansattes bevissthet, kunnskap og holdninger til cybersikkerhet påvirkes av en engasjert ledelse, av tydelig og relevant kommunikasjon, og relevant og regelmessig trening. Det er identifisert suksesskriterier og fallgruver ved mekanismene som kan fremme eller hemme arbeidet med å bygge en god cybersikkerhetskultur. Samtidig er det et samspill mellom mekanismene som gjør at arbeidet med å bygge en god cybersikkerhetskultur er avhengig av et helhetlig og systematisk arbeid med alle mekanismer.

# Forord

Denne oppgaven markerer slutten på fem flotte år ved UiT Norges Arktiske Universitet.

Først og fremst vil jeg rette en stor takk til Maria og Mirva for deres tilgjengelighet, gode innspill og konstruktive tilbakemeldinger i veiledning av oppgaven.

En stor takk rettes til nærmeste familie for god støtte gjennom alle studieår. Til slutt vil jeg takke medstudenter, som gjennom både bachelor- og mastergrad har bidratt til å gjøre studietiden til en positiv opplevelse. Det har vært inspirerende og motiverende å studere med så mange engasjerte og dyktige mennesker.

# Innholdsfortegnelse

## Figuroversikt

# 1 Innledning

## 1.1 Bakgrunn

Norge er det femte mest digitaliserte landet i verden, hvor hele 92% av norske husholdninger er tilkoblet internett (European Commision, 2022). For Norges verdiskapning og vekst er digitalisering avgjørende. Digitaliseringen bidrar også til at samfunnet er tryggere og mer sikkert (Meld. St. 38 (2016-2017), 2017). I Stortingsmelding 10 – Risiko i et trygt samfunn, trekkes informasjons- og kommunikasjonsteknologi (IKT)-sikkerhet fram som et sentralt område innen samfunnssikkerhet (Meld. St. 10 (2016-2017), 2016). I 2017 kom den første stortingsmeldingen om IKT-sikkerhet. I denne peker regjeringen på forebyggende sikkerhet og virksomheters egenevne til å beskytte seg mot digitale hendelser som av særlig betydning for nasjonal IKT-sikkerhet (Meld. St. 38 (2016-2017), 2017). For å øke virksomheters egenevne til å beskytte seg mot digitale hendelser nevnes det i «Tiltaksoversikt til nasjonal strategi for digital sikkerhet», utgitt av Departementene i 2019, at ledelse, risikostyring, og å inkludere digital sikkerhet i virksomhetskulturen er tiltak for å øke egenevnen.

Det legges også vekt på at den nasjonale evnen til å avdekke og håndtere digitale angrep avhenger av et helhetlig og systematisk arbeid med IKT-sikkerhet. Samtidig fremheves også viktigheten av en pålitelig IKT-infrastruktur og sikkerhetskompetanse på alle nivå (Meld. St. 10 (2016-2017), 2016). En systematisk tilnærming vil blant annet avhenge av en god digital sikkerhetskultur i virksomhetene og vil være avgjørende for å unngå uønskede hendelser. I tillegg til teknologiske løsninger er også riktig kunnskap, ferdigheter og holdninger blant de ansatte en forutsetning for at virksomheter kan operere sikkert i det digitale domenet. Virksomheter har derfor et ansvar for at de ansatte, gamle som nye, blir bevisstgjort mulighetene, men også de sikkerhetsutfordringene som digitalisering bidrar til. Samtidig som de ansatte får nødvendig opplæring og mulighet til videre kompetansebygging innen digital sikkerhet (Departementene, 2019)

Allerede i 2012 i rapporten Nasjonalt Risikobilde, påpekte Direktoratet for Samfunnssikkerhet og Beredskap (DSB) at «mange virksomheter og enkeltindivider undervurderer risikoen ved dårlig informasjonssikkerhet.» (DSB, 2012, s, 74). I de senere år har flere av de nasjonale trusselvurderingene utgitt av Nasjonal Sikkerhetsmyndighet (NSM), Politiet, Telenor, Politiets Sikkerhetstjeneste (PST) og Norsk Senter for Informasjonssikring (NorSIS) hatt et økende fokus på den digitale trusselen. For eksempel ser NSM en økning i ondsinnet digital aktivitet mot norske virksomheter og peker på særlig tre samfunnsområder

som er spesielt utsatt for cyberangrep: teknologibedrifter, forskning og utvikling, og til slutt offentlige forvaltningsorganer (NSM, 2022b). Trusselvurderingen fra 2023 bærer også preg av det digitale risikobildet (NSM, 2023). I Norge har virksomheter blitt utsatt for flere store angrep de siste årene. I desember 2021 ble hotellkjeden Nordic Choice utsatt for løsepengevirus, og videre gjennom høytiden ble Nortura og Nordland fylkeskommune også offer for løsepengevirus (NSM, 2022b). Noen måneder senere, i mai 2022 ble en database hos karttjenesten Norkart kompromittert og persondata som inneholdt navn, adresser og fødselsnummer om 3,3 millioner nordmenn kom på avveie (NSM, 2023)

I sin trusselvurdering for 2023 viser PST til nettverksoperasjoner som en av metodene fremmede stater vil utnytte seg av, i hovedsak med spionasje- og etterretningsformål, for å få tilgang til sensitiv eller gradert informasjon. Nettverksoperasjoner initieres som regel med informasjonsinnhenting, i den hensikt å identifisere sårbarheter som senere kan utnyttes. Enkeltpersoner som for eksempel politiske beslutningstakere, forskere og militært personell er i større grad enn tidligere år utsatt for nettverksoperasjoner (PST, 2023). Konsekvensene av angrepene har variert fra store økonomiske tap, driftsforstyrrelser, leveranseutfordringer m.m., og både forbrukere, kunder og virksomhetene selv rammes av slike angrep.

For eksempel kan person-, eller bedriftssensitiv informasjon komme på avveie og utnyttes av angripere umiddelbart ved for eksempel utpressing, eller ved senere anledninger som et ledd i større angrep. Det er for eksempel anslått at 10.1 milliarder euro ble betalt i løsepenger i bare 2019 (NorSIS, 2021; PST, 2023). Penger som er med på å bidra til å finansiere de kriminelle miljøene ytterligere. I dag er de digitale verdikjedene komplekse, mye på grunn av at de er lange og uoversiktlige (NSM, 2022b). Dette betyr at et angrep hos en liten virksomhet på den ene siden av kloden, kan sette en eller flere større virksomheter ut av spill på den andre siden av kloden. Det betyr for eksempel at et sykehus i Norge kan miste tilgang på pasientjournaler, fordi leverandøren av systemet er utsatt for angrep (NorSIS, 2021).

I Politiets trusselvurdering fra 2022 pekes det på at vellykkede datainnbrudd ofte muliggjøres av mennesker, vitende eller uvitende. Helt opp mot 80% av alle cyberangrep kan skyldes menneskelige feil (Nobles, 2018). Mennesker er derfor å anse som det svakeste leddet innen digital sikkerhet og er en av de største utfordringene for organisasjoner. Et utsagn det er bred støtte for i litteraturen (Da Veiga, 2016; Nobles, 2018; Nätt & Heide, 2021; Van Niekerk & Von Solms, 2010). Det er heller ikke uvanlig at ansatte på en arbeidsplass er av oppfatningen at cybersikkerhet er IT-avdelingens ansvar (Alshaikh & Adamson, 2021; Reegård et al.,

2019). Med slike holdninger blir det utfordrende for organisasjoner å oppnå et høyt nivå av cybersikkerhet.

Teknologiske løsninger alene kan ikke forhindre angrep eller uønskede hendelser. Men i kombinasjon med velinformerte og kompetente medarbeidere kan organisasjoner gjøre det enda vanskeligere for angripere å finne sårbarheter som kan utnyttes. Kompetente og velinformerte ansatte er fruktene man høster av en god sikkerhetskultur. Virksomheter er nødt til å fokusere på den menneskelige faktoren i cybersikkerhetsarbeidet. Å bygge en god cybersikkerhetskultur er en måte å sørge for at cybersikkerhet praktiseres i hele organisasjonen, fra ledere på toppen av hierarkiet til de ansatte lenger ned i hierarkiet. Det bidrar til riktig tankesett og økt bevisstheten rundt cybersikkerhet (ENISA, 2018). Dette kan være avgjørende for hvorvidt virksomheter klarer å navigere trygt i det digitale domenet og unngå å bli utsatt for angrep eller andre uønskede hendelser, som kunne vært avverget ved en god cybersikkerhetskultur.

## 1.2 Avgrensning

Cybersikkerhetskultur påvirkes av både interne og eksterne organisatoriske mekanismer. Hvorav eksempler på eksterne påvirkningsmekanismer kan være den nasjonale cybersikkerhetskulturen, nasjonalt/internasjonalt lovverk slik som for eksempel General Data Protection Regulation (GDPR), eller standarder som f.eks. ISO 27000-serien (Huang & Pearlson, 2019). Denne oppgavens fokus er på cybersikkerhetskultur på et organisatorisk nivå og vil derfor avgrenses til å undersøke hvordan interne organisatoriske mekanismer påvirker cybersikkerhetskulturen i virksomheter, i den hensikt å bidra til ytterligere kunnskap og forståelse om de interne mekanismenes påvirkning. Oppgavens bakgrunn for hvilke organisasjoner det skal forskes på tar utgangspunkt i NSMs trusselvurdering fra 2022, og vil videre i oppgaven rette oppmerksomheten mot samfunnsområdet forskning og utvikling.

## 1.3 Tidligere forskning

Solms (2000) argumenterte for at utviklingen innen informasjonssikkerhet best kan beskrives ved å dele det opp i tre bølger, i perioden fra tidlig 80-tallet til midten av 90-tallet. Den første bølgen omtaler han som den «tekniske bølgen». I denne perioden hadde informasjonssikkerhet en teknisk tilnærming, hvor utfordringer var noe som ble ansett og best kunne løses ved hjelp av tekniske hjelpemidler. På dette tidspunktet ble informasjonssikkerhet sett på som å være ansvar tilhørende IT-avdelingene og ikke et ledelsesansvar (Solms, 2000)

Den andre bølgen blir omtalt som «ledelsesbølgen». Etter utviklingen av internett og digitaliseringen av handel, ble ledelsen i organisasjonene i større grad involvert i informasjonssikkerhetsarbeidet. Dette resulterte i informasjonssikkerhetspolicyer og utnevnelsen av personer som kunne lede informasjonssikkerhetsarbeidet. I tillegg ble organisatoriske strukturer etablert for lettere å rapportere og videreutvikle prosedyrer innen informasjonssikkerhet (Solms, 2000).

Den tredje og siste bølgen, «institusjonelle bølgen», viet den menneskelige faktoren større oppmerksomhet. Tekniske hjelpemidler alene var ikke nok for å oppnå god sikkerhet. I tillegg til en god teknisk infrastruktur og utvikling av prosedyrer, ble informasjonssikkerhetskultur et viktig fokusområde. Arbeidet med å få informasjonssikkerhet til å bli et vedvarende tankesett hos alle ansatte i sitt daglige arbeid var en viktig faktor. (Solms, 2000)

Tanken om å vie den menneskelige faktoren større oppmerksomhet har gjort cybersikkerhet som begrep mer fremtredende. Cybersikkerhet favner bredere enn informasjonssikkerhet i den forstand at den menneskelige faktoren vies større oppmerksomhet, hvor blant annet mennesket blir sett på både som mål og deltakende part i cyberangrep, vitende eller uvitende, men også som en ressurs som trenger beskyttelse. (Reid & Van Niekerk, 2014; Von Solms & Van Niekerk, 2013) I starten av århundret argumenterte Schlienger og Teufel (2002) for et paradigmeskifte hvor fokuset rettes mot den menneskelige faktoren, hvor man ser på mennesket som en ressurs i stedet for det svakeste leddet.

Men selv forskning publisert tiår senere peker fortsatt på at mennesker blir sett på som problemet i stedet for løsningen (Zimmermann & Renaud, 2019). Erkjennelsen av at mennesket er problemet har fått forskere til å tenke på kulturbygging som en løsning, og cybersikkerhetskultur er introdusert som et ferskt begrep i nyere tid. Samtidig blir cybersikkerhetskultur sett på som et forskningsfelt som fortsatt er i utvikling og som det ikke er forsket nok på frem til nå (Mwim & Mtsweni, 2022).

Mye av forskningen som er gjort på cybersikkerhet har viet mye av oppmerksomheten mot de teknologiske løsningene. Men på grunn av de menneskelige sårbarhetene er ofte ikke teknologien i seg selv nok. Det er behov for tiltak som adresserer den menneskelige faktoren, og cybersikkerhetskultur blir ansett som ett slikt tiltak (Mwim & Mtsweni, 2022). Dette begrepet har også fått mer fotfeste i de senere år fordi forskere begynte å erkjenne at en organisasjons sikkerhetskultur er et viktig element i å opprettholde et tilfredsstillende

sikkerhetsnivå (Ruighaver et al., 2007). Samtidig argumenterer Gcaza og Von Solms (2017) for at cybersikkerhetskultur er et «ill-defined» problem. Med det mener de at det er uklart hvilke elementer som utgjør selve problemet eller løsningen med cybersikkerhetskultur, og at informasjonen man trenger for å beskrive eller løse problemet enten er ufullstendig eller fraværende. Dette peker de på som områder som trenger mer forskning.

Det er allikevel forsket noe på hvilke faktorer som både påvirker og dikterer arbeidet med å bygge cybersikkerhetskultur. Flere forskere (Georgiadou et al., 2022; Huang & Pearlson, 2019; Mwim & Mtsweni, 2022) har identifisert flere av de faktorer som påvirker cybersikkerhetskultur, og utviklet modeller og rammeverk som danner grunnlaget for det videre arbeidet med å bygge en god cybersikkerhetskultur. Georgiadou et al. (2022) utviklet et rammeverk som består av en kombinasjon av organisatoriske og individuelle faktorer, som sammen utgjør cybersikkerhetskultur. En annen tilnærming kommer fra Huang & Pearlson (2019) og har som en del av sin forskning utarbeidet en modell (figur 2, s. 19) som inkluderer interne organisatoriske mekanismer, men også mekanismer utenfor de organisatoriske grensene, såkalte eksterne mekanismer. De påpeker i sin studie at enhver leder sitt mål med cybersikkerhet er å styre de ansatte mot en sikker digital adferd. Dette gjøres gjennom å bygge en god cybersikkerhetskultur. Denne kulturen påvirkes av både de interne og eksterne mekanismene. De eksterne mekanismene kan ikke ledelsen påvirke, men de interne mekanismene kan ledelsen direkte påvirke for å styre ansattes adferd. Huang & Pearlson (2019) identifiserte de seks interne mekanismer som: Lederskap, kommunikasjon, evaluering, ris og ros, trening, og læring.

Tidligere forskning på cybersikkerhetskultur har definert begrepet og poengtert den viktige rollen mennesket har i dette arbeidet (Corradini, 2020; Da Veiga, 2016; Huang & Pearlson, 2019; Zimmermann & Renaud, 2019) De rammeverk og modeller som er utviklet i forbindelse med forskningen på cybersikkerhetskultur peker på flere elementer som skal bidrar til å styre adferden til individene i en ønsket retning. Det handler om å forvandle mennesket fra å være den største svakheten til å bli den ekstra barrieren eller «brannmuren» som organisasjonene trenger for å beskytte seg. Men hvordan interne organisatoriske mekanismer, slik som de identifiserte mekanismene fra Huang & Pearlson (2019), påvirker cybersikkerhetskulturen er lite utbredt. Hvordan påvirker for eksempel kommunikasjon eller trening denne kulturen. Om noen faktorer har større effekt enn andre, og hvordan faktorene oppleves å påvirke cybersikkerhetskulturen hos ledere og ansatte, er meg bekjent lite utbredt i forskningen. Dette vil oppgaven utforske videre.

## 1.4 Problemstilling

Cybersikkerhetskultur er et felt det er gjort lite eller begrenset med forskning på frem til nå. Noe kan forklares med det som Gcaza og Von Solms (2017) refererer til – cybersikkerhetskultur er et «ill-defined» problem. Den tidligere forskningen som er gjort har identifisert flere elementer en cybersikkerhetskultur består av og hvilke ulike mekanismer som påvirker den, for eksempel kunnskap, trening og ledelse. Med denne oppgaven ønsker jeg å bidra med ytterligere kunnskap som kan hjelpe å forstå mer om samspillet mellom mekanismene, og hvordan mekanismene påvirker cybersikkerhetskulturen.

Dette har resultert i følgende problemstilling:

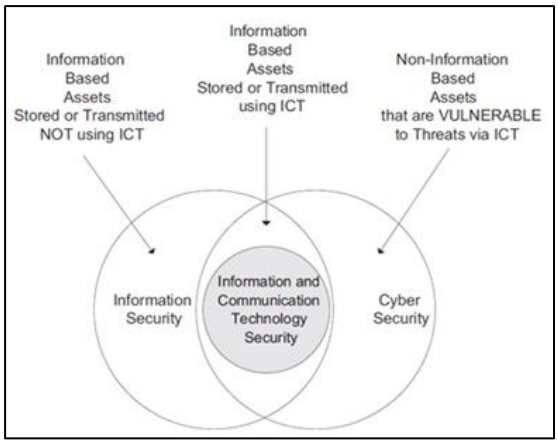
*«Hvordan påvirker interne organisatoriske mekanismer cybersikkerhetskulturen i virksomheter?»*

I det følgende kapittelet redegjøres det for den ulike begrepsbruken som benyttes når man snakker om sikkerhet i det digitale domenet – informasjonssikkerhet, IKT-sikkerhet og til slutt cybersikkerhet. Avslutningsvis presenterer jeg et utvalg av de mest vanlige cybertruslene norske virksomheter utsettes for.

# 2 Kontekst

## 2.1 Informasjons-, cyber-, og IKT-sikkerhet

Når man snakker om sikkerhet som relateres til det digitale domenet er informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet ofte begreper som brukes. I mange tilfeller, både i daglig tale og i litteraturen, brukes de om hverandre for å beskrive det samme, og begrepene er på mange måter overlappende på flere områder. Hovedforskjellen på de tre begrepene er hva som skal beskyttes under informasjons-, IKT-, og cybersikkerhetsbegrepet, illustrert i figur 1. Jeg vil videre gi en kort redegjørelse for hva disse begrepene innebærer.




*Figur 1. Forholdet mellom informasjonssikkerhet, IKT-sikkerhet, og cybersikkerhet (Von Solms & Van Niekerk, 2013)*

### 2.1.1 Informasjonssikkerhet

Informasjonssikkerhet omhandler de prosesser og rutiner en organisasjon har for beskyttelse av egen informasjon og tjenester. Informasjonen kan være både i digital og ikke-digital form. Hensikten med informasjonssikkerhet er å bevare konfidensialiteten, integriteten og tilgjengeligheten til informasjonen, de tre hoved karakteristikker begrepet består av. Disse tre karakteristikkene refereres ofte til som KIT, eller CIA på engelsk (confidentiality, integrity, og availability) (Nätt & Heide, 2021)

Konfidensialitet handler om at informasjon kun skal være tilgjengelig for det personell som har autorisert tilgang til informasjonen. Integritet skal sørge for at informasjonen til enhver tid er korrekt, uten mulighet for uvedkommende til å for eksempel endre på innholdet i informasjonen på veien mellom avsender og mottaker. Til slutt har tilgjengelighet som hensikt å sørge for at informasjonen til enhver tid er tilgjengelig for brukeren (Nätt & Heide, 2021)

Informasjonssikkerhet handler om å beskytte informasjon i tillegg til den underliggende teknologiske infrastrukturen (Von Solms & Van Niekerk, 2013). Mye av verdiene til en organisasjon kan være informasjonen i seg selv. Systemene, menneskene, eller prosedyrene som skal bidra til å beskytte informasjon og etterleve alle elementene i KIT-forkortelsen, kan være utsatt for trusler eller sårbarheter (Reegård et al., 2019). Systemene og prosessene som skal bidra til å beskytte informasjon blir sterkt påvirket av menneskelig adferd. Manglende opplæring, kunnskap eller ren uforsiktighet blant ansatte gjør dem derfor ofte til det svakeste leddet i denne kjeden (Van Niekerk & Von Solms, 2010). Informasjonssikkerhet må ikke ses på som et produkt, men som en prosess, og arbeidet med å beskytte informasjon må endre seg

i takt med utviklingen av teknologien, og kanskje da særlig med tanke på den menneskelige faktoren.

### 2.1.2 Cybersikkerhet

Med begrepet informasjonssikkerhet menes beskyttelse av informasjon. Som en forlengelse av dette innebærer cybersikkerhet ikke bare beskyttelse av informasjon, men også beskyttelse av både cyberdomenet, organisatoriske og menneskelige enheter. Med cyberdomenet menes «brukere, nettverk, enheter, programvare, prosesser, informasjon som lagres eller sendes, applikasjoner, tjenester, og systemer som kan kobles direkte eller indirekte til nettet» (ITU, 2008, s. 2, min oversettelse)

International Telecommunication Union (ITU) er Forente Nasjoners (FN) sin egen avdeling for informasjons- og kommunikasjonsteknologi. De har definert begrepet cybersikkerhet, og denne definisjonen legger også Von Solm og Van Niekerk (2013) til grunn i sin artikkel:

> *Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.*

(ITU, 2008, s. 2; Von Solms & Van Niekerk, 2013, s. 97)

Cybersikkerhet referer ikke bare til beskyttelse av informasjon, men også av de som operer i og de enhetene som kan nås gjennom cyberdomenet. For eksempel mennesker og maskinvare som er koblet til internett. Den menneskelige faktoren forstås også ulikt når man snakker om informasjonssikkerhet og cybersikkerhet. Innen informasjonssikkerhet handler den menneskelige faktoren om individets rolle i prosessen med å beskytte informasjon. Det samme gjelder når vi snakker om cybersikkerhet, men individet blir her sett på som et mulig mål eller som en deltakende eller tilretteleggende part i et cyberangrep (Cavelty, 2014)

Et annet skille er også at dersom noe truer cybersikkerheten kan dette direkte skade eller påvirke mennesker. Dette er ikke tilfelle dersom noe truer informasjonssikkerheten, da vil eventuelt skaden være indirekte (Von Solms & Van Niekerk, 2013). Et eksempel som Von

Solms og Van Niekerk (2013) bruker for å tydeliggjøre dette omhandler mobbing i cyberdomenet. Smarttelefoner og datamaskiner har gjort det lettere å mobbe, trakassere, true eller drive psykisk vold mot andre. Dette i seg selv fører ikke til at konfidensialiteten, integriteten eller tilgjengeligheten på informasjon er truet. I stedet er det individet som er offer for handlingen og påføres skade.

### 2.1.3 Informasjons og kommunikasjonsteknologi (IKT)-sikkerhet

I NOU 2018:14 (2018) – IKT-sikkerhet i alle ledd, blir det påpekt at det ikke finnes en entydig definisjon på begrepet, men at den tradisjonelle bruken av begrepet har handlet om beskyttelse av nettverk og systemer. I dag er betydningen av begrepet utvidet til i større grad å gjelde beskyttelse av informasjonen som systemene og nettverkene behandler, og de tjenestene som systemene leverer. I likhet med informasjonssikkerhet er også her målet å sikre konfidensialitet, integritet og tilgjengelighet av IKT-systemene, informasjonen som behandles i systemene og tjenestene som er tilknyttet systemene (NOU 2018:14, 2018)

### 2.1.4 Oppsummering

For å oppsummere de tre sikkerhetsområdene – informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet – så er det først og fremst flere likheter mellom dem og de overlapper i noen grad. Hver av disse tre områdene har også flere ulike definisjoner knyttet til seg, men i hovedsak handler det i stor grad om hva som skal beskyttes. Dette illustreres i figur 1. IKT-sikkerhet handler om å beskytte selve teknologien som brukes for å lagre eller sende informasjon. Det er gjennom å bevare KIT-elementene at man beskytter informasjon, sammen med den underliggende teknologien, men som oftest innenfor en organisatorisk kontekst. Cybersikkerhet på den andre siden strekker seg utover de organisatoriske grensene fordi informasjonsdeling er mulig på kryss og tvers av disse grensene. Det handler om beskyttelse av de som operer i cyberdomenet, være seg individer, organisasjoner eller til og med nasjoner (Mwim & Mtsweni, 2022; Von Solms & Van Niekerk, 2013)

## 2.2 Cybertrusler

Både informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet har til hensikt å beskytte mot ulike trusler. Noen av disse truslene kan være mennesker i seg selv, som er uaktsom eller som med intensjon har til hensikt å innhente data fra systemene, i form av digital spionasje, eller sabotere/forstyrre systemene. Men mange av truslene angriper direkte gjennom cyberdomenet. En av organisasjonene som jobber for å styrke cybersikkerheten i Europa er The European Union Agency for Cybersecurity (ENISA) og ble etablert i 2004, med nettopp

dette formålet (ENISA, 2021). Byrået har utgitt flere trusselvurderinger de siste årene med en oversikt over de vanligste truslene i cyberdomenet. ENISA kategoriserer trusselaktørene til å tilhøre en av de fire kategoriene – statlig sponsede aktører, cyberkriminelle aktører, hackere for leie (hack-for-hire), og til slutt hacktivister (hacking for å oppnå sosiale eller politiske mål (George & Leidner, 2019)) (ENISA, 2022). Sammen med rapportene fra ENISA og trusselvurderinger utgitt av NSM og NorSIS, vil jeg i neste avsnitt diskutere de mest vanlige truslene norske virksomheter kan utsettes for.

### 2.2.1 Løsepengevirus

Løsepengevirus ble av ENISA ansett som den største trusselen i året 2020-2021 og 2021-2022. Løsepengevirus innebærer at en virksomhets data krypteres helt eller delvis, med et påfølgende krav om å betale løsepenger for å få tilgang til dataen igjen (ENISA, 2021; ENISA, 2022). NorSIS (2021) peker på at løsepengevirus er den største trusselen mot virksomheter, uansett størrelse, i hele Europa. Bare i 2019 er det anslått at det ble betalt 10.1 milliarder euro i løsepenger. Viruset kan spres både gjennom vedlegg og lenker i e-poster, og når viruset først er lastet ned kan det få tilgang til og potensielt kryptere all data i hele virksomheten. Konsekvensene vil avhenge av virusets egenart og organisasjonens sikkerhetstiltak.

Samtlige av trusselvurderingene utgitt av NSM, Politiet og NorSIS etter 2020 peker på løsepengevirus som en av de store digitale truslene mot norske virksomheter. En av utfordringene med løsepengevirus er at det er vanskelig å straffeforfølge de som står bak slike angrep fordi det er vanskelig å spore angrepet tilbake til de skyldige. Samtidig gir slike virus mulighet for høy profitt ved at de som står bak ofte krever enorme summer for å låse opp systemene som er rammet (Politiet, 2022)

### 2.2.2 E-post relaterte trusler

Angripere vil ofte benytte seg av den enkleste metoden for å få tilgang til data fordi det er minst tid- og ressurskrevende. E-post relaterte trusler utnytter menneskelige svakheter gjennom sosial manipulasjon og spiller på frykt, tillit eller fristelse. Frykt ved å få deg til å handle raskt og trykke på lenker eller laste ned vedlegg som avsender ber deg om. Fristelse ved at man kan belønnes eller premieres ved å følge avsenders instruksjoner. Tillit ved at avsender utgir seg for å være noen andre, for eksempel en sjef eller en troverdig organisasjon (ENISA, 2021; NorSIS, 2021). En velkjent e-post relatert trussel er såkalt phising og var en av de vanligste angrepsmåtene mot norske virksomheter i 2022 (NSM, 2023). Dette

innebærer at angripere forsøker å fiske etter opplysninger som bankinformasjon, passord eller annen informasjon som kan utnyttes ved en senere anledning. Dette kan gjøres enten via e-post eller SMS. Trendene man ser er at angrep i større grad rettes mot mennesker og ikke IT-systemene. Dette understreker viktigheten av de ansattes kompetanse om ulike trusler og angripers modus operandi (ENISA, 2021; NorSIS, 2021).

### 2.2.3 Kontokapring

Dersom angripere får tilgang til innloggingsinformasjon som brukernavn og passord, kan de ta kontroll over brukerkontoer. En vanlig måte angripere får tilgang til kontoene på er å prøve å logge seg inn ved hjelp av passord og brukernavn som tidligere er lekket i andre databrudd, eller gjennom phising angrep. En annen måte er å prøve å logge seg inn på virksomheters IT-systemer ved å bruke kjente e-postadresser kombinert med de mest brukte eller vanligste passordene (NorSIS, 2021). På det mørke nettet omsettes lekkede brukernavn og passord i stor skala. I noen tilfeller omsettes de, men utnyttes ikke før flere år senere (NSM, 2022b).

### 2.2.4 Distributed Denial of Service angrep (DDOS)

Tjenestenektangrep, som også var en av de vanligste angrepsmåtene mot norske virksomheter i 2022 (NSM, 2023), innebærer å overbelaste en eller flere ressurser hos en tjeneste med så store mengder datatrafikk at den til slutt kneler. Slike angrep vil kun ramme tjenestens tilgjengelighet slik at brukere av tjenestene ikke får tilgang på informasjon (ENISA, 2022; NSM, 2023). Det finnes flere eksempler på slike angrep i Norge. Senest i juni 2022 opplevde flere norske nettsider slike angrep (NSM, 2022a). Formålet med slike angrep kan være alt fra påvirkningsoperasjoner, til sabotasje eller politisk aktivisme (NSM, 2022b).

### 2.2.5 Oppsummering

Cybertrusler kommer i mange forkledninger og de fire nevnte cybertruslene er bare fire av mange. Hensikten er ikke å liste opp alle mulige trusler, men gi eksempler på noen av metodene som brukes, og hva de potensielle konsekvensene kan bli. Listen med trusler er også levende i den forstand at den kan endre seg fra år til år. Jo sikrere virksomhetene blir, jo mer kreative må angriperne være for å bryte seg inn eller påvirke systemer. Nye angrepsmetoder vil derfor fortsette å utvikle seg i takt med hvor sikker systemene blir og hvor sikkerhetsbevisst menneskene blir.

# 3 Teori

## 3.1 Teoretisk rammeverk

I dette kapitlet vil jeg presentere det teoretiske rammeverket jeg vil støtte meg på i besvarelsen av problemstillingen «hvordan påvirker de interne organisatoriske mekanismene cybersikkerhetskulturen i en virksomhet?». Jeg trekker frem de viktigste elementene fra teorien og diskutere disse i de neste kapitlene. Jeg vil starte med å redegjøre for organisasjonskultur som begrep – hva som menes med organisasjonskultur, hvordan begrepet benyttes i en organisatorisk kontekst og hvordan sikkerhets- og cybersikkerhetskultur kan forstås som egne subkulturer av organisasjonskultur. Jeg vil også utdype hvilke interne organisatoriske mekanismer litteraturen vektlegger som de viktigste for hva en cybersikkerhetskultur inneholder

## 3.2 Organisasjonskultur

Begrepet organisasjonskultur ble etablert etter utgivelsen av bøkene «In search of excellence. Lessons from America's best-run companies» av Peters, T.J., & Waterman, R.H. (1982) og «Corporate Cultures. The rites and rituals of corporate life» utgitt av Deal, T.E., & Kennedy, A.A. (1982) (Einarsen et al., 2017). Forfatterne studerte hva som gjorde at noen organisasjoner lyktes, og andre ikke. Her ble organisasjonskultur pekt på som svaret på hvorfor noen lyktes, men andre ikke (Einarsen et al., 2017). En av de mest innflytelsesrike forskerne på området innen organisasjonskultur ansees å være Edgard H. Schein, som gjennom sin forskning identifiserte de elementene han mener organisasjonskultur består av. Litteraturen som i senere tid har forsøkt å konseptualisere cybersikkerhetskultur har også tatt utgangspunkt i Schein sitt arbeid (Chen et al., 2015; Reegård et al., 2019; Van Niekerk & Von Solms, 2010). De mest brukte måtene å beskrive en kulturs innhold på kjennetegnes av tre kjerneelement – verdier, normer og virkelighetsoppfatninger. Disse tre elementene vil beskrives nærmere i de kommende avsnittene.

Kultur er et komplekst fenomen som det er vanskelig å beskrive nøyaktig hva er, men det oppstår på flere nivåer – i familier, i organisasjoner og i nasjoner. Kultur oppstår når er gruppe i stor nok grad deler noe i fellesskap. For eksempel språk, erfaringer eller etnisitet (Schein, 2009). Schein argumenterer for at kultur er viktig å forstå fordi det kan spores tilbake til et sett med faktorer i underbevisstheten vår. Iboende tause krefter som vanskelig kan forklares av individene selv, men kraftfulle nok til at de styrer både individuell og kollektiv adferd, i tillegg til våre virkelighetsoppfatninger, tankemønster og verdier. På et individuelt

nivå vil adferd være et resultat av kultur. På et organisatorisk nivå vil kultur være avgjørende for strategi, mål og hvordan organisasjonene opptrer (Schein, 2009).

Det finnes flere ulike definisjoner på organisasjonskultur (se for eksempel (Pettigrew, 1979; Schein, 2009; Sun, 2008). Så og enes om én gjeldende definisjon er krevende. Det er allikevel mange fellestrekk i de ulike definisjonene som brukes i litteraturen. Blant annet at en organisasjonskultur består av noe som er felles delt internt i en gruppe. Det være seg verdier, normer eller virkelighetsoppfatninger. En definisjon som fremhever disse elementene, og som i tillegg inkluderer adferd som et resultat av normene, verdiene og virkelighetsoppfatningene, presenteres av Bang (2020) og Einarsen et al. (2017). Denne oppgaven legger deres definisjon av organisasjonskultur til grunn for det videre arbeidet. Definisjonen inkluderer de kjerneelementene som kjennetegner en organisasjonskultur, i tillegg til at den inkluderer adferd som er resultat av disse elementene.

Organisasjonskultur defineres her som:

> *De sett av felles verdier, normer og virkelighetsoppfatninger som utvikles i en organisasjon når medlemmene samhandler med hverandre og omgivelsene, og som kommer til uttrykk i medlemmenes handlinger og holdninger på jobben.*
> (Bang, 2020, s. 23; Einarsen et al., 2017, s. 406)

**Verdier** handler om hva som oppleves som viktig for organisasjonen. Dette kommer ofte til uttrykk gjennom organisasjoners uttrykte verdier. Noen eksempler på verdier kan være respekt, mot, åpenhet, ansvar o.l. (Bang, 2020; Einarsen et al., 2019). Verdier kan defineres som «en vedvarende tro på at en spesiell handlemåte eller slutt-tilstand personlig eller sosialt er å foretrekke fremfor en motsatt eller annerledes handlemåte eller slutt-tilstand» (Rokeach, 1976, s. 345, referert i Bang, 2020, s.50)»

Verdiene virker veiledende på organisasjonens medlemmer og hvordan de skal forholde seg. Både oppførsel, konfliktløsning og beslutningstaking kan ta utgangspunkt i verdiene. Om en av organisasjonens verdier for eksempel er åpenhet, kan man søke å etterleve dette ved å være transparent ovenfor kunder, samarbeidspartnere, samfunnet eller egne ansatte i arbeidsprosesser eller måten organisasjonens oppdrag løses på (Bang, 2020). Om de ansatte overbevises om at åpenhet er en viktig verdi fordi konsekvensene av å etterleve dem er positive, for eksempel ved at de belønnes i form av annerkjennelse for publisert forskningsdata, kan det ha en motiverende effekt og det vil til slutt bli verdier som deles blant

de ansatte og som de vil søke å etterleve (Bang, 2020; Schein, 2010). Til slutt kan de også påvirke de ansattes selvfølelse positivt når de opptrer i tråd med verdiene (Bang, 2020).

**Normer** er organisasjonens skrevne og uskrevne regler, hva som anses å være akseptable og uakseptable handlinger og holdninger. Dette skal sørge for at de ansattes handlinger ikke går på akkord med organisasjonens verdier (Bang, 2020; Einarsen et al, 2019). Normer dannes når medlemmene av organisasjonen samhandler over tid. Det vil da bli dannet et sett med felles delte forventninger hos medlemmene av hva som er vanlig og uvanlig handlemønster og hva som er akseptabelt og uakseptabelt oppførsel. Disse kan være implisitte eller eksplisitte – skrevne eller uskrevne regler (Bang, 2020; Einarsen et al, 2019). Normene kan også påvirkes gjennom diskusjon, hvor medlemmene i organisasjonen blir enige i fellesskap om hvilke regler som skal gjelde eller ved at de bringer med seg sine personlige normer inn i gruppen (Bang, 2020; Einarsen et al, 2019).

Man skiller også mellom normer etter hvordan de har innflytelse på adferden til individene: deskriptive og injunktive normer. (Cialdini & Trost, 1998; Deutsch & Gerard, 1955; gjengitt i Bang, 2020). De deskriptive normene beskriver hvordan individene oppfører seg gjennom informativ innflytelse. Det vil si at individene ser til andre individer i gruppen og hvordan de oppfører seg og kopier oppførselen. Denne formen for innflytelse er sterkest når man ikke er helt sikker på hva som er riktig oppførsel i en gitt situasjon. For eksempel om man er ny i organisasjonen og usikker på hva som er rett adferd (Bang, 2020)

Medlemmene i organisasjonen vil ha en formening om hvilken adferd som anses som akseptabel eller uakseptabel. Dette er injunktive normer og påvirker medlemmenes adferd gjennom normativ innflytelse. Dersom en spesiell adferd belønnes mens en annen straffes, vil medlemmene oppføre seg i tråd med normene forbundet med positive konsekvenser. Det er ofte en link mellom normer og verdier fordi verdiene vil være veiledende for hvordan man skal handle for å realisere dem (Bang, 2020). Dersom en organisasjon anser mot som en viktig verdi, vil normene som beskriver hvordan man skal etterleve dette, implisitt eller eksplisitt, komme til uttrykk gjennom handlinger fra de ansatte. For eksempel at de ansatte oppfordres til å ha mot til å rapportere på egne eller andre sine datasikkerhetsbrudd eller andre avvik.

Det er allikevel viktig å påpeke at normer og adferd ikke er det samme. Gjennom samhandling mellom medlemmene blir etter hvert normene formelle eller uformelle lover og

regler for adferd. Normer trenger heller ikke å være et sett med felles kjøreregler som gjelder for alle i organisasjonen. Det vil være slik at det varierer hvilke normer som gjelder for hvem internt i organisasjonen. Én gruppe kan ha ett sett med normer, og en annen gruppe et annet sett (Bang, 2020; Einarsen et al, 2019).

**Virkelighetsoppfatninger** er hvordan de ansatte opplever hva som skjer rundt dem og hvordan dette skal tolkes (Bang, 2020; Einarsen et al, 2019). Det handler om hvordan medlemmene i organisasjonen oppfatter virkeligheten rundt dem. Disse dannes gjennom daglig samhandling mellom medlemmene og ved å se til hvordan andre handler eller oppfører seg. Konsekvensene av handlingene eller oppførselen vil være med på å forme gruppens oppfatninger om virkeligheten. Hva som er sant og usant, hvordan man skal tolke det som skjer rundt dem og hvilke øyne man skal se verden med (Bang, 2020; Einarsen et al, 2019). Eksempler på en gruppes virkelighetsoppfatning kan være – «ledelsen tar ikke cybersikkerhet på alvor, så hvorfor skal de ansatte gjøre det?»

Virkelighetsoppfatninger kan misforstås eller feiltolkes og skape sinne eller frustrasjon, slik som eksemplet over, ved at det blitt en konstruert sannhet som ikke nødvendigvis stemmer med virkeligheten. Et annet eksempel er om man som nyansatt møter en leder som utrykker at «min dør er alltid åpen», et uttrykk som inviterer til en formell eller uformell prat når som helst. Lederen kan med dette kun ønske å utrykke høflighet og vennlighet. Om den nyansatte tar lederens filosofi bokstavelig, kan hun derimot oppleves som masete og trengende (Bang, 2020).

For å oppsummere så består en organisasjonskultur av kjerneelementene verdier, normer og virkelighetsoppfatninger, som er felles delte blant organisasjonens medlemmer og som kommer til uttrykk i deres holdninger og handlinger. Kulturer kan oppstå som en helhetlig del av organisasjonen, men også som én eller flere subkulturer i ulike avdelinger eller på ulike nivå i organisasjonen. Hva som kjennetegner en subkultur, og eksempler på dette vil diskuteres i neste avsnitt.

## 3.3 Subkultur

Kultur består av de verdier, normer og virkelighetsoppfatninger som er felles delt mellom organisasjonens medlemmer. Men det kan også oppstå ulike sett med delte verdier, normer og virkelighetsoppfatninger innenfor samme organisasjon – såkalte subkulturer (Einarsen et. al., 2019). En leders arbeid med å etablere en god organisasjonskultur kan vanskeliggjøres ved at

i takt med organisasjonens vekst og utvikling vokser det frem én eller flere subkulturer, som i noen tilfeller kan være like sterk eller sterkere enn organisasjonskulturen. Lederen må i så tilfelle være seg bevisst de ulike subkulturene som har vokst frem, og sørge for at de ikke er til hinder, men heller kan bidra til å nå organisasjonens mål (Schein, 2009).

En subkultur kan forstås som en delkultur i organisasjonen.

> *en subkultur er en undergruppe av organisasjonens medlemmer som samhandler jevnlig med hverandre, som identifiserer seg selv og blir opplevd av andre som en distinkt gruppe i organisasjonen, som deler et sett av utfordringer som de fleste i gruppen er enige om, og som rutinemessig handler på grunnlag av gruppens normer, verdier og virkelighetsoppfatninger.*
> (Bang, 2020, s. 28)

At medlemmene i en gruppe har hyppig og nær kontakt er en forutsetning for dannelsen av en subkultur. Organisering av arbeid, rapporteringsvei og fysisk plassering av de ansatte på arbeidsplassen er eksempler på faktorer som kan ha effekt på hvilken subkultur som utvikles på arbeidsplassen (Bang, 2020). Subkulturer dannes over tid og etter hvert som medlemmene deler felles erfaringer med hverandre vil også handlemønstrene og virkelighetsoppfatningene til medlemmene deles i fellesskap. Dette danner grunnlaget for subkulturen. Mange subkulturer utvikles også med bakgrunn i felles ansvarsoppgaver, funksjoner, geografi o.l., og ledere har en viktig rolle i å bygge og håndtere subkulturer (Bang, 2020)

Hva som påvirker subkulturene, og hvordan disse påvirker organisasjonen som helhet er spørsmål som er viktig å stille seg selv (Schein, 2009). For eksempel så kan en cybersikkerhetskultur forstås som en subkultur som kan utvikle seg på ulike nivå i organisasjonen og være enten svak eller sterk. En svak cybersikkerhetskultur kan påvirke organisasjonen og de produkter og tjenester de leverer. Dersom ansatte ikke forstår viktigheten av god cybersikkerhet kan de gjøre organisasjonen sårbar for digitale angrep på grunn av uforsiktig opptreden i cyberdomenet. Derfor er lederens forståelse av hvordan subkulturer kan påvirke organisasjonen, og hvordan håndtere disse, særdeles viktig.

Subkulturer kan som nevnt over, være delkulturer som for eksempel berører sikkerheten i organisasjonen – en sikkerhetskultur. Om arbeidet med en slik kultur forankres godt i organisasjonen vil det ikke bare bidra til at man fortsetter å levere sine tjenester og produkter,

men man gjøre det samtidig som man har fokus på sikkerhet. Hva som kjennetegner en slik kultur, og hvordan sikkerhetskultur har vokst frem som et begrep diskuteres i neste avsnitt.

## 3.4 Sikkerhetskultur

Når begrepet sikkerhetskultur benyttes refererer dette til den delen av organisasjonskulturen som berører sikkerheten i organisasjonen (Nätt & Heide, 2021). I dette ligger arbeid som skal forebygge hendelser eller redusere sannsynligheten og konsekvensen av dem. En velinformert arbeidsstyrke med gode holdninger og kompetanse kan fungere som en sterk barriere mot uønskede hendelser. Derfor er sikkerhetskulturbegrepet blitt mer utbredt – det anerkjennes at sikkerhetsarbeidet i organisasjonen ikke bare avhenger av prosedyrer, rutiner og teknologiske løsninger, men også av de ansattes holdninger, bevissthet, motivasjon og kunnskap for å oppnå et godt sikkerhetsnivå (Nätt & Heide, 2021)

Reason (1997) presenterer følgende definisjon på sikkerhetskultur:

> *The safety culture of an organization is the product of individual and group values, attitudes, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organizations 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 preventive measures*
> (Reason, 1997, s. 194).

Sikkerhetskultur er hva Reason referer til som en informert kultur, kjennetegnet av at den inneholder elementer som en rapporterende, rettferdig, fleksibel og lærende kultur. I en rapporterende kultur oppfordres ansatte til å benytte seg at de systemene organisasjonen har for å rapportere uønskede hendelser eller avvik oppover i systemet. For å oppnå dette avhenger det av at organisasjonen praktiserer en rettferdig kultur. De ansatte må kunne stole på at rapporteringer av uønskede hendelser eller avvik ikke resulterer i ukritisk bruk av straff som korrigerende virkemiddel. Samtidig må de være klar over hva som anses som akseptabel og uakseptabel adferd. En fleksibel kultur kjennetegnes av en evne til å endre organisasjonsstrukturen, ofte fra en hierarkisk til en flatere strukturmodell. Ved hendelser som truer virksomheten kan beslutningsmyndighet tildeles den med størst nærhet til hendelsen. Til slutt vil en lærende kultur bidra til at evnen og kompetansen til å lære av hendelsen og iverksette de riktige tiltakene styrker organisasjonen (Reason, 1997). Reason (1997) påpeker

også at en sikkerhetskultur ikke må anses som et produkt, men en prosess, og det er denne prosessen som er viktig. Kulturen påvirkes også av mange ulike faktorer. Disse vil diskuteres i de kommende avsnittene.

Om prosessen med sikkerhetskulturarbeidet forankres godt i organisasjonen, vil dette danne et godt grunnlag for å videre kunne bli en god cybersikkerhetskultur. Cybersikkerhetskultur kan på mange måter forstås som en forlengelse av sikkerhetskultur. Den delen av organisasjonskulturen som berører sikkerhet, men nærmere bestemt cybersikkerhet. Hva som kjennetegner en cybersikkerhetskultur, vil diskuteres i neste avsnitt.

## 3.5 Cybersikkerhetskultur

Ikke før starten av 2000-tallet begynte forskning å vise at sikkerhetskulturen i organisasjoner spiller en viktig rolle i å opprettholde høye sikkerhetsnivåer i informasjonssystemene som organisasjonene opererer (Reegård et al., 2019). Deretter vokste begrepene informasjonssikkerhets- og cybersikkerhetskultur frem. Som tidligere nevnt favner begrepet cybersikkerhet bredere enn informasjons- og IKT-sikkerhet. Som kulturbegrep – cybersikkerhetskultur – finnes det i likhet med de andre kulturbegrepene nevnt tidligere, flere definisjoner. Mange av definisjonene har flere likheter i den forstand at de inneholder elementene verdier, normer og virkelighetsoppfatninger som resulterer i menneskets adferd (Corradini, 2020; ENISA, 2018; Huang & Pearlson, 2019). En definisjon som dekker disse elementene, er:

> *Cybersecurity Culture (CSC) of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies. CSC is about making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions.*
> (ENISA, 2018, s.07)

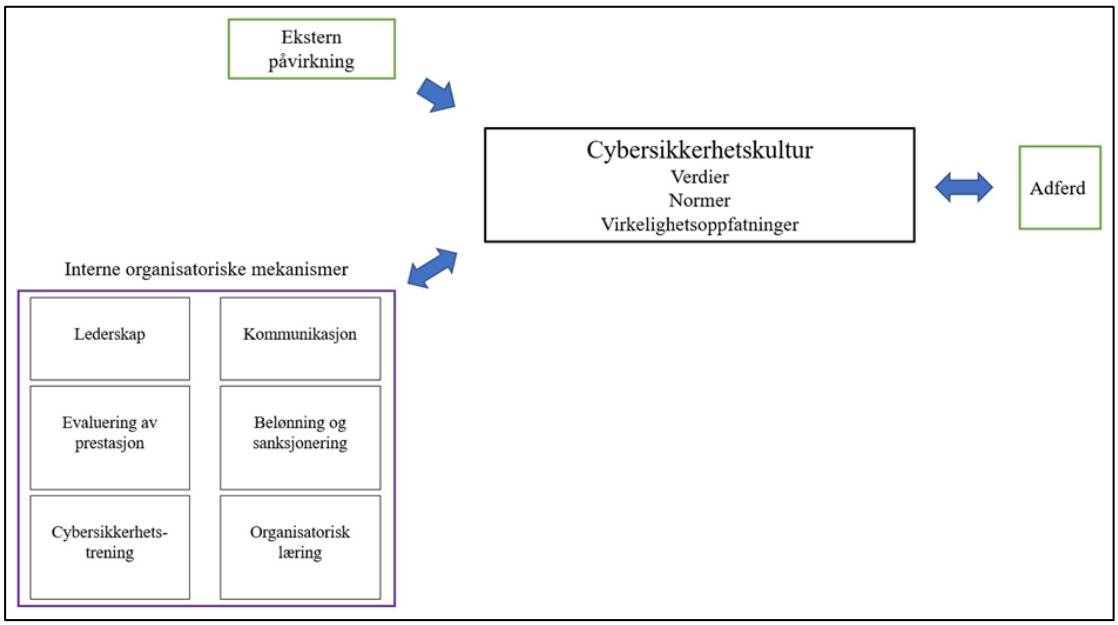
Målet med en cybersikkerhetskultur er å oppnå en adferd som bidrar til å beskytte informasjon, enhetene som kan nås gjennom cyberdomenet og menneskene som operer i og rundt cyberdomenet (Huang & Pearlson, 2019). En cybersikkerhetskultur kan sies å være måten man gjør ting på når man samhandler med cyberdomenet (Da Veiga, 2016). Dette vil gjenspeiles i den kunnskap, virkelighetsoppfatninger, holdninger, grunnleggende antakelser,

normer og verdier som resulterer i adferd som ikke bare beskytter informasjon, slik en informasjonssikkerhetskultur referer til, men også av de som operer i, og de enhetene som kan nås gjennom cyberdomenet. Når individer benytter seg av cyberdomenet kan de utsette seg selv eller organisasjonen de jobber for, for risikoer. En cybersikkerhetskultur er viktig slik at individene kan bruke cyberdomenet på måter som gjør at konfidensialitet, integritet og tilgjengelighet til informasjon og systemene ikke trues (Da Veiga, 2016).

## 3.6 Cybersikkerhetskulturens innhold

En organisasjons cybersikkerhetskultur kan påvirkes av eksterne og interne mekanismer. Huang & Pearlson (2019) presenterer i sin cybersikkerhetskultur modell (se figur 2) en illustrasjon av sammenhengen mellom de interne og eksterne mekanismene, og cybersikkerhetskultur, som til slutt resulterer i en bestemt adferd hos individet.

De eksterne mekanismene er utenfor organisasjonens kontroll og er i liten grad styrbare fra ledelsens side. Eksempler på slike mekanismer kan være den nasjonale cybersikkerhetskulturen, standarder og lovverk. I Norge vil for eksempel Sikkerhetsloven kunne gjelde for mange organisasjoner. Dette er lovverk som ledelsen ikke kan velge bort, men er lovpålagt å følge dersom man faller inn under lovens virkeområde. Andre eksempler er standarder som ISO 27000-serien, som inneholder krav og «best practice» for hvordan sikkerhetsarbeidet skal og kan utføres (Nätt & Heide, 2021).




*Figur 2. Cybersikkerhetskultur-modellen. Hentet fra Huang & Pearlson (2019)*

I figur 2 presenteres cybersikkerhetskultur-modellen og viser hvordan de eksterne og interne mekanismene påvirker virkelighetsoppfatninger, verdier og holdninger – det som samlet utgjør kulturen. Summen av dette resulterer de ansatte adferd.

Denne oppgaven vil fokusere på cybersikkerhetskultur fra et organisatorisk perspektiv. Dermed er de interne mekanismene av større interesse enn de eksterne. Blant annet fordi interne mekanismene er styrbare fra ledelsens side i mye større grad enn de eksterne. Dermed er det mer interessant å se på hvordan de styrbare mekanismene påvirker kulturen, fordi ledere har mulighet til å direkte påvirke de interne mekanismene og deres videre påvirkningskraft på cybersikkerhetskulturen. De eksterne mekanismene er styrbare i mindre grad. Dette betyr at virksomhetene selv kan gjøre lite for å påvirke dem direkte.

De eksterne mekanismene ville på den andre siden måtte blitt studert fra et samfunnsmessig perspektiv da man må inkludere den nasjonale cybersikkerhetskulturen og nasjonalt/internasjonalt lovverk, noe som ikke er denne oppgavens fokusområde. Forskning som tidligere er gjort på området har identifisert mange av de mekanismene som bidrar i å utvikle og måle cybersikkerhetskulturen (Alshaikh, 2020; Da Veiga, 2016; Huang & Pearlson, 2019; Reegård et al., 2019). Men *hvordan* interne organisatoriske mekanismer påvirker kulturen mangler mer forskning. Mitt bidrag er å belyse dette ytterligere. For å avgrense oppgaven vil jeg derfor videre kun fokusere på de interne mekanismene.

### 3.6.1 Organisatoriske mekanismer

### 3.6.2 Lederskap

Ledere er med på å skape organisasjonskultur, og en av deres viktigste oppgaver er å skape og administrere kulturen. Det er også det som gjør en leder til en god leder, deres evne å arbeide med kultur (Schein et al., 1987). Schein et al. (1987) sier videre «at en funksjon som er *unik* for "ledelse", i motsetning til "management" eller "administrasjon", er *skaping og styring av kultur*.» (Schein et al., 1987, s. 145-146). For at arbeidet med å bygge en cybersikkerhetskultur skal få fotfeste er ledelsens prioritering av dette arbeidet avgjørende. Tildeling av ressurser er et viktig signal om at cybersikkerhetskultur er et prioritert område. For eksempel kan det utnevnes en eller flere personer hvor arbeidsoppgaver er å jobbe med å kartlegge og forbedre kulturen. Ledelsens deltakelse i kulturbyggingen ved å være ansiktet utad når det gjelder å kommunisere dette arbeidet kan ha en positiv effekt på de ansatte (Huang & Pearlson, 2019). Ledelsens støtte er en av faktorene som har størst påvirkning på dette arbeidet. Aktiv deltakelse, ressurstildeling, oppfølging og ledelsens synlighet har vist å

være viktig i arbeidet med å formulere og implementere policyer. De ansattes adferd kan også ses i sammenheng med deres ønske om å møte kravene som stilles fra ledelsen. En aktiv ledelse kan dermed påvirke de ansatte adferd (Reegård et al., 2019).

### 3.6.3 Kommunikasjon

Måten cybersikkerhet kommuniseres på er et annet viktig tiltak for å øke bevisstheten blant ansatte om trender og trusler i cyberdomenet. Kurs, workshops, intranett, e-post er noen av mange måte slik informasjon kan kommuniseres på (Huang & Pearlson, 2019). Dersom de ansatte selv blir bevisstgjort eksisterende trusler, trender eller andre faresignaler kan de selv bli i stand til å identifisere farer og ta gode beslutninger på egenhånd. Dersom de ansatte også informeres om hvilket ansvar de har i forbindelse med cybersikkerhet ved å inneha de roller de har, kan dette bidra til at det utvikles en form for eierskapsfølelse til cybersikkerhetsarbeidet innen deres ansvarsområde. Dette åpner også for en dialog hvor man kan diskutere cybersikkerhetstematikk knyttet til sine ansvarsområder. Et godt kommunikasjonsarbeid kan også bidra til å redusere risikoer ved at de ansatte kan gjøre egne tiltak som enten bidrar til å redusere sannsynligheten for eller konsekvensene av uønskede hendelse. (Reegård et al., 2019). Det er også viktig at kommunikasjonsformen ikke er bare er ovenfra og ned, men også nedenfra og opp. Selv om cybersikkerhet må kommuniseres nedover i rekkene i organisasjonen, er det også viktig at de ansatte har mulighet til å rapportere på hendelser oppover i organisasjonen. Slik tilrettelegger man for en god rapporteringskultur (Reason, 1997).

### 3.6.4 Evaluering

De ansattes etterlevelse av sikkerhetspolicyen til organisasjonen kan evalueres på ulike måter. En av måtene kan være ved bruk av såkalte phising-øvelser. Lenker eller vedlegg som skal simulere et phising-angrep kan sendes ut til alle ansatte i organisasjonen. Deretter kan man kartlegge hvor mange som trykket på lenken eller åpnet vedlegget. Slike øvelser kan brukes for å kartlegge hvor styrkene og sårbarhetene befinner seg. Samtidig kan de brukes til å evaluere de ansattes adferd i møte med sikkerhetstruende hendelser (Huang & Pearlson, 2019). Organisasjonen må allikevel finne ut hva som skal evalueres og hvordan. Utdanningsinstitusjoner evalueres basert på hvilke karakterer studentene får. Dårlige resultater taler for eksempel for mer lekser eller flere prøver (Bang, 2020). På samme måte kan organisasjoner ved hjelp av ulike måter å evaluere på, slik som eksemplet med phising-øvelser, iverksette kompetansehevende tiltak som mer trening og øving.

### 3.6.5 Ris og ros

Hensikten med å ha systemer som belønner og straffer akseptabel eller uakseptabel adferd er å oppfordre til videre utførelse av korrekt adferd, eller korrigere uakseptabel adferd. Ulike måter å belønne på kan variere fra for eksempel annerkjennelse av enkeltpersoner eller avdelinger, til sertifiseringer eller arrangement av sosiale aktiviteter (Huang & Pearlson, 2019). Ved å knytte belønning eller straff til den atferden ledelsen er interessert i å oppnå blant sine ansatte, formidler de samtidig viktige verdier (Schein et al., 1987). Metoder for å straffe eller korrigere uakseptabel adferd på kan være å pålegge ansatte videre trening, skriftlige advarsler eller i verste fall oppsigelse av arbeidsforhold.

I tilfeller hvor straff benyttes som virkemiddel er det likevel viktig at straffen er proporsjonal med sikkerhetsbruddet som er gjort (Huang & Pearlson, 2019). Det er allikevel flere fallgruver ved bruk av ris og ros som prinsipp for atferdsendring. For eksempel kan ris være destruktivt eller demotiverende på ansatte dersom man åpenlyst kjefter på en ansatt. Ris ment for å korrigere atferd kan være ineffektivt da den som blir straffet vil prøve å unnslippe straff i stedet for å korrigere atferden som førte til straff. På samme måte kan man dersom man roser atferd som virker negativt på andre ansatte forsterke uønsket atferd (Einarsen et al., 2019) Ris og ros kan også ses i direkte sammenheng med normer. De «spillereglene» som medlemmene blir enige om at skal gjelde i egen organisasjon, vil ikke utvikle seg til etablerte normer dersom brudd på disse spillereglene ikke sanksjoneres (Einarsen et al., 2019).

### 3.6.6 Trening

Kunnskap og bevisstgjøring av de truslene som finnes i cyberdomenet er ansett å være et av de viktigste områdene å jobbe med for å oppnå en god cybersikkerhetskultur. De ansatte må forstå trusselbilde, men også hvordan disse truslene kan påvirke deres eget arbeid eller egen virksomhet (Reegård et al., 2019). «Man kan ikke anta at den gjennomsnittlige ansatte har den nødvendige kunnskapen til å utføre hans/hennes jobb på en sikker måte» (Van Niekerk & Von Solms, 2010, s. 478, min oversettelse). Trening må gjøres interessant, virke engasjerende, men også tilpasses de ulike rollene ansatte ved organisasjonen har, fordi det kan være ulikt behov for trening fra avdeling til avdeling. Treningen bør ikke være et engangstilfelle, men være en gjentakende prosess for å sikre at kunnskapen vedlikeholdes over tid (Reegård et al., 2019). Det er også en måte å utdanne de ansatte innen cybersikkerhet og kan gjøres som en del av «on-boarding» prosessen av nyansatte (Huang & Pearlson, 2019). Regelmessig trening gjør også de ansatte i stand til å vite hvordan man skal respondere på

hendelser (Nel & Drevin, 2019). For eksempel ved å koble datamaskinen fra nettverket eller å trekke ut kontakten om man mistenker at maskinen er infisert med virus.

### 3.6.7 Læring

For å definere læring kan man ta utgangspunkt i tre kriterier: (1) det skjer en endring, (2) endringen varer over tid, (3) læring oppstår gjennom praktisering eller andre former for erfaring. Endringen er enten en adferdsendring eller kapasiteten til å utføre en endring. Den må også vedvare over tid for å klassifiseres som endring. For eksempel vil ikke adferdsendringer som vedvarer noen få sekunder kunne klassifiseres som læring. Til slutt må læring oppstå gjennom erfaringer (Schunk, 2012). Eksempelvis ved at yngre eller uerfarne ansatte lærer om akseptabel og uakseptabel adferd i forbindelse med cybersikkerhet, gjennom samhandling med andre erfarne ansatte

Læring foregår både på individ- og organisasjonsnivå, men læringen som skjer på individnivå danner grunnlaget for at læring kan skje på organisatorisk nivå. Organisasjoner må derfor tilrettelegge for å integrere den individuelle læringen i den organisatoriske læringen (Wang & Ahmed, 2003). Dette kan for eksempel gjøres ved å ha fora hvor man kan utveksle kunnskap og erfaringer. Et annet viktig element med organisasjoner som evner å lære er at det kan gi et konkurransefortrinn ovenfor andre organisasjoner. (Wang & Ahmed, 2003). Relatert til cybersikkerhet kan dette bety at lærende organisasjoner står bedre rustet til å håndtere cybertruende hendelser, enn konkurrerende eller tilnærmet like organisasjoner som ikke lærer.

Som et resultat av disse seks mekanismene peker Huang & Pearlson (2019) på adferden som et resultat av cybersikkerhetskulturen, og kan deles inn i to typer adferd – «in-role» adferd og «extra-role» adferd. Førstnevnte referer til handlemåter som er i tråd med hva som kan forventes av rollen den ansatte har i organisasjonen. Etterlevelse av organisasjonens policy og å unngå brudd på denne er hva som kan forventes av enhver ansatt uavhengig av rollen de har i organisasjonen. Sistnevnte referer til de handlinger den ansatte foretar seg som ikke automatisk kan forventes av dem, eller som er en del av arbeidsoppgavene deres. Det å hjelpe andre til å øke deres bevissthet rundt spørsmål relatert til cybersikkerhet, og det å utrykke sin stemme for å kommentere eller spre sin kunnskap videre for å bedre cybersikkerhetsnivået er to typer extra-role adferd (Huang & Pearlson, 2019).

### 3.6.8 Oppsummering

De interne mekanismene vil alle kunne påvirke kunnskap, virkelighetsoppfatninger, normer og verdier til de ansatte i en organisasjon – det som utgjør cybersikkerhetskulturen. Som igjen vil resultere i de ansattes adferd. Men hvordan de ansatte – ledere, mellomledere og ansatte uten lederansvar – opplever at disse mekanismene påvirker kulturen og hvilke mekanismer som oppleves å ha størst påvirkningskraft, i positiv eller negativ forstand, og hvordan dette manifesteres i de ansattes adferd, vil det i denne oppgaven forskes nærmere på for å besvare problemstillingen «hvordan påvirker de interne organisatoriske mekanismene cybersikkerhetskulturen i en virksomhet?».

# 4 Metode

## 4.1 Forskningsstrategi

Studiens problemstilling og hensikt vil være avgjørende for valg av metode, og den kvalitative metoden egner seg når man ønsker å forstå eller beskrive fenomener eller konsepter (Berg & Lune, 2012). I denne studien er det cybersikkerhetskultur som er fenomenet jeg ønsker å se nærmere på, og forstå hvordan denne påvirkes. Med bakgrunn i studiens formål og problemstilling er det derfor valgt en kvalitativ metodetilnærming, hvor denne studien er det som omtales i litteraturen som en kvalitativ forskningsstudie (Merriam & Tisdell, 2016). Cybersikkerhetskultur som fenomen er et forskningsområde som er lite utbredt. For de fenomener vi ikke kjenner så godt, eller som vi ønsker å få en fyldigere forståelse av, er kvalitativ metode særlig hensiktsmessig (Johannessen et a., 2016). Det er også et overordnet mål i den kvalitative forskningen å få en dypere forståelse av de fenomener som er knyttet til personer og deres sosiale virkelighet (Dalen, 2011).

## 4.2 Datainnsamling

### 4.2.1 Intervju

Intervju er valgt som metode fordi det har vært som mål å få innblikk i informantenes egne erfaringer, tanker og følelser om temaet studien undersøker. Da er intervju spesielt godt egnet til dette formålet (Dalen, 2011). Innen organisatorisk forskning er intervju en de mest brukte metodene for datainnsamling (Cassell, 2009, i Buchanan & Bryman 2009). Det har i denne studien blitt gjennomført seks digitale én-til-én intervjuer med en gjennomsnittsvarighet på ca. 45 minutter som ble gjennomført over en periode på syv dager. Én-til-én intervjuer åpner også for fyldige og detaljerte beskrivelser av forståelse, holdninger, erfaringer og oppfattelse

(Johannessen et a., 2016). Intervjuformen har vært semistrukturert for å gi informantene anledning til å utrykke seg mer fritt enn hva andre metoder ville gjort, slik som for eksempel et spørreskjema. Båndopptaker er benyttet for å heve dataens reliabilitet, men også for å redusere faren for å mistolke informasjonen fra informantene dersom båndopptaker ikke hadde blitt benyttet.

Intervjuene som er gjennomført i denne studien følger en semistruktur som er planlagt på forhånd ved hjelp av en intervjuguide. Det har allikevel vært viktig å være fleksibel og tilrettelegge for et semistrukturert intervju underveis ettersom samtalen utvikler seg, noe som har gjort at rekkefølgen på spørsmålene kan variere. Dette gjør det mulig å kunne bevege seg frem og tilbake mellom spørsmål og fører til en bedre dynamikk i samtalene (Johannessen et a., 2016). Semistrukturert intervju tillater meg å bevege samtalene over på temaer som intervjuguiden ikke dekker. På denne måten kan man få innsikt i ny og relevant tematikk som gjør at informasjonsbehovet for studien utvides (Grønmo, 2004). I tillegg kan informanten «bruke sitt eget språk, sine egne begrepskategorier og sin virkelighetsdefinisjon» (Bang, 2020, s.193)

Før intervjuene har det blitt utarbeidet en intervjuguide (vedlegg 2) for å ha en «sjekkliste» å forholde seg til. Intervjuguiden inneholder en tematisk inndeling av de temaene det er ønskelig å innhente informasjon om. Dette er videre spesifisert ved bruk av flere spørsmål under hvert tema. Det gjorde det mulig å foreta en foreløpig sortering av informasjon under temaer eller kategorier (Grønmo, 2004). Det har vært et stort fokus på å lage den omfattende, men også spesifikk nok til at informantene kan svare på så mange relevante spørsmål knyttet til studiens problemstilling som mulig, i den hensikt å kunne si noe om det som er studiens formål. Det har på forhånd vært tenkt nøye gjennom hvilken informasjon man ønsker å få tilgang på med utgangspunkt i studiens problemstilling og teoretisk rammeverk (Grønmo, 2004).

Det er viktig å være seg bevisst de problemer som kan oppstå under datainnsamlingen. Intervjueren har også en stor oppgave i å «motta, forstå og videreformidle de budskapene som blir gitt» (Aase & Fossåskaret, 2014, s. 105). Derfor er også interaksjonen mellom intervjuer og respondent av stor betydning. Begge parter bringer med seg sine egne biaser, predisposisjoner og holdninger inn i intervjuet som kan påvirke hvilken informasjon man mottar, men det kan også ha betydning for hvordan intervjueren tolker dataen under og etter intervjuene (Merriam & Tisdell, 2016). Et eksempel på et problem som kan oppstå under

selve intervjuet er at informantenes manglende kunnskap eller vilje gjør at de ikke er i stand til, eller ønsker å svare på spørsmål (Grønmo, 2004). At informantene har problemer med å svare på kan også skyldes at spørsmålene fordrer at de må ta stilling til hendelser eller handlinger tilbake i tid, noe de ikke nødvendigvis husker (Grønmo, 2004). For å bøte på disse problemene har informantene fått tilsendt en grov intervjuguide på forhånd. Slik har de fått mulighet til å forberede seg og tenke gjennom spørsmålene før intervjuene startet (Grønmo, 2004). Intervjuformen er ikke problemfri, og det er flere faktorer som kan påvirke informantenes svar. En annen utfordring jeg har tatt høyde for, for ikke å påvirke svarene til informantene i noen som helst retning er å unngå ledende spørsmål. Intervjuet har derfor bestått av åpne spørsmål som i størst mulig grad tillater informanten å forklare fritt.

### 4.2.2 Utvalg

Problemstillingen vil være styrende for hvilke enheter som skal inngå i studien (Grønmo, 2004). Denne studiens problemstilling retter søkelyset mot organisasjoner, hvor enkeltpersoner er rekruttert som representanter for den samme valgte organisasjon. Valgte organisasjon tilhører samfunnsområdet forskning og utvikling og er valgt med bakgrunn i NSM sin trusselvurdering fra 2022. Det er kun én organisasjon som inngår i studien. Dette begrunnes med at for jeg skal kunne uttale meg om interne organisatoriske mekanismers påvirkning på cybersikkerhetskultur, så ønsket jeg å ta for meg kulturen i én organisasjon og unngå å blande kulturer fra flere ulike organisasjoner.

Personer er rekruttert basert på om de kan gi meg nødvendig data, det vil si deres innblikk, egne erfaringer, tanker og følelser om temaet studien undersøker. Hensiktsmessighet har vært viktigere enn representativitet i utvalget (Johannessen et a., 2016). Med hensiktsmessighet menes det at det for eksempel ville vært lite hensiktsmessig å rekruttere en informant som ikke tilhører samfunnsområdet forskning og utvikling, gitt studiens formål. Men på en annen side har det også vært et mål å intervjue så mange som mulig for å ha et godt nok datagrunnlag til å kunne si noe om det studien undersøker.

Siden studien retter søkelys mot samfunnsområdet forskning og utvikling er organisasjonen i denne studien valgt med bakgrunn i om den faller inn under dette samfunnsområdet. Informantene er rekruttert deretter (Johannessen et a., 2016). Utvalgets størrelse i denne studien er seks personer. Det er ingen fasit på hvor stort et utvalg skal være, men om utvalget er lite er det desto mer viktig at utvelgingsprosessen er hensiktsmessig nok til å kunne belyse problemstillingen (Thagaard, 2018). Utvalgets størrelse kunne til fordel vært større, men det

er desto mer viktigere å skaffe et relevant utvalg, enn det er å skaffe et stort utvalg (Johannessen et a., 2016).

Sammensetning av informantene vises i tabell 1. Tre av informantene har lederansvar i sin organisasjon i form av å være seksjonsleder for sin seksjon. To av informantene er ansatte uten lederansvar og den siste informanten er organisasjonens sikkerhetssjef. Informantene er blitt tildelt en egen kode som det refereres til senere i studien. Organisasjonen informantene representerer er også anonymisert. Dette er en vurdering som er gjort på bakgrunn av informasjonen informantene har bidratt med til studien. Gjennom intervjuene framkommer det av informasjonen hvordan organisasjonen arbeider med cybersikkerhet. For eksempel intern trening, opplæring og kommunikasjon knyttet til cybersikkerhet. Det har fra min side ikke vært ønskelig å identifisere organisasjonen og påpeke det som kan tolkes som eventuelle styrker og svakheter med cybersikkerhetsarbeidet, og muliggjøre at denne informasjonen kan spores tilbake til en navngitt organisasjon.

| Organisasjon | Informant | Kode |
|---|---|---|
| **Organisasjon innen samfunnsområdet forskning og utvikling** | Ansatt | I1 |
| | Seksjonsleder | I2 |
| | Seksjonsleder | I3 |
| | Seksjonsleder | I4 |
| | Sikkerhetssjef | I5 |
| | Ansatt | I6 |

*Tabell 1. Informantoversikt*

## 4.3 Samtykke og anonymitet

Samtlige informanter har før intervjuene startet gitt sitt informerte samtykke. Det vil si at de har fått nødvendige opplysninger om studien på forhånd (vedlegg 1). Blant annet hvordan informasjonen de bidrar med til studien behandles, hvem som er behandlingsansvarlig, og deres mulighet til å trekke samtykket når som helst. Det er ikke samlet inn personopplysninger om informantene da dette ikke er nødvendig for studien. Informantene er allikevel anonymisert for at informasjonen de har bidratt med til studien ikke skal kunne spores tilbake til dem (Johannessen et a., 2016).

## 4.4 Dataanalyse

Det innledende steget i dataanalysen etter intervjuene var transkribert, var å høre og lese gjennom intervjuene parallelt. Ved å gjøre dette, samtidig som jeg tok notater fortløpende, kunne jeg notere ned ideer og tanker om hvordan datamaterialet skulle kategoriseres (Maxwell, 2013). Det videre arbeidet med analysen var å bryte ned og forenkle datamaterialet. Dette ble gjort ved hjelp av programvaren NVivo. Programvarer for håndtering av kvalitative data er blitt veldig vanlig å bruke innen forskning (Maxwell, 2013). Bruken av NVivo har gjort det mulig for meg å få til en effektiv håndtering av rådata fra intervjuene ved at de enkelt kan organiseres og kodes etter mitt eget ønske. Slik er det også blitt brukt, som et tidsbesparende verktøy for å systematisere datamaterialet.

I analysen har jeg benyttet meg av det som betegnes som en qualitative content analysis (QCA) (Schreier, 2012). QCA er brukt for å tolke innholdet og få frem meningen i datamaterialet. Ved å benytte meg av QCA har jeg redusert datamaterialet og fokusert på utvalgte deler som jeg mener er relevant for å besvare studiens problemstilling (Schreier, 2012). I denne studien er det benyttet en hybrid av induktiv og deduktiv tilnærming til QCA. Hovedkategoriene er opprettet med bakgrunn i det teoretiske rammeverket til Huang og Pearlsson (2019) sine seks interne organisatoriske mekanismer (ledelse, kommunikasjon, evaluering, osv.) og datamaterialet er kodet til disse kategoriene. I tillegg er det også opprettet kategorier som ikke har utspring fra det teoretiske rammeverker, men fra selve datamaterialet. For eksempel ble det sett etter likheter og mønster i informantenes besvarelser av hvordan de selv forstår begrepet cybersikkerhetskultur. Her var *holdninger*, *bevissthet* og *forståelse* begreper som gjentok seg blant flere informanter. Dette var informasjon som ble kodet under kategorien *informantenes forståelse av begrepet cybersikkerhetskultur*.

«Kvalitative data ikke taler for seg selv. De må tolkes.» (Johannessen et a., 2016, s.161). Å tolke data betyr at det må ses i en større sammenheng, å se mening i noe som ikke spesifikt og tydelig uttrykkes. Dette kan gjøres ved å knytte funnene opp mot relevant teori og tidligere forskning for området det forskes på for å forstå og forklare funnene (Johannessen et a., 2016). Et eksempel på dette gis i følgende avsnitt.

Hvordan interne organisatoriske mekanismer påvirker cybersikkerhetskultur i en virksomhet må besvares ved å tolke helheten i det informantene sier. For eksempel er det informantenes oppfatning at cybersikkerhet ikke står øverst på ledelsens prioriteringsliste. Dette trenger ikke være en etablert sannhet, men dette er informantenes virkelighetsoppfatning, deres egen

etablerte sannhet. Dersom ledelsen på øverste nivå i organisasjonen hadde blitt intervjuet kunne man fått et annet svar – at ledelsen prioriterer cybersikkerhet i høyeste grad. Dersom man ser dette i sammenheng med ledelsens synlige involvering når det gjelder cybersikkerhet, eller mangel på kommunikasjon, kan ansatte få inntrykket av at cybersikkerhet ikke prioriteres, fordi ledelsen ikke er synlig involvert eller ikke kommuniser viktigheten av det. Dette kan da tolkes i den retning av at ledelsens involvering i cybersikkerhetstematikk og deres evne til å kommunisere denne tematikken til organisasjonen, kan påvirke de ansattes virkelighetsoppfatning – et element kulturbegrepet består av, hentet fra det teoretiske rammeverket.

Hvordan data presenteres er også en del av analyseprosessen. Noe av hensikten med å presentere data er å fremstille den på en organisert og sammenfattet måte slik at det er mulig å trekke analytiske konklusjoner. En måte å presentere datafunn på er for eksempel gjennom sitater fra intervjuene eller ved bruk av modeller (Berg & Lune, 2012). Jeg har basert på resultatene fra studien utarbeidet en modell for å visualisere funnene, hvor figur 3 (s. 42) er en visualisering av disse resultatene. Den gir leseren en enkel presentasjon av funnene og tillater oss å trekke analytiske slutninger (Berg & Lune, 2012, s. 56).

## 4.5 Metodiske vurderinger

### 4.5.1 Reliabilitet

Forskningsdataens pålitelighet refereres til som reliabilitet. Med dette menes nøyaktigheten knyttet til undersøkelsens data, måten den samles inn på og hvordan den bearbeides. Dersom denne studien gjennomføres på eksakt samme måte på et senere tidspunkt og oppnår samme resultat, kan man anse reliabiliteten som høy (Johannessen et al., 2016).

Målet med studien har være å få en dypere forståelse og mer kunnskap om cybersikkerhetskultur som fenomen, ikke å ende opp med en statistisk generalisering. Studien har med dette hatt et klart mål. Rekruttering av informanter må derfor ses i sammenheng med ønske om å oppnå dette målet. Informantene i studien er relevante og gode kilder for å kunne gi informasjon om cybersikkerhetskulturen i organisasjonen, og hvordan de organisatoriske mekanismene kan påvirke denne. Men for å kunne si noe om cybersikkerhetskultur i organisasjonen er det viktig å ikke bare intervjue informanter fra ett sted i organisasjonen. For å få helheten av ulike syn på kulturen i organisasjonen, og hvordan de organisatoriske mekanismene påvirker cybersikkerhetskulturen, er det viktig å samle data fra alle sjiktene i

organisasjonen (Bang, 2020). Denne studien mangler informanter som representerer ledelsen fra øverste hold i organisasjonen. Ledere på et høyere nivå i organisasjonen kunne gitt ytterligere verdifull innsikt i de forhold studien ønsker å si noe om. Studien har allikevel informanter som representerer mellomledernivå og ned, med en lik fordeling av ansatte med lederansvar og ansatte uten.

På en annen side er det svakheter knyttet til det å gjennomføre semistrukturerte intervju, slikt som er tilfelle for denne studien. Intervjuer med åpne svaralternativer og med ulik tilnærming til spørsmålene fra gang til gang, gjør at intervjuene ikke er direkte sammenlignbare. Det kan derfor være variasjon fra intervju til intervju (Bang, 2020). Et annet viktig element når man studerer samfunnsmessige eller sosiale fenomener er at disse er i stadig endring, derfor er det ikke alltid mulighet til å gjennomføre samme type studie igjen og forvente å få eksakt samme resultat (Grønmo, 2004).

I motsetning til kvantitative studier hvor studiens reliabilitet er enklere å teste og beregne ved hjelp av standardiserte metoder, er ikke dette like lett i kvalitative studier. I kvantitative studier kan man anta at for eksempel et spørreskjema eller observasjonsskjema vil fungere på samme måte, uavhengig av hvem det brukes av (Grønmo, 2004). I kvalitative studier vil reliabilitet i større grad avhenge av meg som forsker. Som nevnt tidligere tillater et semistrukturert intervju at man kan utforske temaer som intervjuguiden ikke dekker. Hva jeg ønsker å utforske videre, eller hva jeg ønsker informantene skal utdype mer om, baseres på min subjektive mening om hva som er formålstjenlig å vite mer om. Derfor kan det bli nærmest umulig å gjennomføre uavhengige datainnsamlinger basert på samme undersøkelsesopplegg og få samme resultat (Grønmo, 2004). I tillegg vil det kunne, dersom samme undersøkelsesopplegg gjennomføres i en annen organisasjon, gi et helt annet datagrunnlag.

### 4.5.2 Validitet

Hvor gyldig datamaterialet er for å besvare studiens problemstilling refereres til som validitet. Dersom datainnsamlingen resulterer i data som er relevant for å besvare problemstillingen, kan man si at validiteten er høy. Studien kan også tilskrives høy validitet dersom undersøkelsesopplegget er velegnet til å samle inn data relevant for problemstillingen (Grønmo, 2004).

Det er flere utfordringer knyttet til å undersøke kultur i en organisasjon, som igjen kan påvirke validiteten i stor grad. For det første kan informantene med viten og vilje ha til hensikt å villede intervjueren ved å gi uriktig informasjon. Dette kan være grunnet i et ønske om ikke å sette egen organisasjon i et dårlig lys, eller fordi informanten ikke stoler på min lovnad om anonymitet (Bang, 2020). Informanten kan også oppgi uriktig informasjon fordi han eller hun selv ikke sitter på riktig informasjon selv. Dermed villedes jeg uten at dette er informantens hensikt. Til slutt kan det være utfordrende for en informant å oppgi informasjon om kultur dersom informanten faktisk ikke har kunnskap om de forhold som trengs for å si noe om kulturen. Dette har vært en annen utfordring jeg måtte ta stilling til – informantene bør være kulturisert (Bang, 2020). Det vil si at de burde kjenne kulturen så godt at de faktisk har mulighet til å si noe om den. Derfor bør informantene ha vært i organisasjonen i minimum ett år og de bør være en del av kulturen i dag (Bang, 2020). For en av informantene er ikke dette tilfellet, da vedkommende sluttet i organisasjonen like før intervjuet fant sted. Det ble allikevel vurdert til at informanten fortsatt hadde kjennskap til egen organisasjon og intervjuet ble derfor gjennomført. De resterende informantene har over ett års fartstid i organisasjonen og regnes derfor som godt nok kulturisert til at de kjenner organisasjonen godt.

Studiens datamateriale er kun basert på intervjuer gjennomført med informanter. En videre styrking av studiens validitet kunne vært gjort dersom organisasjonens egne interne dokumenter også hadde vært analysert. Ved å studere arkivmateriale kan man finne ut hvordan

> *hvordan organisasjonen ønsker og velger å fremstå overfor medarbeidere, kunder og øvrige interessenter. Det er altså organisasjonens forfektede verdier som kommer frem i dette materialet […] I tillegg kan det være interessant å se hvor stort sprik det er mellom organisasjonens presentasjon av seg selv og den interne oppfatning medlemmene har av organisasjonen*
> (Bang, 2020, s. 201)

Under studien hadde jeg ikke tilgang på organisasjonens egne dokumenter som for eksempel IKT-sikkerhetsinstruks eller andre relevante dokumenter. Tilgang på disse kunne ha styrket studiens validitet ytterligere. Det kunne gitt muligheter til å sammenligne organisasjonens presentasjon av seg selv, med informantenes oppfatning av organisasjonen – deres virkelighetsoppfatning, samt fått innblikk i organisasjonens forfektede verdier.

Et spørsmål man også må stille seg er hvorvidt innholdet i denne studiens undersøkelse er dekkende for det studien har til hensikt å finne ut – det man kan kalle innholdsvaliditet (Grennes, 2013). Det må for eksempel gjøres et utvalg av mange mulige spørsmål som potensielt skal inngå i intervjuguiden. Om de utvalgte spørsmålene ikke er dekkende for å finne ut det studien har til hensikt å si noe om, kan dette gå på bekostning av studiens validitet. Om samme studie gjennomføres av andre forskere, men med en annen innfallsvinkel til utforming av intervjuspørsmålene kan resultatene fra datainnsamlingen peke i andre retninger enn i denne studien. Dette går på bekostning av den eksterne validiteten – hvorvidt resultatene kan sies å være gjeldene hos andre organisasjoner enn den som inngår i denne studien (Grennes, 2013).

# 5 Empiri

Strukturen på empirien er ledet av studiens problemstilling – hvordan påvirker interne organisatoriske mekanismer en virksomhets cybersikkerhetskultur – og følger til del samme oppbygning som det teoretiske rammeverket – Først presenteres informantenes egen forståelse av begrepet cybersikkerhetskultur. Deretter presenteres funnene knyttet til de interne organisatoriske mekanismene: ledelse, kommunikasjon, evaluering, ris og ros, trening og opplæring, og læring.

## 5.1 Forståelsen av cybersikkerhetskultur

Det er en noe lik forståelse av begrepet cybersikkerhetskultur blant informantene. Flere av informantene vektlegger holdninger i sin forståelse (I1, I2, I6). Dersom man for eksempel velger å bruke innloggingspassord «123» på organisasjonens interne systemer, vitner dette om en holdning hvor enkle løsninger er å foretrekke fremfor sikre løsninger. Gode personlige holdninger blir derfor ansett som viktige for å kunne ivareta cybersikkerheten i organisasjonen. Gode holdninger er en av måtene man kan bidra til at uvedkommende ikke får tilgang til organisasjonens systemer (I6). For flere av informantene handler det altså om å ha en bevisst holdning til at informasjon om organisasjonen kan være av interesse for andre og gjøre egne tiltak for å verne om de digitale interessene (I1, I2).

Forståelse og bevissthet er andre begreper informantene også trekker frem i sin tolkning av cybersikkerhetskultur (I3, I4, I6). Det å være seg bevisst sitt ansvar som enkeltperson og hvor viktig hvert enkelt individ er i arbeidet med cybersikkerhet. En av informantene referer til en pågående kampanje fra Sivil Klareringsmyndighet – «en dråpe er nok» – som omhandler

nettopp dette (I3). Kampanjen understreker at hvert enkelt individ er en viktig brikke for å beskytte informasjon og grunnleggende verdier. Videre sier I3 at mye av fokuset i egen organisasjon handler mye om dette, å få hver enkelt ansatt til å være seg bevisst sitt ansvar, fordi litt uforsiktighet eller uforstand kan være nok til å slippe inntrengere inn i systemene.

Forståelse innebærer også den «generelle forståelsen i instituttet for hvordan vi tar vare på sikkerheten i all vår digitale omgang og kommunikasjon» (I4). Samtidig som man har en generell forståelse for trusselen og trusselaktørene, slik at man evner å reagere om man blir utsatt for eksempel for phising-angrep. I5 peker på det samme – forståelsen og kunnskapen man har for å vite hva trusselen er og når man eventuelt blir utsatt for noe, men det handler også om tilliten man har til hverandre sånn at man på den måten tør å rapportere hendelser uten å frykte sanksjoner. Med den riktige forståelsen og de riktige holdningene kan man opererer på arbeidsgivers materiell på en trygg og sikker måte (I6)

I en forlengelse av informantenes egen forståelse av begrepet cybersikkerhetskultur, reflekterte de også over hvordan denne oppleves i egen organisasjon. En informant sier at kulturen kan oppleves som naiv, men understreker at dette kan ha med å gjøre at som forskningsinstitusjon så er man opptatt av åpenhet (I1). Forskning og data som produseres ønsker man å formidle til resten av verden. På den ene siden skal alt være åpent, men på den andre siden skal man også tenke sikkerhet å verne om informasjon (I2).

En annen informant peker på at kulturen nok kan variere (I4). Dette kan ha sammenheng med sammensetningen av personell i organisasjonen. Ledelsen i organisasjonen har brukt tid og krefter på å rette fokus mot cybersikkerhet, men organisasjonen har også et høyt antall Ph.d.-, og noen masterstudenter, kanskje så mye som fra rundt 30 forskjellige nasjoner (I3), som har kortere opphold i organisasjonen. Dette betyr et noe gjennomtrekk av personer. Det kan derfor variere i hvor stor grad disse blir brakt i sikkerhetskulturen (I4), og hvor enkelt det er for de å bli en del av kulturen om oppholdene er av kortere karakter. Det oppleves allikevel at det er et fokus på cybersikkerhet. Spesielt etter at organisasjonen fikk en egen sikkerhetsmedarbeider har cybersikkerhetstematikk i større grad blitt kommunisert til de ansatte (I6). Hvordan de organisatoriske mekanismene spiller inn på cybersikkerhetsarbeidet, og på hvilken måte det kan påvirke cybersikkerhetskulturen vil diskuteres i de neste avsnittene.

## 5.2 De organisatoriske mekanismene

### 5.2.1 Ledelse

Informantene opplever ikke at ledelsens prioritering av cybersikkerhet står øverst på agendaen. Men tematikken ble sporadisk tatt opp, spesielt om det var hendelser i nyhetsbildet som gjorde at det ble et ekstra fokus på det (I1-I5). I slike tilfeller ble allmøter brukt som en arena hvor ledelsen ofte hadde cybersikkerhet som et eget tema (I1). Det er allikevel et inntrykk av at cybersikkerhet prioriteres i ord, men «de fine ordene og festtalene blir ikke helt ført opp i praktisk budsjettarbeid» (I5). Dette er også inntrykket til I6 – «budsjettet er ikke skrudd inn til den store satsingen» (I6). Fordeling av forskningsmidler tar gjerne en større del av budsjettet enn cybersikkerhet (I1), noe som ikke er direkte overraskende, gitt det faktum at forskning er et av organisasjonens hovedområder. Men organisasjonen har i løpet av de senere år fått en egen sikkerhetssjef. Dette i seg selv er et tegn på at det er fokus på et helhetlig og systematisk sikkerhetsarbeid, og at det best kan oppnås ved å nedfelle dette arbeidet i en egen stilling. Men hvorvidt cybersikkerhet løftes frem på agendaen er opp til denne fagressursen (I1).

Som en av informantene påpeker så starter all kultur med ledelsen (I2). Ledelsen har en viktig rolle i form av at de sender et viktig signal til resten av organisasjonen dersom de involverer seg i cybersikkerhetstematikk. «Folk lytter til ledelsen, enten de liker dem eller ikke» (I3). Sikkerhet, og herunder cybersikkerhet, er et av de første punktene som diskuteres på allmøter i organisasjonen. Enten det handler om ulykker eller nestenulykker ute på de ulike lokasjonene organisasjonen opererer fra, eller cyberrelaterte hendelser. Dette viser både alvoret i hva organisasjonen kan utsettes for, men troverdigheten i budskapet øker også når det kommer fra ledelsen – «det er sterkt når det kommer fra direktøren selv. Så det kan ikke bli sterkere da, når han sier det skal være sånn» (I3). Hyppigheten i budskapet og hvor konsekvent det er har også effekt på de ansatte, i den grad at det bidrar til økt årvåkenhet og signaliserer ovenfor de ansatte at det også er et fokusområde fra ledelsen sin side. Ledelsen har også en viktig rolle i form av å være eksemplets makt og være kravstillere. Dersom ledelsen tar snarveier, viser lite engasjement eller neglisjerer cybersikkerhetstrusler kan dette smitte over på resten av de ansatte. Derfor er det helt vesentlig at ledelsen involverer i å bygge kultur (I2, I5).

Der er allikevel en konsensus blant informantene at ansvaret for cybersikkerheten ikke ligger ene og alene hos ledelsen. Selv om det formelle hovedansvaret ligger hos ledelsen, så ligger

mye av ansvaret hos den enkelte (I1). Kravene må komme fra toppledelsen, men som en av informantene sier «så er det jeg som har ansvar for at jeg ikke har passord '123'» (I2). Dette bildet deler også I4 – Det formelle ansvaret ligger hos toppledelsen, men så drypper det videre ned på seksjonsledere, avdelingsledere og den enkelte ansatte. Ansvaret for å tilrettelegge cybersikkerhetsarbeidet med for eksempel ressurser, ligger hos ledelsen. Så ligger det et ansvar hos de ansatte følge de krav og retningslinjer som følger fra øverste nivå.

### 5.2.2 Kommunikasjon

Cybersikkerhetstematikk kommuniseres i hovedsak på tre måter, via e-post eller gjennom organisasjonens egen intranettside, men det løftes også frem på fellesmøter. Budskapet i det som kommuniseres blir ofte sett i sammenheng med det gjeldende trusselbildet og de åpne trusselvurderingene fra blant annet E-tjenesten, NSM og PST. Men det kan også være konkrete hendelser som gjerne har vært belyst i media som gjør at det blir satt et ekstra fokus på det. For eksempel er løsepengevirus et tema som har blitt kommunisert til de ansatte ved flere anledninger. Noe av budskapet er også det som omtales som «trivielt» (I4), for eksempel det å huske å låse PC og døra til kontoret når man forlater arbeidsplassen, eller ikke trykke på mistenkelige lenker i e-poster. Ansatte i organisasjonen har noe reisevirksomhet i forbindelse med jobb, både til inn- og utland. Organisasjonen har retningslinjer angående cybersikkerhet i forbindelse med reising og disse retningslinjene blir ofte kommunisert til de ansatte. For eksempel understrekes det at private telefoner og PC ikke bør tas med på reise til f.eks. Kina, men at man bruker PC og telefon som er utlevert fra arbeidsgiver og som er ment for reiseformål.

Flere av informantene peker på at kommunikasjonen angående cybersikkerhet til fordel kunne vært mer skreddersydd til den enkeltes seksjon eller avdeling sitt arbeidsområde (I1, I2, I5, I6). Hvordan organisasjonen til fordel kunne kommunisert cybersikkerhet for å øke bevissthet og kunnskap blant de ansatte sier en av informantene

> *å putte det i en bedre ramme og setting. I stedet for å ta enkeltepisoder, nyansere det med eksempler og hvorfor man er sårbare […] Hvorfor er vår institusjon i det hele tatt interessant, og aktualisere det med trusselbilde. Om det så er statlige aktører eller kriminelle. Synliggjøre forskjellige innfallsvinkler en aktør kan bruke for å få innpass i våre datasystemer.* (I1).

Flere informanter peker på det samme, å tilpasse budskapet i større grad slik at de ansatte skjønner hvorfor deres data eller institusjon i det hele tatt er av interesse. Det å «prøve å kommunisere hvorfor mine data kan være av interesse» (I2) virker å være noe som kan gjøre at de ansatte får økt bevisstheten rundt viktigheten av å beskytte dataen. Samtidig så kan det, dersom verdien av dataen tydeliggjøres, føre til en økt eierskapsfølelse og en større forståelse av viktigheten av den og hvordan den kan utnyttes i en større sammenheng. Informanten eksemplifiserer videre med at «i fjor så telte vi 917 fjellrever, 10 000 reinsdyr, og isbreen har krympet […] Så det går på å kommunisere at det er ikke bare det lille snevre som du holder på med som er av interesse, men porten inn i så mye annen informasjon» (I2). Denne type data kan for den enkelte forsker, isolert sett, virke ubetydelig og uinteressant for en fremmed makt eller for kriminelle. Men det kan være informasjon som kan utnyttes ved senere anledninger.

En annen ting som påpekes er at dataintegritet er viktig for en forskningsinstitusjon. Det å beskytte dataene mot uautorisert endring er et viktig fokusområde. Mye av datagrunnlaget som produseres i organisasjonen er ment å virke som faglige råd til norske myndigheter. At dataene er troverdige, er derfor særdeles viktig. For eksempel er det en fare for at noen er ute etter å manipulere verdiene eller analyseresultater i forskningsdata til fordel for seg selv (I6). At forskningsdata tidligere har vært manipulert av forskere selv for karrierevinning, eller av ondsinnede aktører finnes det eksempler på i forskningsverdenen (I4). Cybersikkerhet må kommuniseres i slike sammenhenger, å understreke hvorfor cybersikkerhet er viktig og hvordan ditt arbeid kan være av interesse for andre. Dette peker også en av informantene på – informasjonen som kommuniseres må føles relevant for den jobben man er satt til å gjøre (I5)

Det å kommunisere cybersikkerhetstematikk er et viktig element som bidrar til å øke forståelse og kunnskap blant de ansatte. Man oppnår økt bevissthet rundt de trusler som finnes i cyberdomenet, som igjen fører til at de ansatte tar tryggere valg eller stiller spørsmålstegn ved mistenkeligheter. Samtidig er det viktig å sørge for at informasjonen er relevant og rettidig. En annen utfordring er å ikke overdrive mengden eller hyppigheten av informasjonen. Dette kan virke utmattende og de ansatte kan «bli trøtt» (I3) eller «gå lei» (I4). Det å finne den rette balansen kan resultere i at cybersikkerhet til slutt blir en integrert del av måten man tenker og forholder seg til cybersikkerhet på (I6).

### 5.2.3 Evaluering

Informantene oppgir at organisasjonen ikke har en egen måte å evaluere de ansattes etterlevelse eller brudd på policyer eller instrukser. Derfor blir temaet evaluering kun et hypotetisk spørsmål om hvordan den tenkte effekten av dette kan være. Informantene blir presentert et eksempel på måter å evaluere ved bruk av phising-øvelser. En slik øvelse kan foregå månedlig hvor sikkerhetssjef eller IT-avdelingen sender ut en tilsynelatende harmløs e-post til de ansatte med en lenke de blir bedt om å trykke på. Ved å se hvor mange som rapporterer e-posten som mistenkelig, eller hvor mange som trykker på lenken, kan man få tall på hvor mange som hadde blitt lurt, dersom e-posten hadde vært reell.

Det er ulike meninger blant informantene om hvorvidt slike måter å evaluere de ansatte handlemåter eller kompetanse på hadde vært hensiktsmessig. Det kan være et effektivt verktøy for sikkerhetssjefen for å se hvor det svakeste leddet i kjeden ligger, for så å bruke det man lærer av en slik evaluering til å kunne repetere tidligere leksjoner eller kurs (I3, I4). Det kan også være en øyeåpner for de ansatte om resultatene fra en slik evaluering presenteres. Det kan føre til at de ansatte justerer egen adferd, dersom de vet at organisasjonen har verktøy for å kunne evaluere de ansatte. (I5). Men det pekes på at en slik evaluering ikke må ha til hensikt å henge ut de som ikke «består» en slik test, men heller bruke det som en måte å illustrere hvor enkelt det kan være å bli lurt.

Det virker allikevel til at å evaluere de ansatte kan ha en stor bakside. Noen av informantene mener det er viktig å vokte seg for at det ikke blir en form for «big brother»-mentalitet i organisasjonen (I1). Dersom de ansatte føler de blir overvåket, eller at de utsettes for en slags skjult kamera operasjon, vil dette kunne svekke tilliten man har til ledelsen og egen organisasjon, og man blir unødvendig mistenksom på annen informasjon som kommer fra egen organisasjon (I2). En av informantene sier videre at en fare er at det utvikles en fryktkultur i organisasjonen. De ansatte kan få følelsen av å bli overvåket og uthengt dersom man gjør feil (I5).

Som en av informantene påpeker så er det allikevel viktig å tenke på at dersom evalueringen gjøres på riktig måte, så er hensikten god. Ved å kartlegge hvor i organisasjonen man er mest sårbar, kan man iverksette tiltak for å bøte med dette. For konsekvensene kan bli store dersom man slipper uvedkommende inn i systemene sine. «Den ene tabben som en kan gjøre kan jo ødelegge tiår med arbeid, millioner eller statlig sett milliarder med investeringer på

datasikkerhet, […] vi risikerer jo økonomisk tap, omdømmetap, og vi kan kanskje gjøre skade utenfor vår organisasjon» (I3).

Informanten bruker videre metaforen for det å ha sertifikatet til bil. Dersom man ikke er i stand til å håndtere en bil, kan man miste sertifikatet. En evaluering kan i verste fall fungere på samme måte. Dersom man gjentatte ganger utviser hensynsløs adferd når det gjelder cybersikkerhet, kan en konsekvens være å ta fra eller begrense vedkommende sin tilgang på informasjon eller systemer (I3)

### 5.2.4 Ris og ros

Ifølge informantene har ikke organisasjonen et formelt etablert system som belønner etterlevelse på interne rutiner eller policyer. Men organisasjonen har systemer for å sanksjonere brudd på rutiner eller policyer, men det vil, avhengig av brudd, være opp til ledelsesgruppen og direktører og sanksjonere, men dette vurderes i hvert enkelt tilfelle (I1). Men om man «ved grov uforstand har forvoldt katastrofe, så skal du jo teoretisk kunne straffes» (I3). En av informantene utdyper videre at det ikke er et system for å belønne, men det er et system for å sanksjonere det som kalles informasjonssikkerhetsbrudd, dersom det er gjentakende eller med vilje. I slike tilfeller sanksjoneres det enten ved advarsel, eller i verste fall med oppsigelse av arbeidsforhold. Men behovet for et belønningssystem har ikke vært åpenlyst (I5).

Siden organisasjonen ikke har et formelt etablert system for å belønne eller sanksjonere blir informantene spurt om hvordan de stiller seg til å ha hatt et slikt system i organisasjonen. En visshet blant de ansatte om at etterlevelse av sikkerhetsrutiner og policyer, eller fravær av sikkerhetsbrudd, belønnes eller sanksjonering ved brudd på rutiner eller policyer. Det er ulike meninger hvordan dette kan oppleves i organisasjonen. Dersom det allerede er en del av organisasjonskulturen, for eksempel at ulike avdelinger «konkurrerer» mot hverandre for å oppnå gode resultater i form av å forhindre sikkerhetsbrudd, så kan belønningssystemer være gode ordninger, uten at det gis eksempler, for å motivere de ansatte og oppnå en varig endring i adferd (I2, I5).

Andre tror at etablerte systemer for belønning og sanksjonering kan ha effekt på de ansattes holdninger til cybersikkerhet. Den ene informanten (I3) trekker frem at organisasjonen har mange forskere og doktorgradsstudenter, mange som er inne i en periode av livet hvor de investerer mye tid i arbeidet sitt. Et tydelig sanksjonssystem som for eksempel resulterer i tap

av tilganger til systemer eller informasjon ved brudd på sikkerhetsrutiner, kan gjøre at doktorgradsstudenter risikerer at doktorgradsstudiet blir satt på vent, eller i verste fall ikke blir fullført (I3). Derfor kan slike systemer ha en holdningsskapende effekt ved at man blir mer bevisst rundt de gjeldende sikkerhetsrutiner og policyer, og forsøker å etterleve disse.

På en annen side påpekes det at systemer for belønning og sanksjonering kan virke «masete» og at det som informanten omtaler som «barnepike-holdning» fra ledelsen, og at slik informanten kjenner sine kolleger så vil de reagere negativt på slike systemer og det vil oppleves som kontraproduktivt. Informasjon og lederopplæring mener informanten vil ha sterkere effekt (I4). I tillegg sier en annen informant at slike systemer kan bidra til at det utvikles en fryktkultur. Man risikerer å bli paranoid og «redd for å trykke på ting» på datamaskinene i frykt for at feil handling skal påvirke belønninger og man kan sanksjoneres (I6). Informanten utdyper videre at man ønsker at de ansatte skal rapportere sikkerhetstruende hendelser, men at belønnings- og sanksjoneringssystemer kan være et hinder fordi ansatte kan frykte at det går utover potensielle belønninger, eller at man risikerer å bli sanksjonert.

### 5.2.5 Trening og opplæring

Samtlige informanter oppgir at de ansatte har ikke et trenings- eller opplæringsprogram satt i system for å øke bevisstheten rundt de trender og trusler som finnes i cyberdomenet. Ikke noe annet enn den generelle informasjonen som kommer angående cybersikkerhet (I4). De dryppene som kommer med informasjon i opplæringsøyemed, virker å være litt tilfeldig (I1) og foregår ikke på faste intervall. To av informantene trekker frem NSMs årlige sikkerhetsmåned i oktober, hvor direktoratet sender ut informasjon på e-post for å øke kunnskap og bevissthet om digital sikkerhet, som det eneste som kan karakteriseres som opplæringsmateriell (I2, I4).

Organisasjonen har også en egen intranettside hvor de ansatte må lese gjennom de gjeldende instrukser og policyer. Etiske retningslinjer, gaver i nære relasjoner, arbeidsforhold, lønn, ferie og utvikling er eksempler på hva instruksene og policyene inneholder, hvorav cybersikkerhet også er et tema. Men det ingen måte å kontrollere at de ansatte har lest gjennom og forstått innholdet i dette. Det er heller ingen måte for de ansatte å signere at de har lest gjennom innholdet i disse instruksene og policyene. «Så det er ikke et godt system» (I3). Men sikkerhetssjefen sier at de jobber aktivt med å nå ut til de ansatte med ny og rettidig informasjon. For eksempel ble nasjonal sikkerhetsmåned i oktober benyttet til å leie inn eksterne aktører for å holde foredrag. Senere samme uke var fokuset rettet mot

organisasjonens interne dokumenter, både IKT-, og reisepolicy. Dette ble gjort for å høyne bevisstheten blant de ansatte. Videre blir det kommunisert til de ansatte, både med bakgrunn i eksterne trusselvurderinger, men også trender man ser på bakgrunn av informasjon som kommer fra Computer Emergency Responce Team (CERT) – miljøet på nasjonalt nivå, hva som er trendene å være oppmerksomme på.

Siden organisasjonen ikke har organiserte trenings- eller opplæringsprogram blir informantene spurt om hvordan de skulle ønske slike program var, dersom de hadde hatt det, eller i fremtiden starter med det. Trening og opplæring med faste intervall, årlig eller halvårlig blir trukket frem som en løsning som kan bidra til å holde kunnskapsnivået oppe (I2). Flere informanter mener også at slike trenings- og opplæringsprogram burde ha et spisset innehold mot deres egen organisasjon. Hvorfor er organisasjonen vår interessant, hva kan vi bli utsatt for og hvordan forholder vi oss dersom noe skjer (I2, I3, I6), dette er spørsmål som bør adresseres i utformingen av trening- og opplæringsmoduler. En informant foreslår at demoer kan være en interessant innfallsvinkel til slike treningssammenhenger. Ved å fysisk demonstrere hvor enkelt det kan være å ta seg inn i systemene og eksemplifisere skaden man kan gjøre, eller informasjonen man kan få tilgang på, kan være en tankevekker for mange og øke bevisstheten blant de ansatte. Samtidig fjerner man naiviteten om at «dette skjer ikke oss» fordi man kan fysisk vise til hvor enkelt det er.

De fleste informantene er veldig positive til regelmessig trening og opplæring innen cybersikkerhet. Dette bidrar til å holde et stabilt høyt kunnskapsnivå samtidig som man også blir mer bevisst de ulike måter man kan rammes på, av hvem, og hvorfor. Men en av informantene mener det også er viktig at dersom trening og opplæring gjennomføres så må det føles relevant. Trening og opplæring må ha en hensikt for at det skal oppleves relevant og ikke bli «masete» på de ansatte (I4)

### 5.2.6 Læring

Det tydeligste tegnet på endringer som har skjedd i organisasjonen relatert til arbeidet med cybersikkerhet, er ansettelsen av en sikkerhetsansvarlig. En av informantene sier at etter organisasjonen fikk en egen sikkerhetsansvarlig, for ca. 4-5 år siden, har det skjedd en merkbar forandring knyttet til sikkerhetsarbeidet, som for eksempel ordentlige retningslinjer og verktøy for IKT-sikkerhet, CIM som et risikostyringsverktøy, samt fått etablert rutiner i ledergruppa (I4). Hyppigheten av oppdateringer og informasjon knyttet til cybersikkerhet som ansatte mottar på e-post har også økt etter organisasjonen fikk en sikkerhetsansvarlig (I2).

Men mange av endringen som har skjedd i organisasjonen har skjedd på et overordnet systemnivå og ikke brukernivå (I5). Det er uklart om det med dette menes et overordnet teknisk systemnivå, eller et organisatorisk systemnivå.

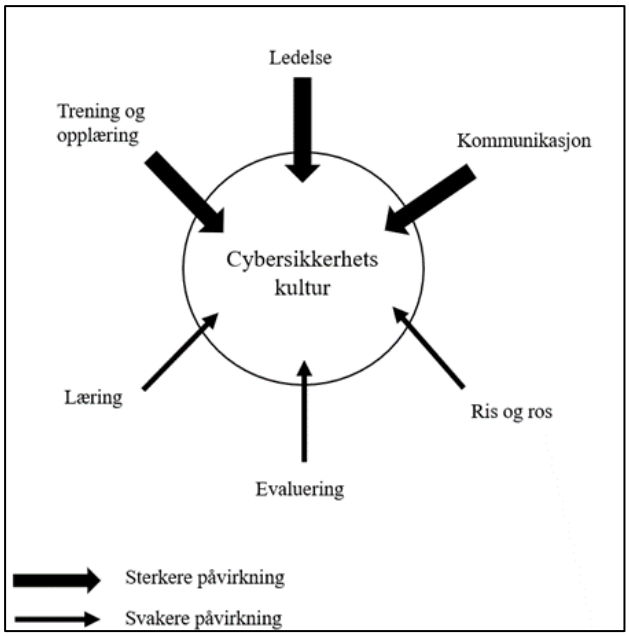
Organisasjonen har egne samlinger eller fora for erfaringsutveksling og kunnskapsdeling, men disse skjer på ledelsesnivå. Ledergruppemøter trekkes frem som et slags fora hvor blant annet cybersikkerhetstematikk diskuteres, dersom det for eksempel har vært hendelser som gjør det naturlig å diskutere (I3). IT-seksjonen i organisasjonen har også egne samlinger eller møter med andre aktører hvor cybersikkerhet diskuteres (I6). Men disse samlingene eller foraene er enten forbehold ledergruppen eller IT-avdelingen.

Noen av informantene mener at regelmessige samlinger eller fora for å diskutere cybersikkerhet, for alle ansatte, kunne vært hensiktsmessig. Muligheten til å bli oppdatert på trusselbilde eller diskutere gjeldende prosedyrer – hva funker og hva funker ikke, kan være positivt for de ansatte (I1). Det kan være en god arena for å lære de ansatte om cybersikkerhet og hva det egentlig er. For mange er cyber noe man ikke ser eller vet hva er, «cybersikkerhet det er ullent» (I2). Det å kunne ha en plass å diskutere kan igjen bidra til å øke bevisstheten rundt tematikken og lære av hverandre eller andre.

### 5.2.7 Hvilke mekanismer påvirker kulturen i størst grad

Til slutt ble informantene bedt om å rangere de tre mekanismene de tror kan ha størst påvirkning på kulturen. Resultatene er visualisert i figur 3 og vil bli utdypet videre. (1) Trening og opplæring, (2) ledelse og (3) kommunikasjon er de tre mekanismene informantene trekker frem som de som kan ha størst påvirkning på cybersikkerhetskulturen.

Funnene viser at ledelsen staker ut retningen for organisasjonen og har makt til å prioritere cybersikkerhetsarbeidet. Samtidig går ledelsen foran som et eksempel og setter standarden for resten av organisasjonen. Dersom ledelsen ikke virker å verken prioritere eller er opptatt av cybersikkerhet, kan dette smitte over på resten av de ansatte i organisasjonen.




*Figur 3. Utarbeidet av empiri og viser oversikt over mekanismenes påvirkning på cybersikkerhetskultur*

Kommunikasjon er viktig for å øke bevisstheten blant de ansatte rundt cybersikkerhet. At de ansatte holdes oppdatert på de trender og trusler i cyberdomenet kan bidra til økt årvåkenhet. Samtidig får man en bredere forståelse av hvorfor ens egen virksomhet og arbeid kan være av interesse for andre, og de potensielle konsekvensene som kan ramme. Det er også viktig at de krav som stilles til de ansatte med bakgrunn i interne rutiner og prosedyrer formidles til de ansatte. Dette kan påvirke hvilken adferd de ansatte utviser i cyberdomenet.

Trening og opplæring kan, dersom det gjøres systematisk og regelmessig, bidra til å øke kunnskapsnivået blant de ansatte. Det er allikevel viktig at treningen oppleves som relevant og er tilpasset den enkelte. Kurs, samlinger eller fysiske demonstrasjoner vil bidra til å opprettholde et godt kunnskapsnivå. Det signaliseres også ovenfor de ansatte at cybersikkerhet er et område som det er viktig for organisasjonen at de ansatte har kunnskap om. Trening og opplæring kan også være avgjørende for å forebygge uønskede digitale hendelser, men også hvordan de håndteres om man blir utsatt for et angrep.

### 5.2.8 Andre faktorer

Informantene nevner også andre mekanismer, som ikke er en del av de seks mekanismene det jobbes utfra i denne studien, som også kan påvirke cybersikkerhetskulturen. S*creening* trekkes frem som et interessant element. En screeningprosess innebærer en grundigere gjennomgang av kandidater før en evt. ansettelse. I1 viser til at screening kan ses i sammenheng med ansettelser til lederstillinger. Ledelse vil være viktig, for ved «fravær av

ledelse da blomstrer ukulturen» (I1). Derfor kan en akademiker «som kun har levd i universitetsverdenen hele sitt liv som skal utøve ledelse, kanskje være annerledes enn en ikke-akademiker som utøver ledelse, så det er kanskje viktig ting for å bygge de rette kulturene.» (I1). Screeningprosesser handler ikke bare om å tilsette egnede ledere til lederstillinger, men også ha riktige ansatte i riktige stillinger.

Et annet punkt som trekkes frem er innføring av det som kan oppleves som unødvendige sikkerhetstiltak. Tiltak må være proporsjonale med risikoen. Om tiltakene ikke gjenspeiler risikoen kan organisasjonen bruke overdrevent med ressurser. Det kan også gå på bekostning av cybersikkerhetskulturen i den forstand at verdier, normer og virkelighetsoppfatninger formes basert på en overdreven bruk av sikkerhetstiltak. Om tiltakene som iverksettes er til hinder for det dagligdagse arbeidet til de ansatte, vil de jobbe rundt tiltakene for å få jobben gjort (I6).

# 6 Diskusjon

## 6.1 Forståelsen av begrepet cybersikkerhetskultur

Schein (2009) argumenterer for at kultur er viktig å forstå fordi den styrer både vår kollektive og individuelle atferd. Det vil også være avgjørende for en organisasjons opptreden, strategi og mål. Det er derfor viktig at både ansatte og ledere er seg bevisst hva man legger i begrepet kultur. Om en organisasjon føler det er behov for en kulturendring må man vite hva man skal endre på. Informantenes forståelse av cybersikkerhetskultur er på flere områder sammenfallende med hvordan ENISA (2018) definerer det, hvor holdninger, bevissthet og kunnskap også inngår som en del av informantenes forståelse. At det er en relativt lik forståelse av hva som inngår i begrepet er et godt utgangspunkt for å arbeide med å bygge en cybersikkerhetskultur.

Resultatene fra studien viser at det er en felles oppfatning blant informantene om hvem som har ansvaret for cybersikkerhetsarbeidet i virksomheten – hver enkelt ansatt. Alle, fra toppen av hierarkiet til bunnen av det har et ansvar for å utføre arbeidet sitt i tråd med de retningslinjer som organisasjonen har lagt til grunn. Denne felles oppfatningen er et godt tegn og tyder på at man har beveget seg bort i fra tankegangen som preget det Von Solms (2000) beskrev som den «tekniske bølgen» fra 80 til midten av 90-tallet, hvor dette var ansett å være IT-avdelingene sitt ansvar. At den enkelte ansatte er seg bevisst sitt ansvar i

cybersikkerhetsarbeidet kan man ikke understreke viktigheten av nok ganger. For slik man leser trendene i det digitale trusselbilde er angrepene i større grad rettet mot mennesker og ikke selve IT-systemene. Det er nærliggende å tro at dette kan ses i sammenheng med Nobles (2018) sin tallfestede prosentandel på hvor ofte mennesker er skyld i at cyberangrep lykkes – mennesker gjør feil. Det gjør dem også til lette mål.

## 6.2 Mekanismenes effekt på cybersikkerhetskultur

### 6.2.1 Ledelse

Ledelsens involvering i cybersikkerhetsarbeidet kan påvirke hvordan de ansatte selv opplever viktigheten av å ha et strengt rettet fokus mot det. Selv om ledelsens prioritering og satsning på cybersikkerhet kan oppfattes å være lav hos ansatte, trenger ikke dette være virkeligheten. Tildeling av for eksempel økonomiske ressurser for å styrke arbeidet med cybersikkerhet gjennom kurs, øvelser etc., er en måte å signalisere satsning mot dette området. Men i en organisasjon hvor hovedområdet er forskning og utvikling kan det lett tenkes til at fordeling av forskningsmidler tar en større del av budsjettet enn cybersikkerhet. De ansattes virkelighetsoppfatning om at cybersikkerhet ikke prioriteres av ledelsen, kan være basert på en misforståelse eller feiltolkning (Bang, 2020, s.56). Det kan for eksempel tenkes til at ledelsen har cybersikkerhet som et høyt prioritert satsningsområdet, men at de ikke har økonomiske ressurser til å signalisere det i aktive tiltak. Ansettelsen av en egen sikkerhetssjef, og arbeidet vedkommende har lagt ned, er allikevel lagt merke til blant informantene (I1, I2, I3, I4, I6) og organisasjonen har med det signalisert at sikkerheten skal ivaretas av en egen fagressurs.

Signaleffekten ved en aktiv og involvert ledelse er sterk. Ansatte lytter til ledelsen og budskapet oppleves som ekstra sterk når det kommer fra øverste hold (I3). Derfor kan en engasjert aktiv ledelse bidra til økt årvåkenhet blant ansatte. I tillegg er de det man kan kalle en norm-setter. De ansatte vil ofte se til ledelsen etter det som Einarsen et al. (2019) og Bang (2020) refererer til som akseptable og uakseptable handlinger. Nettopp fordi ledelsen på mange måter vil være eksempler til etterfølge. Etter hvert som de ansatte i organisasjonen samhandler over tid dannes det et bilde over hva som er akseptabelt og uakseptabelt å gjøre (Einarsen et al., 2019). Normene dannes gjennom en informativ innflytelse hvor man kopierer adferden til ledelsen. Som Reegård et al. (2019) viser til er også ledelsen kravstillere.
På bakgrunn av de krav som stilles fra ledelsen vil man kunne bli nødt til å justere egen atferd for å imøtekomme disse kravene. Eksempler på krav kan være om at ansatte skal gjennomføre

årlige treningsmoduler tilknyttet cybersikkerhet, eller at krav som stilles gjennom prosedyrer, for eksempel handlemåter ved mottak av e-post fra ukjent avsender.

Som resultatene viser vil det kunne oppstå utfordringer med å bygge kultur om man ikke skiller på ledelse og styring (I2). Med styring menes at hovedfokuset til ledelsen kun er å styre organisasjonen etter de strategier, mål og rammer som er satt for driften. Ledelse på den andre siden handler også om å styre organisasjonen i riktig retning, men ved å lede de ansatte på et mellom-menneskelig plan. Samhandling med de ansatte, involvere seg i deres arbeid og bygge en god kultur samtidig som man styrer organisasjonen i riktig retning. Dette kan ses i sammenheng med det Schein (1987) viser til som unikt for *ledelse*, kontra *management*. Ledelse innebærer skaping og styring av kultur. Derfor kan en god screeningsprosess være et godt utgangspunkt for å sørge for at man faktisk får en *leder* i en lederstilling.

### 6.2.2 Kommunikasjon

Reason (1997) fremhever at en positiv sikkerhetskultur blant annet karakteriseres av kommunikasjon og delte oppfatninger om viktigheten av sikkerhet. For å opprettholde bevisstheten til de ansatte er det viktig med hyppig, rettidig og relevant informasjon. Hvordan cybersikkerhet kommuniserer kan derfor være et kompetansehevende tiltak. For som Van Niekerk & Von Solms (2010) påpeker er manglende kunnskap en av grunnene til at ansatte ofte utgjør det svakeste leddet i cybersikkerhetsarbeidet.

Resultatene fra studien viser at cybersikkerhetstematikk absolutt kommuniseres ut til de ansatte, gjennom flere kanaler. Sikkerhetssjefen er også opptatt av at informasjonen som kommuniserer er relevant for den jobben de ulike ansatte er satt til å gjøre. Som det tidligere i denne studien er vist til er kontokapring en vanlig angrepsmåte. Dersom ansatte for eksempel bruker e-post adressen til sin jobbmail-konto i privat sammenheng, for eksempel om man skal registrere en bruker på Finn.no e.l., og denne nettsiden blir utsatt for et angrep som medfører at brukerinformasjon kommer på avveie, så vil de som står bak slike angrep kunne forsøke å utnytte dette. For eksempel ved å prøve å logge seg inn på en virksomhets IT-systemer ved å bruke jobbmail-kontoen kombinert med de mest brukte eller vanligste passordene. Dette er et eksempel på informasjon som kan kommuniseres til de ansatte og som er relevant for hele organisasjonen. Informasjon som kan bidra til å øke kunnskap og bevissthet.

De årlige trusselvurderingene utgitt av for eksempel NSM og PST er bakgrunnen for noe av informasjonen som kommuniseres internt i organisasjonen. Men det holder ikke å tro at så

lenge de overordnede vurderingene kommuniseres så opprettholder man et godt kunnskaps- og bevissthetsnivå. Resultatene mine viser at dersom budskapet ikke er relevant, ikke treffer den riktige mottaker og ikke kommer på rett tid, da kan det oppleves som «trivielt» (I4) og uten stor nytteverdi for den enkelte. Som Reegård et al. (2019) påpeker så er det viktig at de ansatte forstår trusselbilde og hvordan truslene kan påvirke deres eget arbeid eller egen virksomhet, slik som eksemplet i avsnittet over viser. Dette nevner også informantene – det er vel så viktig å tilpasse budskapet til den enkelte avdeling eller seksjon (I1, I2, I5, I6). Ved å kommunisere hvorfor organisasjonen i det hele tatt er interessant kan være av stor betydning. Dersom forsker X og forsker Y blir bevisstgjort at deres forskningsdata har betydning i nasjonal eller internasjonal sammenheng, samtidig som det er aktører som er ute etter nettopp denne dataen for å manipulere den til fordel for seg selv, kan man bli mer oppmerksom på metoder angripere vil bruke for å få tak i denne informasjonen.

En velinformert arbeidsstyrke med god kompetanse kan være en sterk barriere mot uønskede hendelser (Nätt & Heide, 2021, s. 367). Dette kan være en av grunnene til at kommunikasjon utpeker seg som en mekanisme med sterk påvirkning på cybersikkerhetskultur – de ansatte virker selv å være klar over at kunnskap er viktig for å ta velinformerte valg og detektere avvik fra normalbildet. Ved å kommunisere hvorfor organisasjonen er interessant, for eksempel ved å understreke at noen kan ha interesse av å manipulere klimadata og derfor viktigheten av å beskytte den, kan man med det også signalisere at integritet er en viktig verdi for organisasjonen. Verdier henger også sammen med normer i den forstand at de er veiledende for hvilken atferd som skal til for å realisere dem (Bang, 2020, s.55).

For å eksemplifisere så kan det tenkes til at dersom integritet anses som en viktig verdi, kan ansatte tilpasse sin atferd for å leve i tråd med denne verdien. For eksempel ved at de blir flinkere på å rapportere om mistenkelige hendelser, låser PC når de forlater arbeidsstasjonen eller styrker passordet de bruker på organisasjonens systemer, fordi de er opptatt av å beskytte datamaterialets integritet. Summen av dette kan for eksempel være at de ansattes virkelighetsoppfatning – hvordan de tolker det som skjer rundt dem – blir at «organisasjonens forskningsdata er interessant for fremmede aktører, men vi er kollektivt opptatt av å verne om disse verdiene ved at vi har et stort fokus på cybersikkerhet». Kommunikasjon kan derfor bidra til at man oppnår det som er mye av kjernen i ENISAs (2018) definisjon på cybersikkerhetskultur – å gjøre cybersikkerhet til en integrert del av de ansattes tankesett i deres dagligdagse jobbutførelse.

### 6.2.3 Evaluering

Evaluering av de ansattes etterlevelse av instrukser og policyer kan ifølge Huang og Pearlson (2019) være effektive måter for å kartlegge hvilke områder organisasjonens cybersikkerhet er sterk og på hvilke områder den er sårbar. Som det er eksemplifisert tidligere kan phising-øvelser være en måte å evaluere på. Det er delte meninger blant informantene hvorvidt evaluering kan ha effekt på organisasjonens cybersikkerhetskultur. En av de største utfordringene med å evaluere ansatte for å få kartlagt styrkene og svakhetene med cybersikkerheten er at det må gjøres med omhu. Det er bekymringer knyttet til at det kan utvikles en «big brother»-mentalitet i organisasjonen hvor de ansatte føler seg overvåket og frykter for å bli uthengt dersom man gjør feil (I1, I5). Dette kan ha en påvirkning på de ansattes virkelighetsoppfatning hvor man tenker at «organisasjonen er ute etter å ta de som gjør feil».

Det burde være en felles oppfatning fra hele organisasjonen at hensikten med evalueringer er ikke å «ta» ansatte som ikke handler i tråd med instrukser, prosedyrer eller policyer. Resultatene mine viser at evaluering kan være et effektivt hjelpemiddel for å kartlegge de områder man er mest sårbare (I3, I4), på samme måte som skoler evaluer hvilke fag studentene gjør det dårligst i (Bang, 2020). Hvorfor man er sårbare på enkelte områder kan skyldes mangler eller uklarheter i interne instrukser, prosedyrer eller policyer. Ved å identifisere dette har man mulighet til å lage nye instrukser og prosedyrer, eller revidere allerede eksisterende. Dette gjør at det dannes nye normer. Nye nedskrevne regler. Da dannes det nye forventning om hva som er vanlig eller uvanlig handlemåter i ulike tilfeller (Einarsen et al, 2019; Bang, 2020). For som det fremkommer i studien så kan én tabbe fra ett enkeltindivid ødelegge et tiår med arbeid (I3). Det er mulig at de 80% av cyberangrep som skyldes menneskelig feil (Nobles, 2018) kan reduseres ved å kontinuerlig og systematisk evaluere og kartlegge sårbare områder, for så å iverksette kompetansehevende tiltak som for eksempel med trening eller kursing.

### 6.2.4 Ris og ros

Det er en frykt for at systemer for belønning og sanksjonering kan gå på bekostning av det Reason (1997) omtaler som en rapporterende kultur, et element av det som utgjør en sikkerhetskultur. Dersom organisasjonen har et ønske om at ansatte skal rapportere på uønskede hendelser eller avvik, kan de ansatte frykte at dersom man rapporterer inn avvik om seg selv eller andre så vil dette gå utover potensielle belønninger, eller det vil ramme en selv

eller kolleger i form av sanksjoner. Men som studien viser kan det på en annen side være at belønning og sanksjonering kan ha en holdningsskapende effekt (I3). Spesielt om de potensielle sanksjonene er av stor betydning for de ansatte. Eksempelvis doktorgradsstudenter som kan risikere å miste tilganger til viktige systemer eller informasjon. Det kan derfor tenkes til å ha effekt ved at man endrer atferd for å etterleve normene i organisasjonen, i frykt for sanksjoneringer. Videre viser studien at man også kan risikere at det utvikles en fryktkultur. Ansatte kan utvikle en paranoia som kan hindrer dem i å utføre sitt daglige arbeid fordi man blir ekstra redd for å utføre handlinger på organisasjonens systemer, i frykt for at feil handling skal påvirke belønninger eller føre til sanksjoner.

Derfor er det like viktig med en rettferdig kultur (Reason, 1997). Ansatte må kunne ha tillitt til at innrapporterte avvik ikke resulterer i ukritisk bruk av sanksjoneringsvirkemidler. For å kunne utvikle sikkerheten i organisasjonen er man avhengig av innrapporterte avvik fra ansatte. Frykt for represalier kan derfor ikke ta en ledende plass i de ansattes tankesett. Derfor er det som Huang og Pearlson (2019) peker på, viktig at sanksjonering ikke er uproporsjonal i forhold til sikkerhetsbruddet. Organisasjonen i denne studien har systemer for å sanksjonere brudd, og dette er som Einarsen et al. (2019) påpeker viktig dersom man ønsker at organisasjonens «spilleregler» skal utvikle seg til etablerte normer.

### 6.2.5 Trening og opplæring

Van Niekerk & Von Solms (2010) sier det er viktig å ikke ha en forutinntatthet om at «den gjennomsnittlige ansatte har den nødvendige kunnskapen til å utføre hans/hennes jobb på en sikker måte» (Van Niekerk & Von Solms, 2010, s. 478, min oversettelse). Trendene man ser peker også i retning av at cyberangrep i større grad rettes mot mennesker. Noe som understreker behovet for kompetanse om ulike trusler og angripernes metoder (ENISA, 2021; NorSIS, 2021). Derfor er trening og opplæring, på samme måte som kommunikasjon, viktige faktorer som bidrar til å øke kunnskaps- og bevissthetsnivået. Som informantene sier så har ikke organisasjonen et systematisk trenings- eller opplæringsprogram. Derfor virker det til at informasjon som kommer i opplæringsøyemed er tilfeldig. Organisasjonen har interne instrukser og policyer som de ansatte må sette seg inn i, men sikkerhetsarbeidet i en organisasjon avhenger ikke bare av prosedyrer, rutiner og tekniske løsninger. De ansattes holdninger, bevissthet og kunnskap er vel så viktig for å opprettholde et godt sikkerhetsnivå (Nätt & Heide, 2021). Holdninger og bevissthet er også begreper informantene trekker frem i sin egen forståelse av hva en cybersikkerhetskultur er.

Nasjonal sikkerhetsmåned i oktober blir brukt av sikkerhetssjefen for å nå ut til ansatte med relevant og rettidig informasjon. Blant annet ved å videreformidle informasjon som kommer fra for eksempel NSM, men også til å leie inn eksterne foredragsholdere eller gjennomgå interne dokumenter. Nettopp for å øke bevisstheten blant de ansatte. Men siden det ikke er formelle systemer for trening og opplæring kan dette ses på som ad hoc løsninger. Ikke bare er det nok at organisasjonen driver trening og opplæring. Den må også tilpasses den enkelte ansatte eller avdeling fordi man har ulike roller, dermed også et ulikt behov. I tillegg bør trening og opplæring være en gjentakende prosess som sikrer at man vedlikeholder kunnskapen (Reegård et al., 2019). Dette er også informantenes mening – trening og opplæring burde spisses mot den enkelte avdeling og gå gjennom faste intervall. Ferdigheter og kunnskap taper seg i takt med tiden det går mellom hver gang det trenes (Perry, 2004). Samtidig er teknologien i stadig utvikling og angrepsmetodene vil utvikle seg i takt med denne. Regelmessig og relevant trening kan derfor bidra til å øke ferdighets- og kunnskapsnivået.

Trening bare for treningens skyld, uten et mål og en hensikt, kan oppleves som «masete» og fremprovosere holdninger om at trening kun er en formalitet man er pålagt å gjennomføre ved faste intervall. Dette bidrar ikke til et ønske og motivasjon blant ansatte til å øke kunnskap. Dette er gjennomgående blant informantene også – tilpasset og relevant trening vil være motiverende og tankevekkende. Det vil også kunne danne grunnlaget for å arrangere fremtidige øvelser, da øvelser er en form for trening i den forstand at den enkelte får øvet på hvordan man skal respondere på hendelser (Perry, 2004) De ansatte får og mulighet til å teste kunnskapen opparbeidet seg gjennom trening- og opplæringsprogrammer. Kultur oppstår også når en gruppe deler erfaringer i fellesskap (Schein, 2009) og disse delte erfaringene kan oppnås gjennom for eksempel øvelser hvor man involverer hele eller deler av organisasjonen.

Som resultatene i studien viser er informantene positive til trening og opplæring. Men det som også er viktig å tenke på dersom man velger å gjennomføre trening og opplæring, er at det må gjøres en vurdering på hvorvidt denne skal være obligatorisk eller frivillig å delta på. En fare ved at den er frivillig er at man risikerer et ulikt kunnskaps- og bevissthetsnivå i organisasjonen. De som deltar vil kunne få ny og relevant kunnskap, mens de som ikke deltar vil sitte på gammel og utdatert kunnskap. Det er da det kan oppstå ulike subkulturer i organisasjonen – egne undergrupper i organisasjonen med andre verdier, normer og virkelighetsoppfatninger enn resten av medlemmene (Bang, 2020). Dette peker Schein (2009)

på at er viktig for ledelsen å være klar over, dersom det vokser frem subkulturer kan disse vokse seg sterke bli til hinder for at organisasjonen kan nå sine mål.

At trening og opplæring også utpeker seg som er mekanisme med sterk påvirkning på cybersikkerhetskultur kan henge sammen med at det er en mekanisme som er veldig synlig for de ansatte. Ved å ha et fokus på hyppig og relevant trening så signaliserer man at organisasjonen har et ønske om å øke kunnskapsnivået blant sine medarbeidere. De ansatte blir også direkte berørt ved at de må aktivt må ta del i treningen, for eksempel ved å gjennomgå ulike kurspakker eller være til stede på foredrag. Effekten av trening og opplæring blir derfor godt synlig for de ansatte.

### 6.2.6 Læring

At organisasjonen evner å lære av hendelser er viktig for å gjøre dem i stand til å implementere nye endringer som hever sikkerhetsnivået. Som Schunk (2012) viser til så tar læring utgangspunkt i at det skjer en endring, at endringen vedvarer over tid og at endringen enten er en atferdsendring eller kapasiteten til å utføre en endring. Informantene trekker frem ansettelsen av en egen sikkerhetsansvarlig som et eksempel på endringer som organisasjonen har gjennomgått. Dette er en stilling som har vedvart siden den ble opprettet. Med denne stillingen øker man også kapasiteten til videre å utføre endringer relatert til sikkerhetsarbeidet i organisasjonen, fordi sikkerhetsansvarlig kan være en pådriver for å øke kunnskap og ferdigheter, implementere nye planverk og prosedyrer, og bidra til atferdsendring blant ansatte innen cybersikkerhet.

Funnene fra studien peker på at mange av endringene, basert på identifiserte læringspunkter, skjer på et overordnet systemnivå og ikke på brukernivå (I5). Dersom endringene for eksempel skjer på et overordnet nivå i de tekniske systemene, kan disse endringene fremstå som usynlige for de ansatte. Det kan derfor være vanskelig i det hele tatt å vite om endringer har skjedd, ettersom man ikke nødvendigvis påvirkes direkte, ser dem, eller blir kommunisert hvilke endringer som har skjedd. Hvordan verdier, normer eller virkelighetsoppfatninger påvirkes kan derfor være vanskelig å si noe om dersom endringer ikke legges merke til.

Læring foregår både på individ- og organisasjonsnivå, men læringen som skjer på individnivå danner grunnlaget for at læring kan skje på organisatorisk nivå. Organisasjoner må derfor tilrettelegge for å integrere den individuelle læringen i den organisatoriske læringen (Wang & Ahmed, 2003). Fora for erfaring- og kunnskapsutveskling kan være gode arenaer for å

tilrettelegge for læring. For eksempel kan organisasjonens egne skrevne og uskrevne regler – normene – diskuteres og endres eller revideres basert på hvilke erfaringer man har gjort seg. Det gir også rom for å diskutere hva som oppleves som viktig for organisasjonen, altså verdiene.

Slike fora har organisasjonen, men de er enten forbeholdt ledergruppen eller IT-avdelingen. Studien viser at det kunne vært hensiktsmessig å ha samlinger som inkluderer flere i organisasjonen. Diskusjoner rundt gjeldende prosedyrer, og hvorvidt de er tilstrekkelig for å opprettholde et tilfredsstillende cybersikkerhetsnivå kan være positivt for de ansatte. For eksempel kan nye normer for organisasjonen komme som et resultat av slike samlinger. Det vil også være en mulighet for ansatte å lære om mer om cybersikkerhet, eller lære av tidligere hendelser, både i og utenfor organisasjonen. Slik kan man tilrettelegge for å inkludere den individuelle læringen i den organisatoriske læringen. Det vil selvfølgelig være utfordringer knyttet til å inkludere store deler av arbeidsstyrken i store felles fora for kunnskap- og erfaringsutveksling da det både er tid- og ressurskrevende, men å tilrettelegge for systematisk læring kan ha en effekt på cybersikkerhetskulturen.

### 6.2.7 Mekanismenes effekt på cybersikkerhetskultur

Som dataene viser vil alle mekanismene, isolert sett, kunne ha ulik påvirkning på både holdninger, normer, verdier, virkelighetsoppfatninger og kunnskap – mye av det som utgjør cybersikkerhetskulturen om man ser til den tidligere definisjonen av begrepet i seksjon 5.4. Det kan og sies at mekanismenes påvirkningsgrad kan ses i sammenheng med hverandre, det er et samspill mellom dem. For eksempel kan cybersikkerhetstematikk kommuniseres gjennom godt etablerte kommunikasjonskanaler, med relevant og tidsriktig informasjon, men dersom ledelsen ikke stiller seg bak det som kommuniseres, tar avstand fra det, eller neglisjerer cybertrusler så vil ikke budskapet oppleves som noe å ta hensyn til. Nettopp fordi det ikke forankres hos øverste ledelse at den cybersikkerhetstematikken som kommuniseres i ord, den skal følges opp i handling. Det vil for eksempel kunne oppstå et misforhold mellom organisasjonens mål om å øke kunnskap og bevissthet blant de ansatte, og organisasjonens evne til å forebygge uønskede digitale hendelser dersom ressurser for å gjennomføre trening og opplæring ikke er tilstrekkelig.

En forutsetning for å få til gode øvelser eller treningsmoduler, og at man lærer av dem, er at det trenes og øves så realistisk som mulig slik at de ansatte får oppleve hva som faktisk kan skje under en reell hendelse (Berlin & Carlstrom, 2015). Trening og opplæring vil derfor

kunne miste mye av sin verdi dersom innholdet i treningen ikke samsvarer med det digitale trusselbildet som kommuniseres i organisasjonen, og videre tilpasses trusler som er spesifikke for ens egen organisasjon og de verdiene organisasjonen forvalter. Dersom man ikke tar dette til etterretning vil man risikere at treningen ikke oppleves som relevant.

Et annet eksempel er at evaluering av ansatte vil heller ikke ha en hensikt dersom man ikke har systemer for å lære av de feil som avdekkes under slike evalueringer. Som Reason (1997) understreker så må ikke en sikkerhetskultur ses på som et produkt, men som en prosess. Derfor må det jobbes helhetlig og systematisk med alle mekanismene for å en total effekt av samtlige mekanismer. Studien viser at det på enkelte områder, slik som trening og opplæring, læring, og ris og ros, ikke virker til å være et systematisk arbeid, mens det på andre områder, som kommunikasjon er tegn til en voksende forståelse av viktigheten av å ha en systematisk tilnærming. De tre mekanismene identifisert, de med størst påvirkning, kan være et lite steg på veien til å gjøre cybersikkerhetskultur mindre «ill-defined», som Gcaza og Von Solms (2017) viser til. Hva som utgjør selve problemet, eller hva som utgjør løsningen med cybersikkerhetskultur er utfordrende å peke på, men de tre mekanismene *ledelse*, *kommunikasjon* og *trening og opplæring* kan være en start på veien mot arbeidet med å bygge cybersikkerhetskultur.

# 7 Konklusjon

## 7.1 Studiens funn og bidrag

Denne studien har bidratt til å øke forståelsen og kunnskapen om *hvordan* de interne organisatoriske mekanismene påvirker cybersikkerhetskultur, og med dette forsøkt å gjøre cybersikkerhetskultur til et mindre «ill-defined» problem. Studien har identifisert suksesskriterier, men også fallgruver med de ulike mekanismene, og med dette pekt på hvordan disse kan påvirke cybersikkerhetskulturen.

Ledelse, kommunikasjon, og trening og opplæring er de mekanismene som virker å ha størst effekt på cybersikkerhetskulturen. Dette kan være fordi effekten av dem er mer synlig og påvirker de ansatte direkte i større grad enn de tre resterende mekanismene. Ved å forstå alle de ulike mekanismenes suksesskriterier og fallgruver, og hvordan de påvirker cybersikkerhetskultur kan man målrettet arbeide mot å bygge en sterk cybersikkerhetskultur.

Studien har videre vist at det også er et samspill mellom mekanismene. Selv om det er et stort fokus rettet mot en eller flere mekanismer, kan den potensielle positive effekten utebli som

følge av manglende fokus rettet mot andre mekanismer. For eksempel kan effekten av tydelig, rettidig og relevant informasjon relatert til cybersikkerhet utebli dersom ledelsen ikke stiller seg bak og følger opp budskapet. Studien har derfor også adressert behovet for et helhetlig og systematisk arbeid med alle mekanismene.

Denne studien har både teoretiske og praktiske implikasjoner. Fra et teoretisk ståsted er forholdet mellom interne organisatoriske mekanismer og cybersikkerhetskultur i samsvar med den tidligere forskningen. Denne studien har bidratt til å nyansere dette forholdet ytterligere ved å utforske *hvordan* de interne organisatoriske mekanismene påvirker cybersikkerhetskultur. Funnene er nyttige for at virksomheter skal kunne utvikle en cybersikkerhetskultur, ved at suksesskriterier, fallgruver, samspillet mellom mekanismene, og viktigheten av et helhetlig og systematisk arbeid er identifisert.

## 7.2 Videre forskning

Som følge av avgrensningene i denne studien er det kun sett på interne organisatoriske mekanismer. Et naturlig veivalg for den videre forskningen kan være å inkludere eksterne faktorer, som for eksempel nasjonalt lovverk og ISO-standarder, se hvordan dette påvirker cybersikkerhetskulturen.

En god nasjonal cybersikkerhetskultur kan være avgjørende for hvor sårbare enkeltindivider og virksomheter er i fremtiden. Forskning på hvordan vi kan utvikle en god nasjonal cybersikkerhetskultur er også områder som trenger mer forskning. Kartlegging av kunnskap og holdninger til cybersikkerhet blant befolkningen er det og et behov for. Dette vil danne grunnlaget for hvordan man skal jobbe videre med å kommunisere og øke kunnskap blant befolkningen.

# Litteraturliste


Alshaikh, M. & Adamson, B. (2021). From awareness to influence: toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, *25*(5), 829-841. https://doi.org/10.1007/s00779-021-01551-2

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

Berg, B. L. & Lune, H. (2012). *Qualitative research methods for the social sciences* (8th. utg.). Pearson.

Berlin, J. M. & Carlstrom, E. D. (2015). Collaboration Exercises: What Do They Contribute? - A Study of Learning and Usefulness. *Journal of contingencies and crisis management*, *23*(1), 11-23. https://doi.org/10.1111/1468-5973.12064

Buchanan, D. A. & Bryman, A. (2009). *The SAGE handbook of organizational research methods*. Sage.

Cavelty, D. M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, *20*(3), 701-715.

Chen, Y., Ramamurthy, K. & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11-19.

Corradini, I. (2020). *Building a cybersecurity culture in organizations* (Bd. 284). Springer.

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. 2016 SAI computing conference (SAI),

Dalen, M. (2011). *Intervju som forskningsmetode* (2. utg. utg.). Universitetsforl.

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

DSB. (2012). Nasjonalt risikobilde 2012. I. Direktoratet for samfunnssikkerhet og beredskap

Einarsen, S., Martinsen, Ø. L., Skogstad, A. & Keeping, D. (2017). *Organisasjon og ledelse*. Gyldendal akademisk.

ENISA. (2018). *Cyber Security Culture in organisations*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

ENISA. (2021). *ENISA threat landscape 2021*. The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

ENISA. (2022). *ENISA Threat Landscape 2022*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

European Comission. (2022). *Digital Economy and Society Index (DESI) 2022 - Norway*. https://digital-strategy.ec.europa.eu/en/policies/desi

Gcaza, N. & Von Solms, R. (2017). Cybersecurity culture: an ill-defined problem. Information Security Education for a Global Digital Society: 10th IFIP WG 11.8 World Conference, WISE 10, Rome, Italy, May 29-31, 2017, Proceedings 10,

George, J. J. & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, *29*(3), 100249. https://doi.org/https://doi.org/10.1016/j.infoandorg.2019.04.001

Georgiadou, A., Mouzakitis, S., Bounas, K. & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, *62*(3), 452-462.

Grenness, T. (2012). *Hvordan kan du vite om noe er sant? : veiviser i forsknings- og utredningsarbeid for studenter, ledere, konsulenter og journalister* (2. utg. utg.). Cappelen Damm akademisk.

Grønmo, S. (2004). *Samfunnsvitenskapelige metoder*. Fagbokforl.

Huang, K. & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. Proceedings of the 52nd Hawaii International Conference on System Sciences,

International Telecommunication Union (ITU). (2008). ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity 2008. I. https://www.itu.int/rec/T-REC-X.1205/en

Johannessen, A., Christoffersen, L. & Tufte, P. A. (2016). *Introduksjon til samfunnsvitenskapelig metode* (5. utg. utg.). Abstrakt.

Maxwell, J. A. (2013). *Qualitative research design : an interactive approach* (3rd. utg., Bd. 41). Sage.

Meld. St. 10 (2016-2017). (2016). *Risiko i et trygt samfunn*. Justis- og beredskapsdepartementet. www.regjeringen.no

Meld. St. 38 (2016-2017). (2017). *IKT-sikkerhet - et felles ansvar*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/

Merriam, S. B. & Tisdell, E. J. (2016). *Qualitative research : a guide to design and implementation* (Fourth edition. utg.). Jossey-Bass, a Wiley Brand.

Mwim, E. N. & Mtsweni, J. (2022). Systematic review of factors that influence the cybersecurity culture. Human Aspects of Information Security and Assurance: 16th IFIP WG 11.12 International Symposium, HAISA 2022, Mytilene, Lesbos, Greece, July 6–8, 2022, Proceedings,

Nel, F. & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security*.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(3), 71-88.

NorSIS. (2021). *Trusler og trender 2021*. Norsk Senter for Informasjonssikring. https://norsis.no/publikasjoner/

NOU 2018:14. (2018). *IKT-sikkerhet i alle ledd: Organisering og regulering av nasjonal IKT-sikkerhet*. D. s.-o. serviceorganisasjon. https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/

NSM. (2022a). *Målrettede tjenestenektangrep mot norske nettsteder*. Nasjonal Sikkerhetsmyndighet. Hentet 13.02.2023 fra https://nsm.no/aktuelt/malrettede-tjenestenektangrep-mot-norske-nettsteder

NSM. (2022b). *Nasjonalt digitalt risikobilde 2022*. Nasjonal Sikkerhetsmyndighet.

NSM. (2023). *Risiko 2023 - Økt uforutsigbarhet krever høyere beredskap*. Nasjonal Sikkerhetsmyndighet.

Nätt, T. H. & Heide, C. F. (2021). *Datasikkerhet : ikke bli svindlerens neste offer* (2. utgave. utg.). Gyldendal.

Perry, R. W. (2004). Disaster exercise outcomes for professional emergency personnel and citizen volunteers. *Journal of contingencies and crisis management*, *12*(2), 64-75.

Pettigrew, A. M. (1979). On Studying Organizational Cultures. *Administrative Science Quarterly*, *24*(4), 570-581. https://doi.org/10.2307/2392363

Politiet. (2022). *Politiets trusselvurdering 2022*. Kripos. https://www.politiet.no/om-politiet/tall-og-fakta/politiets-trusselvurdering/

PST. (2023). *Nasjonal trusselvurdering 2023*. Politiets sikkerhetstjeneste.

Reason, J. (1997). *Managing the Risks of Organizational Accidents* (1. utg.). Taylor & Francis. https://doi.org/10.4324/9781315543543

Reegård, K., Blackett, C. & Katta, V. (2019). The concept of cybersecurity culture. 29th European Safety and Reliability Conference,

Reid, R. & Van Niekerk, J. (2014). From information security to cyber security cultures. 2014 Information Security for South Africa,

Ruighaver, A. B., Maynard, S. B. & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56-62. https://doi.org/10.1016/j.cose.2006.10.008

Schein, E. H. (2009). *The corporate culture survival guide* (Bd. 158). John Wiley & Sons.

Schein, E. H. (2010). *Organizational culture and leadership* (4th. utg.). Jossey-Bass.

Schein, E. H., Arnulf, K. & Brun, H. (1987). *Organisasjonskultur og ledelse : er kulturendring mulig?* Mercuri media forl.

Schreier, M. (2012). *Qualitative content analysis in practice : Margrit Schreier*. SAGE.

Schunk, D. H. (2012). *Learning theories an educational perspective*. Pearson Education, Inc.

Solms, B. V. (2000). Information security-The third wave? *Computers & Security*, *19*(7), 615-615.

Sun, S. (2008). Organizational culture and its themes. *International Journal of Business and Management*, *3*(12), 137-141.

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

Van Niekerk, J. & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476-486.

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102.

Wang, C. L. & Ahmed, P. K. (2003). Organisational learning: a critical review. *The learning organization*, *10*(1), 8-17.

Zimmermann, V. & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169-187.

Aase, T. H. & Fossåskaret, E. (2014). *Skapte virkeligheter : om produksjon og tolkning av kvalitative data* (2. utg. utg.). Universitetsforl.

# VEDLEGG

## Vedlegg 1 - Informasjonsskriv og samtykkeskjema

## Vil du delta i forskningsprosjektet

**Interne organisatoriske mekanismers påvirkning på cybersikkerhetskultur**

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke hvordan interne organisatoriske mekanismer påvirker cybersikkerhetskultur. Bakgrunnen er Nasjonal Sikkerhetsmyndighets trusselvurdering fra 2022, hvor de blant annet peker på samfunnsområdet forskning og utvikling som et av områdene særlig utsatt for cyberangrep. I dette skrivet gir jeg deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

**Formål**

Formålet med prosjektet er å få inngående kunnskap i hvordan interne organisatoriske mekanismer påvirker cybersikkerhetskulturen i organisasjoner. Problemstillingen til prosjektet er «hvordan påvirker interne organisatoriske mekanismer cybersikkerhetskulturen i virksomheter». Prosjektet er avsluttende masteroppgave ved studieretningen samfunnssikkerhet ved UiT Norges Arktiske Universitet.

**Hvem er ansvarlig for forskningsprosjektet?**

UiT Norges Arktiske Universitet er ansvarlig for prosjektet.

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

Du får spørsmål om å delta fordi du representerer en aktør relevant for oppgavens problemstilling og formål. Du kontaktes fordi du har uttrykt interesse for å bidra i prosjektet etter å ha mottatt en mail som kort beskriver dette prosjektet. Kontaktinformasjonen din er videreformidlet til meg på e-post med bakgrunn i din interesse om å delta.

**Hva innebærer det for deg å delta?**

Hvis du velger å delta i prosjektet innebærer det at du deltar i et intervju, fysisk eller digitalt, på ca. 30-45 minutter. Intervjuet inneholder spørsmål vedrørende de interne organisatoriske mekanismene og hvordan de påvirker cybersikkerhetskulturen. De interne mekanisme er ledelse, kommunikasjon, evaluering, belønning og sanksjoner, trening og læring. Jeg tar lydopptak og notater fra intervjuet og dataen blir oppbevart til prosjektets slutt, innen midten av juli 2023.

**Det er frivillig å delta** Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

**Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger**

Jeg vil bare bruke opplysningene om deg til formålene jeg har fortalt om i dette skrivet. Jeg behandler opplysningene konfidensielt og i samsvar med personvernregelverket. De som vil ha tilgang til dine opplysninger er undertegnede og veiledere for masteroppgaven. For å sikre at uvedkommende ikke får tilgang til dine personopplysninger vil jeg erstatte navnet og kontaktopplysningene dine med en kode som lagres på en egen navneliste adskilt fra øvrige data. Informasjonen gitt under intervjuet vil tas opp på båndopptaker før den digitale lydfilen videre lagres på universitetets egne servere.

Som deltaker vil du ikke kunne identifiseres i oppgaven, men om du har lederansvar eller ikke vil kunne publiseres i oppgaven. Organisasjonen du representerer vil også kunne bli nevnt.

**Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?**

Prosjektet vil etter planen avsluttes når oppgaven blir godkjent, medio juli 2023. Ved prosjektets slutt vil all data som er samlet inn om og fra deg slettes.

**Hva gir oss rett til å behandle personopplysninger om deg?**

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra UiT Norges Arktiske Universitet har Sikt – Kunnskapssektorens tjenesteleverandør 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:

Christer Thomassen Furøy
E-post: cfu002@uit.no
Tlf: 930 89 570
Student

Maria Sydnes
E-post: maria.sydnes@uit.no Tlf: +47 776 60 363
Førsteamanuensis – Veileder for oppgaven

Sølvi Brendeford Anderssen
E-post: personvernombud@uit.no
Tlf: 776 46 153
Vårt personvernombud

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:
Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen
Christer Thomassen Furøy

# Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «*Interne organisatoriske mekanismers påvirkning på cybersikkerhetskultur»*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

☐ å delta i intervju (med lydopptak og transkribering)

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet. (Samtykke kan gis ved skriftlig signatur i dette skjemaet, et skriftlig samtykke til meg på e-post, eller muntlig på lydopptak før intervjuets start)

---

(Signert av prosjektdeltaker, dato)

# Vedlegg 2 - Intervjuguide

Intervjuspørsmål

Hva forstår du med begrepet cybersikkerhetskultur?

**Interne organisasjonsfaktorer**

**Ledelse:**

1. Hvordan prioriterer du cybersikkerhet i din seksjon/avdeling?
2. Hvilke ressurser har du å tildele din seksjon for å styrke cybersikkerhetsarbeidet?
3. Hvordan vil du beskrive din egen deltakelse ovenfor din seksjon/avdeling når det gjelder cybersikkerhetstematikk?
4. Hvordan følger du opp arbeidet med cybersikkerhet i din avdeling?
5. Hvilke krav stiller du til dine ansatte/seksjon/avdeling når det gjelder cybersikkerhet?
6. Hvordan tror du ledelsens involvering kan påvirke cybersikkerhetskulturen i virksomheten?

**Kommunikasjon:**

1. Hvordan kommuniseres cybersikkerhetstematikk i organisasjonen?
    a. Hvilken informasjon kommuniseres?
    b. Hvordan gjøres det?
2. På hvilken måte er ansvaret du har ifm. cybersikkerhet, ved å inneha din rolle, kommunisert til deg?
3. Hvordan mener du organisasjonen skal kommunisere cybersikkerhetstematikk for å øke de ansattes bevissthet og kunnskap?
4. Hvilke systemer har organisasjonen for å rapportere om cybersikkerhetshendelser (mistenkelig mail osv.?)
5. Hvordan tror du kommunikasjon knyttet til cybersikkerhet kan påvirke cybersikkerhetskulturen?

**Evaluering:**

1. Hvilke systemer har organisasjonen for å evaluere de ansattes etterlevelse av cybersikkerhetspolicy/cybersikkerhetsinstrukser?
    a. Hvis ja: Hvordan evalueres det?
    b. Hvem gjør det?
    c. Hvor ofte?
    d. Hva resulterer slike evalueringer i?
2. Hvordan tror du evaluering av de ansatte kan påvirke cybersikkerhetskulturen?

Ris og Ros:

3. Hvordan belønnes eller straffes ansatte eller avdelinger ved organisasjonen ved etterlevelse/brudd på cybersikkerhetspolicy/instrukser?
4. Hvordan tror du systemer som belønner/sanksjonerer akseptabel/uakseptabel adferd kan påvirke cybersikkerhetskulturen?

Trening:

5. Hvordan trenes/opplæres ansatte for å øke bevisstheten rundt de trender og trusler som finnes i cyberdomenet?
    a. Hvis ja: hva er innholdet i treningen/opplæringen?
    b. Hvor ofte trenes det?
    c. Hvem trenes?
    d. Noe du savner?
6. Hvordan vil du beskrive din egen kunnskap om cybersikkerhetstrusler og konsekvensene av disse?
7. Hvordan tror du trening kan påvirke cybersikkerhetskulturen?

**Læring**

1. Har det skjedd endringer i organisasjonen (f.eks nye sikkerhetstiltak eller nye måter å gjøre ting på) som følge av cybersikkerhetshendelser
    a. Når skjedde det?
2. Gjelder disse endringene fortsatt?
3. Har dere samlinger/fora for erfaringsutvekslinger med hverandre?
4. Hvordan har måten organisasjonen arbeider med cybersikkerhet endret seg over tid?
    a. På hvilken måte har det ført til endringer for eksempel cybersikkerhetspolicy/instrukser/treningsprogram/kommunikasjon?
5. Hvordan tror du læring påvirker cybersikkerhetskulturen?

- Om du skulle rangert de seks faktorene – ledelse, kommunikasjon, evaluering, ris og ros, trening og læring – fra minst til størst påvirkning på cybersikkerhetskulturen, hvordan ville du rangert de?