UiT Norges arktiske universitet

Fakultet for humaniora, samfunnsvitenskap og lærerutdanning, Institutt for samfunnsvitenskap

Informasjonssikkerhetskultur - en litteraturstudie

Hva skaper og påvirker informasjonssikkerhetskultur og hvilke tiltak kan føre til forbedring av informasjonssikkerhetskulturen?

Øyvind Friborg

Masteroppgave i strategisk ledelse og økonomi STV 3910 - desember 2023

Forord

Denne masteroppgaven markerer slutten på 2.5 år med studier ved siden av jobb og familie. Perioden har vært full av læring, utvikling og knallharde prioriteringer. Jeg skylder en stor takk til min tålmodige og støttende kone for tilrettelegging. Øvrig familie må også takkes for oppmuntring og støttende ord underveis. En stor takk også til forelesere og ansatte ved UiT for et flott program hvor opparbeidet erfaring møter akademisk utvikling. Til slutt vil jeg også rette en takk til Thor Øivind for å lose meg i havn med oppgaven med faglige innspill.

Øyvind Friborg

Oslo, november 2023

Sammendrag

Informasjonssikkerhet har som følge av den digitale transformasjonen de siste tiårene fått et økende fokus i organisasjoner. Det er også en økende annerkjennelse i forskning at tekniske sikkerhetstiltak ikke er tilstrekkelig for å møte dagens komplekse sikkerhetsutfordringer. Når den menneskelige faktoren ofte identifiseres som det svakeste leddet innen informasjonssikkerhet kan en styrket informasjonssikkerhetskultur bidra til å sikre organisasjoners informasjon. Denne studien har derfor undersøkt hva som kan skape og styrke en informasjonssikkerhetskultur gjennom problemstillingen: *Hva skaper og påvirker informasjonssikkerhetskultur og hvilke tiltak kan føre til forbedring av informasjonssikkerhetskulturen?*

Gjennom en litteraturstudie har studien fokusert på definisjoner av informasjonssikkerhetskultur og identifisert faktorer som påvirker informasjonssikkerhetskulturen. Oppgaven presenterer en gjennomgang av de syv faktorene som er mest gjengitt i litteraturen og foreslår en inndeling av de totalt 43 identifiserte faktorene.

Innholdsfortegnelse

Liste over figurer og tabeller

Tabelliste

Figurliste

1 Tema og problemstilling

1.1 Innledning

I oktober 2023 besluttet Norges statsminister, Jonas Gahr Støre, å opprette et eget digitaliseringsdepartement med effekt fra januar 2024. Støre begrunnet dette med at «*økt bruk av teknologi og digitalisering påvirker hverdagen til hver og en av oss, men også samfunnet som helhet. Det gir enorme muligheter, men krever også kunnskap*» (Gjessing, 2023). I november 2023 markeres ett år siden ChatGPT ble tilgjengelig for alle, og med det ble kunstig intelligens og generativ AI, gjort tilgjengelig for allmennheten. I oktober 2023 skrev Nasjonal sikkerhetsmyndighet (NSM) at Norge er under digitale angrep hver dag og konkluderer med at den digitale sikkerheten må bli bedre (NSM, 2023). I dagens samfunn dominerer altså teknologi og digitale løsninger stadig flere områder av våre liv og inkluderer blant annet helse, jobb, strømforsyning, telekommunikasjon, skole og utdanning, barnehager og fritidsaktiviteter. Et av resultatene er komplekse verdikjeder og underleverandører av IT-systemer med store tilganger. Arbanas et al. (2021) hevder at den digitale transformasjonen de siste tiårene har gjort informasjonssikkerhet til et av de viktigste aspektene for organisasjoner. Med dette øker kravet til å beskytte sensitive opplysninger, som personlige data og konfidensielle forretningshemmeligheter i alle ledd. Norges nasjonale etterretning- og sikkerhetstjenester, Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST), og NSM peker stadig på det store spennet i trusselbildet Norge står ovenfor. Truslene er sammensatte og sektorovergripende, og kombinasjonen av ulike virkemidler gjør trusselbildet utfordrende (Forsvaret, 2022). Tidligere var forskningen hovedsakelig konsentrert rundt tekniske aspekter, med fokus på teknologiske og fysiske sikkerhetskontroller. I lys av nyere forskning, anerkjenner stadige flere forskere at teknologi alene ikke er tilstrekkelig for å adressere kompleksiteten i dagens sikkerhetsutfordringer. Sikkerhet anses nå ikke bare som et «teknisk» problem, men også i økende grad som et «menneskelig» problem. Denne erkjennelsen understreker behovet for en mer helhetlig tilnærming som integrerer både tekniske løsninger og menneskelige aspekter for effektivt å forvalte og beskytte informasjon i en stadig mer digitaliserte verden (Arbanas et al, 2021).

Ett av tiltakene for å øke den digitale sikkerheten er å styrke sikkerhetskulturen i organisasjoner, og mer spesifikt for den digitale sfæren, informasjonssikkerhetskulturen. Den menneskelige faktoren identifiseres ofte som det svakeste leddet innen informasjonssikkerhet (Mahfuth et al., 2017). Likevel er den menneskelige faktoren ofte oversett (Thomson et al., 2006). Ved å fokusere på å utvikle og styrke informasjonssikkerhetskulturen kan

medarbeidere og organisasjoner bidra til å skape en sikrere digital verden. NSM definerer sikkerhetskultur som *et sett med verdier som deles av medarbeidere i en virksomhet, og som er med på å påvirke deres tanker og forventinger til sikkerhet. Ved å motivere medarbeiderne til å handle på en måte som ivaretar sikkerheten, kan virksomheten skape en god sikkerhetskultur* (NSM, 2020a). Forenklet sagt kan vi si at begrepet informasjonssikkerhetskultur begrenser seg til organisasjoners kultur knyttet til informasjonssikkerhet, og ikke tar for seg hele bredden i begrepet sikkerhet. En definisjon av informasjonssikkerhetskultur er eksempelvis de *oppfatninger, holdninger, verdier og kunnskap om hvordan ting gjøres i en organisasjon for å følge opp nødvendige informasjonssikkerhetskrav med mål om å beskytte informasjonsverdier* (Alhogail & Mirza, 2014). Gitt den rivende teknologiske utviklingen med Generativ AI tilgjengelig for allmenheten, komplekse verdikjeder og et utfordrende trusselbilde, er det nødvendig å oppdatere forskningen innen informasjonssikkerhetskultur.

1.1.1 Problemstilling og forskningsspørsmål

Denne studien velger å legge til grunn at informasjonssikkerhetskultur kan styres. I denne oppgaven vil jeg derfor se nærmere på begrepene informasjonssikkerhetskultur og hvordan en god informasjonssikkerhetskultur kan benyttes som et av tiltakene for å oppnå høyere informasjonssikkerhet. Oppgaven legger også til grunn at en god sikkerhetskultur kan bidra til å beskytte organisasjoner og samfunnet mot trusler og sårbarheter.

Min problemstilling er følgelig:

Hva skaper og påvirker informasjonssikkerhetskultur og hvilke tiltak kan føre til forbedring av informasjonssikkerhetskulturen?

For å utforske dette vil jeg se nærmere på følgende forskningsspørsmål:

i. Hvordan defineres informasjonssikkerhetskultur?
ii. Hvilke faktorer har størst påvirkning på organisasjoners informasjonssikkerhetskultur?

Det første forskningsspørsmålet omhandler hva begrepet informasjonssikkerhetskultur innebærer. Hensikten med forskningsspørsmålet er å belyse og undersøke ulike forståelser av informasjonssikkerhetskultur. Dette danner videre grunnlaget for hvilke faktorer som er sentrale i arbeidet med å utvikle en sterkere informasjonssikkerhetskultur. Videre omhandler det andre forskningsspørsmålet hva informasjonssikkerhetskultur påvirkes av, herunder hva

som kan forbedre den. Hensikten med spørsmålet er å utforske faktorer som kan påvirke sikkerhetskulturen i organisasjoner.

1.2 Avgrensing

Jeg har valgt å avgrense denne oppgaven til å fokusere på aspekter ved organisasjonskultur spesifikt relatert til informasjonssikkerhet og vil i analysen derfor ikke gå inn på det norske språkets manglende skille mellom «safety» og «security». Det er likevel aspekter ved terminologien som er interessante i forskning innenfor sikkerhetsdomenet. I NOU 2006: 6 *Når sikkerhet er viktigst* får vi følgende definisjon av «safety»: «sikkerhet mot uønskede utilsiktede hendelser» og «security»: «sikkerhet mot uønskede tilsiktede hendelser» (Eskeland, 2017). Jeg adresserer heller ikke hvordan man kan endre informasjonssikkerhetskultur grunnet oppgavens begrensende omfang.

1.3 Oppgavens oppbygning

Tabell 1 Oppgavens oppbygning

Kapittel 1 Innledning og begrepsavklaring	Introduksjon til oppgavens tema presenteres. Bakgrunnen for problemstillingen og selve problemstillingen, inkludert forskningsspørsmål, forklares. Jeg vil også presentere avgrensninger for oppgaven i dette kapittelet. Videre vil jeg også gjennomgå sentrale begrep innenfor digital sikkerhet ettersom det er et svært bredt tema.
Kapittel 2 Teori	I dette kapittelet presenteres det teoretiske bakteppet for oppgaven knyttet til samfunnsvitenskapen. De analytiske dimensjonene som danner grunnlaget for empirien og analysen presenteres også her.
Kapittel 3 Metode	Her presenteres metodiske valg jeg har gjort for det empiriske og analytiske arbeidet, samt styrker og svakheter ved metodikken.
Kapittel 4 Empiri	I kapittel 4 presenteres de empiriske resultater fra litteraturstudien.
Kapittel 5 Diskusjon	Her drøftes empiriske resultater opp mot teoretisk rammeverk, og de viktigste funnene drøftes opp mot forskningsspørsmålene.
Kapittel 6 Konklusjon	Problemstillingen diskuteres og oppgaven konkluderes. Avslutningsvis deles tanker rundt videre forskning.

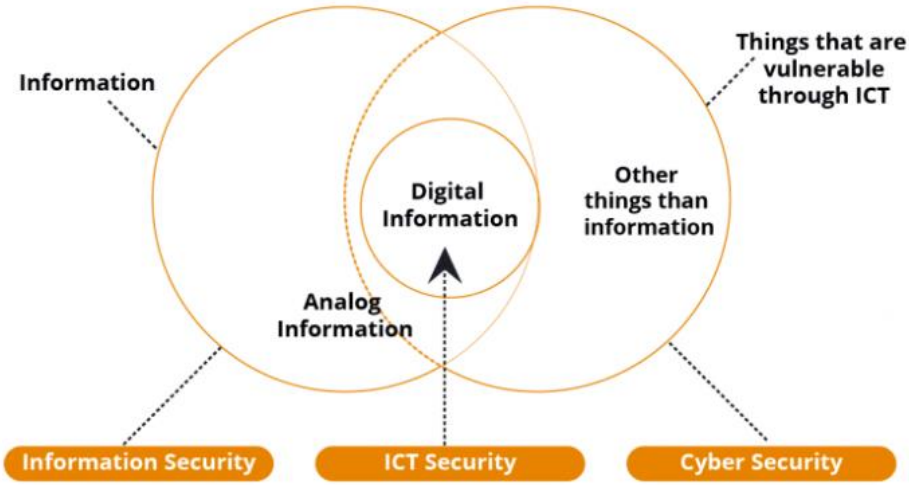
1.4 Begrepsavklaringer – digital sikkerhet

Innledningsvis vil jeg utforske og definere nøkkelbegrepene som er sentrale innen digital sikkerhet. Digital sikkerhet er et felt i stadig endring og utvikling, og det er derfor viktig å ha en klar og oppdatert forståelse av de terminologier og konsepter som brukes. Denne

begrepsavklaringen er ment å fungere som en grunnstein for resten av oppgaven, og vil gi et solid utgangspunkt for å forstå de diskusjonene og analysene som følger. Det er også ulike oppfatninger av de ulike begrepene som brukes. Ved å etablere et klart definert begrepsapparat fra starten, vil jeg formidle hva jeg legger i begrepene og begrunne valg som er tatt.

1.4.1 Cyber-, informasjons-, og IKT-sikkerhet

Cybersikkerhet, informasjonssikkerhet og IKT-sikkerhet er alle begrep som benyttes når vi snakker om digital sikkerhet. I flere tilfeller brukes disse begrepene om hverandre og tidvis helt eller delvis synonymt (NOU, 2018). Eksempelvis brukes begrepene «IKT-sikkerhet», «digital sikkerhet» og «cybersikkerhet» synonymt i enkelte EØS-posisjonsnotater (Regjeringen, 2023). Selv om begrepene er overlappende på flere områder, har de også noen forskjeller. Oppsummert kan vi si at cybersikkerhet fokuserer på beskyttelse mot digitale angrep, informasjonssikkerhet omhandler bredere beskyttelse av all type informasjon, både digital og fysisk, mens IKT-sikkerhet er et mer overordnet begrep som dekker sikring av all informasjons- og kommunikasjonsteknologi. Dette er illustrert i figur 1. I det følgende vil jeg gi en kortfattet, men litt mer utfyllende beskrivelse av begrepene.



Figur 1 Illustrasjon av forholdet mellom informasjonssikkerhet, IKT-sikkerhet, og cybersikkerhet. Figuren er hentet fra Leverage Edu (2023) og bygger på Von Solms & Van Niekerks fremstilling (2013).

1.4.2 Informasjonssikkerhet

Informasjonssikkerhet handler om å beskytte informasjon, uavhengig om denne er digital, fysisk eller verbal. Beskyttelsen manifesterer seg i de praksiser, prosedyrer og systemer

designet for å beskytte og bevare informasjonens konfidensialitet, integritet og tilgjengelighet. For å oppnå hensiktsmessig beskyttelse, balanserer informasjonssikkerhet forebyggende, detekterende, reagerende, og korrektive tiltak, som defineres basert på ulike organisasjoners ressurser, risikotoleranse, og forretningsbehov (ISO, 2022). Informasjonssikkerhetsverdiene konfidensialitet, integritet og tilgjengelighet forkortes ofte til KIT på norsk eller CIA på engelsk (confidentiality, integrity, og availability) (Nätt & Heide, 2021). Konfidensialitet vil si at bare de som skal ha tilgang til data og systemer har tilgang. Dette forhindrer uautorisert tilgang og avsløring av informasjon. Integritet dreier seg om at informasjonen er korrekt og at ingen uautoriserte kan endre innholdet uten at dette synliggjøres. Digitaliseringsdirektoratet (u.å) sier at informasjon har mistet sin integritet «dersom den er endret utilsiktet eller av uautoriserte». Tilgjengelighet sikrer at informasjon er tilgjengelig når den er nødvendig (ISO, 2022).

I organisasjonssammenheng er målet med informasjonssikkerhet å redusere risikoen til et akseptabelt nivå og å opprettholde organisasjonens evne til å oppfylle sine mål, oppdrag og visjon. Arbeidet med informasjonssikkerhet formaliseres ofte i et styringssystem for informasjonssikkerhet (ISMS). Her beskrives det hvordan hensiktsmessige policyer, prosedyrer, teknologiske løsninger, og opplæring av ansatte skal understøtte organisasjonenes overordnede mål (ISO, 2022).

Informasjonssikkerhet skal videre også beskytte den underliggende teknologien som benyttes i behandlingen av data (Von Solms & Van Niekerk, 2013). Det er altså systemer og prosedyrer som skal beskytte informasjonen, som ofte er en sentral del av verdiene til en organisasjon, og ivareta informasjonens KIT. Reegård et al. (2019) påpeker at disse praksisene, systemene og prosedyrene kan være utsatt for sårbarheter og trusler. Samtidig blir disse prosessene og systemene håndtert av mennesker og dermed påvirket av menneskelig adferd når individer i en organisasjon skal behandle informasjon. Manglende kunnskap, begrenset eller ingen opplæring og uforsiktige handlinger er årsaker som medvirker til at mennesker ofte pekes på som det svakeste leddet i informasjonssikkerhet (Mahfuth et al., 2017; Van Niekerk & Von Solms, 2010). Ettersom teknologien vi anvender er i stadig endring, innebærer dette at prosedyrer og systemer også kontinuerlig må tilpasses og oppdateres. Informasjonssikkerhet er derfor ikke en tilstand eller et produkt, men en iterativ prosess (ISO, 2022). Det samme påpeker Reason (1997) som Bostrøm et al. (2021) har oversatt på en elegant måte: «*Det er umulig å se på god sikkerhetskultur som et ferdig*

produkt. Som i religion er det prosessen og ikke produktet som er viktig. Belønningen ligger i selve arbeidet mot målet som alltid blir liggende foran oss.»

1.4.3 IKT-sikkerhet

Begrepet IKT-sikkerhet har endret seg fra tidligere å fokusere på beskyttelse av nettverk og systemer til også å inkludere informasjonen som behandles i disse systemene. I tillegg inkluderes også de tjenestene som systemene leverer (NOU, 2018). En årsak til dette er ifølge NSM (2020b) at informasjonssystemer tidligere ofte var isolerte systemer som det var enkelt å sikre, men at disse nå i større grad er sammenkoblet for økt funksjonalitet. Det eksisterer også et ønske og en forventing om mer mobile løsninger. Oppsummert definerer NOU (2018) IKT-sikkerhet som «*beskyttelse av IKT-systemene, samvirket mellom systemene, tjenestene som leveres av systemene, eller informasjon som behandles i systemene*». I likhet med informasjonssikkerhet er sikkerhetsmålene til IKT-sikkerhet knyttet til å sikre KIT. NSM (2020c) omtaler derfor sine grunnprinsipper for IKT-sikkerhet som «*et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk.*»

1.4.4 Cybersikkerhet

Som vi ser av figur 1 rommer cybersikkerhet også andre ting enn informasjon, inkludert det som er sårbart gjennom IKT-systemer. Dette rommer brukere, nettverk, enheter, programvare, prosesser, informasjon i transitt eller i lagret tilstand, applikasjoner, tjenester, og systemer som kan kobles direkte eller indirekte til nettet (Furøy, 2023; ITU, 2008). Rent konkret definerer International Telecommunication Union (ITU, 2008, s.2) cybersikkerhet som:

Samlingen av verktøy, policyer, sikkerhetskonsepter, sikkerhetstiltak, retningslinjer, tilnærminger til risikostyring, handlinger, opplæring, beste praksiser, sikkerhetsgarantier og teknologier som kan brukes til å beskytte det digitale miljøet og organisasjonens og brukerens eiendeler. Organisasjonens og brukerens eiendeler inkluderer tilkoblede databehandlingsenheter, personell, infrastruktur, applikasjoner, tjenester, telekommunikasjonssystemer og totaliteten av overført og/eller lagret informasjon i det digitale miljøet

ITU sin definisjon samsvar i stor grad med Von Solms & Van Niekerk (2013, s101) sin definisjon av cybersikkerhet som: *Beskyttelsen av selve cyberspace, elektronisk informasjon, IKT-systemene som støtter cyberspacet, og brukerne av cyberspace i deres personlige, samfunnsmessige og nasjonale kapasitet, inkludert noen av deres interesser, enten de er håndgripelige eller immaterielle, som er sårbare for angrep som stammer fra cyberspace*.

National Institute of Standards and Technology (NIST) presenterer en enda kortere definisjon, som likevel rommer de to overordne og sier *at cybersikkerhet er evnen til å beskytte eller forsvare bruken av cyberspace fra cyberangrep* (NIST, u.å,). Vi ser oppsummert at cybersikkerhet rommer flere og andre elementer enn bare informasjon, eller IKT-systemer.

1.5 oppsummering

Oppsummert ser vi at Cybersikkerhet, informasjonssikkerhet og IKT-sikkerhet skilles i akademia og blant myndighetsorgan. Samtidig er de tett knyttet sammen og brukes om hverandre uten å endre innhold blant annet av norske myndighetsorganer. Det er også min erfaring at beslutningstakere i virksomheter blander begrepene uten at det endrer *hva* de snakker om. Selv om man kan argumentere for at begrepene beskriver ulike er nyanser innen digital sikkerhet vil jeg i denne oppgaven behandle dem som synonymer. Dette med bakgrunn i at både norske myndigheter og virksomheter som arbeider med cyber- og informasjonssikkerhetskultur benytter begrepne uten å bevisst skille på innholdet (NOU, 2018; Regjeringen, 2023). Den praktiske konsekvensen dette får for denne studien er at jeg inkluderer både begrepene cybersikkerhetskultur og informasjonssikkerhetskultur i søkekriteriene som jeg kommer tilbake til i kapittel 3.3 operasjonalisering hvor jeg ser på inklusjonskriterer for litteraturstudien. Videre i oppgaven benytter jeg begrepet informasjonssikkerhetskultur ettersom «information security culture» var begrepet majoriteten (10/11) av utvalgte artikler for denne studien benyttet. Den siste artikkelen (Uchendu et al. 2021) bruker begrepet cyber sikkerhetskultur, men har også inkludert sikkerhetskultur og informasjonssikkerhetskultur begrepene i litteraturstudien som ble gjennomført.

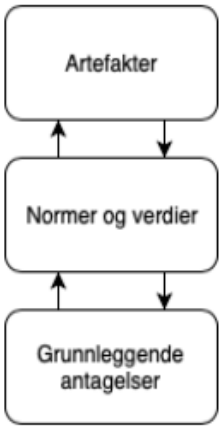
2 Teori

Som nevnt innledningsvis er målet til denne studien å utforske hva som skaper og påvirker informasjonssikkerhetskultur og hvilke tiltak kan føre til forbedring av informasjonssikkerhetskulturen. For å kunne gjennomføre en hensiktsmessig analyse er det nødvendig å se på de vitenskapelige/akademiske teoriene som danner grunnlaget for problemstillingen. I dette kapittelet vil jeg derfor presentere det analytiske rammeverket som benyttes i oppgaven og redegjøre for de overordnede begrepene denne studien bygger på. Organisasjonskultur er fundamentet som sikkerhetskultur og informasjonssikkerhetskultur bygger på. Det er derfor naturlig å starte med organisasjonskultur før vi vi undersøker de andre nivåene av organisasjonskulturen (Reason, 1997; Fernández-Muñiz et al., 2007).

2.1 Kultur og organisasjonskultur

Kultur er et begrep som benyttes med ulike assosiasjoner. I 1954 eksisterte det minst 160 ulike definisjoner av begrepet kultur (Kroeber & Kluckhohn, 1954). Den samme ulike tilnærmingen til begrepet ser vi i dag og Alvesson (2002) skriver at begrepene kultur og organisasjonskultur benyttes svært variert. Videre hevder han at betegnelsen «kultur» fortsatt har ikke noen omforent definisjon. Antonsen (2009) har på sin side foreslått den vide definisjonen «Alt som ikke er natur, er kultur». En slik bred definisjon kompliserer imidlertid forskningsprosessen da det blir ekstremt mange elementer å hensynta. Selv om det også eksisterer mange definisjoner av organisasjonskultur, finnes det noen likhetstrekk. De mest siterte inkluderer ofte normer, verdier, antagelser og virkelighetsoppfatninger som sentrale faktorer. Ifølge Jacobsen og Thorsvik (2021), er Edgar Schein sin definisjon den mest refererte i organisasjonslitteraturen. Schein definerer organisasjonskultur som «*et mønster av felles grunnleggende antagelser som ble lært av en gruppe i det den taklet sine eksterne tilpasnings- og interne integrasjonsproblemer, som har fungert bra nok til å bli betraktet som gyldige, og som derfor læres bort til nye medlemmer som den rette måten å oppfatte, tenke og føle på i relasjonen til disse problemene*» (Schein, 2010, s.18). Henning Bang (2020, s.23) oppsummerer definisjonene til Schein (2010), Deal & Kennedy (1982) samt Carlsson (1984) og konkluderer med at «*organisasjonskultur er de sett av felles verdier, normer og virkelighetsoppfatninger som utvikler seg i en organisasjon når medlemmene samhandler med hverandre og omgivelsene, og som kommer til uttrykk i medlemmenes handlinger og holdninger på jobben*».

For å illustrere ulike nivåer av hva en organisasjonskultur består av har Schein (2010) utviklet en modell (figur 2) bestående av *artefakter* (eksempelvis observerbare objekter, strukturer, prosesser samt oppførsler), *verdier og normer* (eksempelvis idealer, holdninger, mål, aspirasjoner og skriftlige strategier) og *grunnleggende antakelser* (Schein & Schein, 2017). Grunnleggende antakelser er det som «tas for gitt» og dermed også vanskeligst å endre, spesielt uten stor motstand, ifølge Schein (Kongsvik et al., 2018). Eksempler på grunnleggende antakelser kan være overenstemmighet rundt svar på spørsmål som om organisasjonen skal fokusere på fortid, nåtid eller fremtid, hvorvidt mennesker er grunnleggende «late» og om menneskers handlinger er styrt av følelser eller rasjonelle (Jacobsen & Thorsvik, 2021). Innsikt i en organisasjons grunnleggende antakelser ville krevd integrering i organisasjonen over lengre tid og anses derfor ikke som hensiktsmessig for denne studien (Schein & Schein, 2017). Edwards et al., (2013) formidler at en rekke teorier og perspektiver rundt sikkerhetskultur har sin opprinnelse i organisasjonsteori. Det har følgelig vært hensiktsmessig å benytte denne forskningen som del av bakgrunnen for den videre oppgaven. Med dette bakteppet skal vi se nærmere på sikkerhetskultur og informasjonssikkerhetskultur.



Figur 2 Kulturnivåer i en organisasjonskultur. Hentet fra Flakstad (2019)

2.2 Sikkerhetskultur og informasjonssikkerhetskultur

Når organisasjoner gjennomfører aktiviteter og utfører handlinger oppstår det ulike former for risiko som håndteres av organisasjonene. Ulike teorier byr på ulike tilnærming til hvordan man mest hensiktsmessig kan håndtere risiko og usikkerhet i organisasjoner (Cooper, 2001). Jeg vil innledningsvis kort redegjøre for tre teorier med påvirkning på forskningen innen sikkerhet og sikkerhetskultur for å vise noe av bakteppe for dagens forskning før vi ser på begrepet sikkerhetskultur.

En av de toneangivende forskerne som har hatt innflytelse på dagens forskning om sikkerhetskultur er Barry Turner. I 1978 publiserte han teorien Man-Made Disaster basert på doktorgraden han leverte om samme tema i 1976. Som bakgrunn hadde Turner gjennomført en komparativ studie av ulykkessekvenser i storulykker. I teorien beskriver Turner (1978) hvordan kultur kan være et premiss for systemers sårbarhet og følgelig øke risikoen for ulykker. Turner hever at antagelser og normer kan styre organisasjonens kollektive oppmerksomhet og dermed også ansattes adferd relatert til risiko og sikkerhet. Følgelig kan det oppstå misoppfatninger og et avvik mellom antakelser og faktiske hendelser. Dette kan

kumulere i en kulturell blindhet for farer og trusler (Turner & Pidgeon, 1997). I tillegg til Turner var også forskerne Roberts, La Porte og Weick tidlig ute med å studere sikkerhet og risiko i sammenheng med kultur. De lanserte teorien *High Reliability Organisations* hvor fokuset var på å undersøke og forklare organisasjoner som til tross for deres kompleksitet og tette koblinger unngikk storulykker (Antonsen 2009). Charles Perrow presenterte teorien Normal Accident Theroy og hevder gjennom den at i komplekse, tett-koblede systemer er ulykker et uunngåelig resultat av uforutsette inter-systemiske samspill, noe som antyder at selv om risikoer kan reduseres, kan de ikke helt elimineres på grunn av slike systemers iboende natur (Perrow, 2011). Han stiller seg kritisk til teorien om sikkerhetskultur fordi han mener det fokuseres for lite på betydningen av eksempelvis økt tempo i produksjonen for å øke effektiviteten. Perrow påpeker at bedriftsledere må avveie kostnadene med å utvikle en sikkerhetskultur som kan være betraktelige, mot kravet om økonomisk lønnsomhet for virksomheten. Et eksempel som Perrow benytter er Challengerulykken hvor lederne prioriterte effektivitet høyere enn sikkerhet, noe som fikk katastrofale konsekvenser (Perrow, 2011). Fagpersonene så her bort fra enkelte sikkerhetsprosedyrer og opplevde dette som en akseptabel risiko under oppskytingen. Det Perrow (ibid) kritiserer er et manglende fokus på ledernes makt i analyse av sikkerhetskultur. Eksempelvis utvikler ledere og medarbeidere sikkerhetskulturen sammen, med lederne er i posisjon til å sette premissene for kulturen. Antonsen (2009) belyser også at ledere med makt kan midlertidig endre adferden til medarbeidere, men ikke nødvendigvis deres normer, verdier og grunnleggende antagelser. Spørsmålet blir da om man da snakker om en reel kulturell endring eller en midlertidig tilpasning.

2.3 Sikkerhetskultur og informasjonssikkerhetskultur

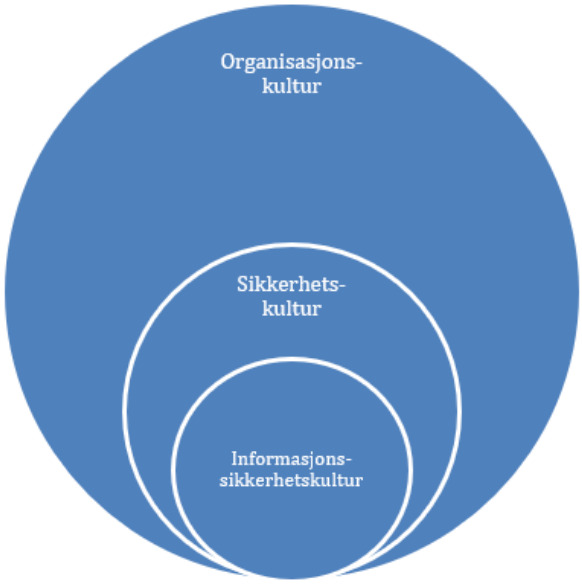
Sikkerhetskultur som begrep fikk et økt fokus etter Challenger og Tsjernobyl-ulykkene i 1986. I ettkant av ulykkene har svak sikkerhetskultur blitt pekt på som påvirkende årsak bak ulykkene. Etterforskningen av Tsjernobyl-ulykken pekte spesielt på brudd på prosedyrer som en av hovedårsakene (Antonsen, 2009; Cox & Flin, 1998). Sikkerhetskultur har også blitt brukt som forklaringsfaktor i granskninger av ulykker som Piper Aplha, Kings Cross og Columbia (Antonsen, 2009).

Med økende interesse for sikkerhetskultur, dukker det parallelt opp et behov for å definere begrepet og flere definisjoner av sikkerhetskultur har blitt foreslått. Eksempelvis ser Kongsvik, et.al. (2018) til Bang (2020) sin definisjonen av organisasjonskultur og definerer sikkerhetskultur som «de sett av felles verdier, normer og virkelighetsoppfatninger relatert til

sikkerhet som utvikler seg i en organisasjon når medlemmene samhandler med hverandre og omgivelsene» (Kongsvik et al., 2018, s. 222). En annen definisjon fra James Reason som er blant de mest gjengitte forskerne innen sikkerhetskultur er:

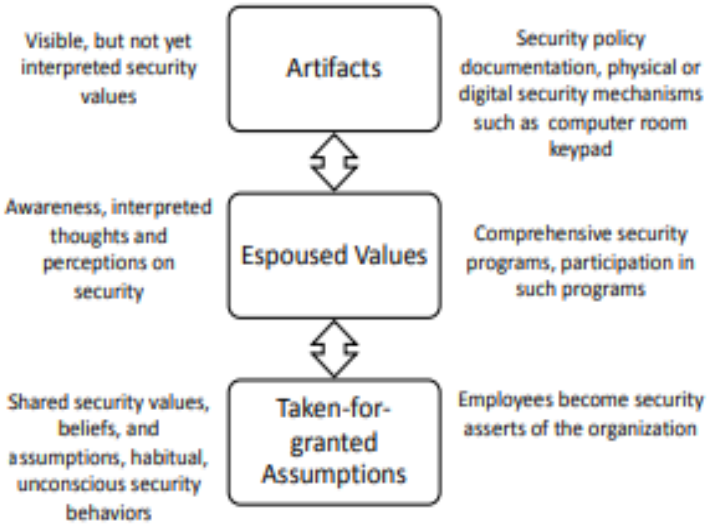
*«…summen av individenes og gruppens verdier, holdninger, kompetanse og atferdsmønstre som viser deres forpliktelse og ferdigheter til å følge organisasjonens helse- og sikkerhetsprogrammer. Organisasjoner med god sikkerhetskultur kjennetegnes av en kommunikasjon bygget på gjensidig tillit, delt oppfatning av sikkerhetsbegrepet og en tiltro til effekten av forebyggende tiltak». (*Reason, 1997, s. 194*).*

Flere hevder at sikkerhetskultur er den delen av organisasjonskultur som er relatert til sikkerhet (Karlsen, 2004). På samme måte kan informasjonssikkerhetskultur beskrives som den delen av sikkerhetskulturen som er relatert til informasjonssikkerhet. Da Veiga (2018) beskriver informasjonsskilter som en subkultur av organisasjonskultur. Dette kan illustreres som vist i figur 3. Videre hevder Da Vega (ibid) at informasjonssikkerhetskulturen i en organisasjon enten kan bidra til beskyttelse av informasjon eller introdusere en risiko. Hvis alle organisasjoner har en informasjonssikkerhetskultur blir da spørsmålet om den er god eller dårlig, altså om den bidrar til å beskytte informasjon eller om den introduserer en risiko. Derfor har denne studien inkludert *forbedring* i problemstillingen.



Figur 3 Informasjonssikkerhetskultur som en del av sikkerhetskulturen, som igjen er en del av organisasjonskulturen (egenprodusert modell)

For å illustrere de ulike nivåene av informasjonssikkerhetskultur bygger Chen et al. (2015) på Schein sin inndeling av kultur (som illustrert i figur 2) og viser til konkrete elementer innen informasjonssikkerhetskultur vi finner i de ulike kulturlagene. Dette er også en tilnærming Da Veiga (2018) støtter.



Figur 4 Chen et al. (2015) sin inndeling av kulturnivåer for informasjonssikkerhetskultur.

For å fostre en god informasjonssikkerhetskultur hevder Van Niekerk & Von Solms (2010) at laget «kunnskap» bør legges til Schein sin inndeling under grunnleggende antakelser. Med kunnskap mener her Van Niekerk & Von Solms nødvendig og underliggende kunnskap om informasjonssikkerhet. De hevder at kunnskap bør være et eget punkt, og ikke et underpunkt i hvert av de andre lagene, fordi denne inndelingen gjør det enklere å tydelig vise effekten kunnskap, eller mangelen av, har på den overordnede sikkerhetskulturen (Van Niekerk & Von Solms, 2010). En ytterligere grunn for dette er at det ikke kan antas at ansatte har tilstrekkelig med kunnskap om informasjonssikkerhet på samme måte som man går utfra at ansatte har nok kunnskap til å utføre de dagligdagse arbeidsoppgavene sine. For å sikre et tilstrekkelig nivå av kunnskap blant ansatte henviser Van Niekerk & Von Solms (ibid) til ISO 27001-standarden som anbefaler bruk av bevisstgjøringskamapanjer for informasjonssikkerhet. I tillegg er det ifølge Reason (1997) fire nøkkelkomponenter som er essensielle for organisasjoner som ønsker å bygge en robust sikkerhetskultur. Dette er 1) en rapporterende kultur noe som innebærer at ansatte tør å rapportere feil, nesten-ulykker, og andre hendelser uten frykt for represalier. 2) En rettferdig kultur som sikrer at det er en balanse mellom ansvar og læring. Videre innebærer dette at ansatte blir behandlet rettferdig og at brudd på regler for konsekvenser. 3) En fleksibel kultur innebærer at organisasjoner evner å tilpasse seg endrende omstendigheter, noe vi så er svært aktuelt for arbeid med informasjonssikkerhet i innledningen. 4) En lærende kultur sikrer at organisasjoner jobber med kontinuerlig forbedring av sikkerheten gjennom læring fra erfaringer, både positive og negative. Og i forlengelsen at det iverksettes tiltak basert på læringen.

2.4 Perspektiver på organisasjonskultur og sikkerhetskultur

Med den økende interessen for sikkerhetskultur har spørsmålet om hvordan man kan skape en god sikkerhetskultur steget frem. I tillegg til Reason (1997) har flere forskere undersøkt hvordan man kan skape en sikkerhetskultur (Roughton & Mercurio, 2002, og Hudson, 2007). Å forbedre sikkerhetskultur er et tema som konsulenthus, herunder PwC (2023) og McKinsey (2022), og nasjonale myndighetsorgan som NSM (2020) også er opptatt av. Synet på hvorvidt organisasjonskultur og sikkerhetskultur lar seg forme er likevel sprikende. NSM (ibid) fremmer en liste med anbefalte tiltak for å bygge en god sikkerhetskultur. Konsulenthusene tilbyr rammeverk og tjenester som kan måle, implementere og utvikle sikkerhetskultur som en av sine tjenester (PwC, 2023). Forutsetningen er altså at kultur er en variabel som kan måles og endres i en bestemt retning med konkrete tiltak. Dette synet finner vi i ledelseslitteratur (Peters, 1982) og blant akademikere (Hudson, 2007; Westrum, 2004). Imidlertid deler ikke alle akademikere perspektivet om at kultur så enkelt lar seg forme (Guldenmund, 2000; Haukelid, 2008). Hervé Laroche (2018) hevder at «… *kultur er vanskelig å endre og derfor ikke kan benyttes som et styringsverktøy på kort sikt»* og legger til at: *«det er ingen grunn til at sikkerhetskultur skal være et unntak*».

I organisasjonsteorien kan vi oppsummere de to ulike perspektivene i henholdsvis verktøyperspektivet og symbolperspektivet. Perspektivene har sterke knytninger til det som omtales som det instrumentelle og institusjonelle perspektivet samt flere andre perspektiver (Christensen et al., 2021). Disse perspektivene har blitt benyttet av flere i forbindelse med forskning på sikkerhetskultur, eksempelvis Fladeby (2014), Antonsen et al. (2017) og Flakstad (2019). Figur 5 viser hvordan verktøy- og symbolperspektivet kan sammenfatte flere ulike perspektiver fra organisasjons- og sikkerhetskulturforskning. Ved å oppsummere flere perspektiv i to hovedkategorier kan vi søke å gi en bred og i større grad helhetlig forståelse av, og tilnærming til, sikkerhetskultur. Å kombinere egenskaper fra etablerte perspektiver i en pragmatisk tilnærming kan sees i arbeidet til flere forskere. Blant andre har Edwards et al. (2013), Guldenmund (2010), Antonsen (2009) og Richter & Koch, (2004) benyttet en slik pragmatisk tilnærming.

Figur 5 Illustrasjonen er hentet fra Flakstad (2019)

I denne oppgaven legger jeg til grunn at informasjonssikkerhetskultur er noe man kan styre og lener meg følgelig på verktøyperspektivet. Dette perspektivet støtter ideen om at selv om kultur er kompleks og mangefasettert, er det fortsatt mulig å ta bevisste steg mot å forme en sikkerhetskultur som er robust og tilpasningsdyktig.

3 Metode og gjennomføring av undersøkelsesopplegg

Hensikten med dette kapittelet er å beskrive hvilken metodologi denne oppgaven er bygget på. Jeg har valgt å benytte litteraturstudie som metode for å besvare studiens problemstilling som er: Hva skaper og påvirker informasjonssikkerhetskultur og hvilke tiltak kan føre til forbedring av informasjonssikkerhetskulturen? I dette kapittelet presenterer jeg litteraturstudie som valgt metode ved å initialt beskrive hva metoden innebærer, før jeg går inn på hvordan jeg har operasjonalisert metoden i denne studien.

3.1 Valg av metode

Halvorsen (2008) definerer metode som «læren om de verktøy som kan benyttes for å samle inn informasjon. Det er en systematisk måte å undersøke virkeligheten på og en fremgangsmåte for å komme frem til ny kunnskap». Metode er da et vitenskapelig verktøy som hjelper oss å forstå hvorfor ting er som de er gjennom forskning. I denne studien har jeg valgt en litteraturstudie for å kunne gjennomgå både kvantitativ og kvalitativ forskning innen informasjonssikkerhetskultur. Dette anser jeg som hensiktsmessig for å få ulike perspektiv på forskning som er gjort innen fagfeltet. Denne metoden har gitt meg en bred oversikt over informasjonssikkerhetskultur og empiriske funn som har vært mulig å bearbeide og trekke konklusjoner fra. Som med alle andre metoder har litteraturstudie styrker og svakheter.

3.2 Litteraturstudie som metode

Hart (1998) definerer litteraturstudie som studie av «et utvalg av tilgjengelige dokumenter (både publiserte og upubliserte) om et emne, som inneholder informasjon, ideer, data og bevis skrevet fra et bestemt ståsted for å oppfylle bestemte mål eller uttrykke visse synspunkter om emnete og hvordan det skal undersøkes samt effektiv evaluering av utvalgte dokumenter relatert til den foreslåtte forskningen.». Hart (ibid) stiller videre følgende krav til litteraturstudier. De skal ha tilstrekkelig dybde og brede, være grundig, konsistent, klar og konsis, samt ha en hensiktsmessig analyse og syntese. Aveyard (2014) beskriver litteraturstudier i noe kortere ordlag som «en omfattende studie og tolkning av litteratur relatert til et bestemt emne». Oppsummerer vi de to definisjonene kan vi si at en litteraturstudie skal være en studie som gir et logisk argument basert på inngående kunnskap om et emne gjennom en overbevisende avhandling. Samtidig skal det være foretatt et utvalg og en evaluering av dokumenter om valgt emne basert på dokumentenes innhold og relevans.

For å oppnå dette kreves en systematisk gjennomgang, hvor man analyserer og sammenfatter tilgjengelig forskning om et valgt tema for å besvare en definert problemstilling. Da er det avgjørende å identifisere litteraturens hovedpoenger og konklusjoner. Ved å bruke litteraturstudie kan man innhente relevant data, uten selv å måtte utføre en empirisk studie. En klar fordel ved en slik studie er at jeg kan benytte store mengder allerede innhentet data. Dette er svært tidsbesparende. Samtidig er bearbeidelse av tidligere funn og identifisere gjennomgående antakelser om et tema er samtidig i seg selv en tidkrevende prosess.

Litteraturstudier kan ifølge Hart (1998) benyttes til ulike formål. Eksempelvis kan litteraturstudie brukes for å besvare forhåndsformulerte spørsmål, noe jeg har lagt opp til med denne oppgaven. Aveyard (2014) beskriver meta-analyse som en fremgangsmåte innen litteraturstudier hvor man kan analysere hva litteraturen sier om et valgt emne gjennom å presentere funn i statistikk eller tabeller. I denne oppgaven oppsummerer jeg kvantitativt funn fra litteraturen i to tabeller, en for definisjoner og en for faktorer. Med dette ønsker å jeg å tilby en klar og strukturert oversikt over de ulike definisjonene og faktorene som påvirker informasjonssikkerhetskultur.

For å sikre kravet til bredde vil jeg gå bredt ut i søkeprosessen, for senere å snevre inn. For å tilfredsstille kravet om dybde i analysen vil jeg prioritere litteratur av høy akademisk standard. Det er essensielt at slik litteratur oppfyller kriteriene for validitet og reliabilitet; det vil si at publikasjonene nøyaktig representerer det de hevder, og at de ikke har målefeil eller andre aspekter som kan underminere troverdigheten. En svakhet ved litteraturstudie er at jeg ikke har førstehåndskjennskap til studiene. For å styrke kredibiliteten til dokumentasjonsunderlaget for denne studien vil jeg kreve at litteraturen er fagfellevurdert.

For å sikre en konsistent analyse benytter jeg forskningsspørsmålene konsekvent i gjennomgangen av inkludert litteratur. I det påfølgende delkapittelet vil jeg presentere operasjonaliseringen av de nevnte tiltakene.

3.3 Operasjonalisering

For å finne og avgrense litteratur som er relevant for studien i henhold til litteraturstudie som metode, stiller jeg krav til litteraturen i form av inklusjons- og eksklusjonskriterier. Dette gjøres konkret ved å utarbeide klare og definerte kriterier. Dette bidrar til å sikre at studier som inkluderes i oppgaven ikke er utenfor problemstillingen.

For å få bredde i tilfanget av litteratur har jeg benyttet ulike formuleringer og kombinasjoner av informasjonssikkerhetskultur. Litteraturen i denne studien er begrenset til nyere studier.

Studier som er eldre enn år 2003 er derfor ekskludert. Valget er gjort da jeg ønsker å forske på nyere studier. I tillegg var det først på starten av 2000-tallet at forskning begynte å vise sammenhengen mellom sikkerhetskulturen i virksomheter og deres evne til å opprettholde høye sikkerhetsnivåer i informasjonssystemene som disse benytter (Reegård et al., 2019). Det er altså først på starten av 2000-tallet at begrepene informasjonssikkerhets- og cybersikkerhetskultur for alvor vokser frem. Videre kreves det at forskningen er fagfellevurdert. Dette bidrar, men er ikke eneste faktor, til å sikre at forskningen holder av høy akademisk standard. Til slutt er oppgaven begrenset til studier som er skrevet på engelsk norsk, svensk eller dansk. Studier på andre språk ville tatt uhensiktsmessig lang tid å gjennomgå. Kriterier er samlet i følgende liste som beskriver inklusjons- og eksklusjonskriterier.

Tabell 2 Inklusjons- og eksklusjonskriterier

Inklusjonskriterier	Eksklusjonskriterier
Publisert litteratur fra 2003 til 2023 (20år)	Publisert litteratur før år 2003
Nøkkelord i artikkel må inneholde begrepene: Informasjonssikkerhetskultur eller cybersikkerhetskultur eller Cyber sikkerhetskultur" eller "Information Security culture" eller "cybersecurity culture" eller "Cyber security culture") og (Organizational eller Organisational) og culture	Artikler som ikke inneholder nøkkelord: Informasjonssikkerhetskultur eller cybersikkerhetskultur eller Cyber sikkerhetskultur" eller "Information Security culture" eller "cybersecurity culture" eller "Cyber security culture") og (Organizational eller Organisational) og culture
Litteraturspråk: engelsk, norsk, svensk og dansk	Litteraturspråk som ikke er engelsk, norsk, svensk og dansk
Publiserte artikler skal være peer-review som er kvalitetssikret og fagfellevurdert	Artikler som ikke er peer-review og dermed ikke er fagfellevurdert. Artikler som er knyttet til en spesifikk hendelse i et spesifikt land (kan eventuelt inkluderes, men vurderes kritisk)

Et annet grep jeg har gjort for å sikre bredde i tilfanget av litteratur er å søke i ulike databaser. Disse er som følger:

Oria er en søketjeneste som muliggjør innhenting av elektroniske materialer fra flere fag- og forskningsbiblioteker i Norge, I denne studien har jeg benyttet Oria som en av fire databasene for litteratursøk. Jeg benyttet denne databasen for å kunne oppnå en relativt stor mengde treff. Orias funksjon «avansert søk» ga samtidig mulighet for å avgrense søk på litteratur til oppgavens forskningsområde.

Web of Science hevder selv å være verdens ledende vitenskapelige søkeplattform for siteringer og analytisk informasjon. Den brukes både som et forskningsverktøy som støtter et bredt spekter av vitenskapelige oppgaver innen forskjellige kunnskapsområder, akademiske disipliner, samt som et datasett for store dataintensive studier.

BASE er en av verdens mest omfattende søkemotorer, spesielt for akademiske nettressurser. BASE gir tilgang til mer enn 340 millioner dokumenter fra mer enn 11,000 innholdsleverandører. BASE drives av Bielefeld University Library og har flere verktøy og tjenester for brukere, databaser og arkivforvaltere.

Google Scholar er en elektronisk spesialisert søkemotor som gir tilgang til akademisk litteratur på tvers av mange ulike fagdisipliner. Søk i Google Scholar gir muligheten til innhenting av blant annet artikler, journaler, akademiske bøker, konferansepapirer, avhandlinger og rapporter. Søkemotoren indekserer fulltekst eller metadata for akademisk litteratur innen de fleste typer formater og på tvers av disipliner.

3.4 Pilotsøk

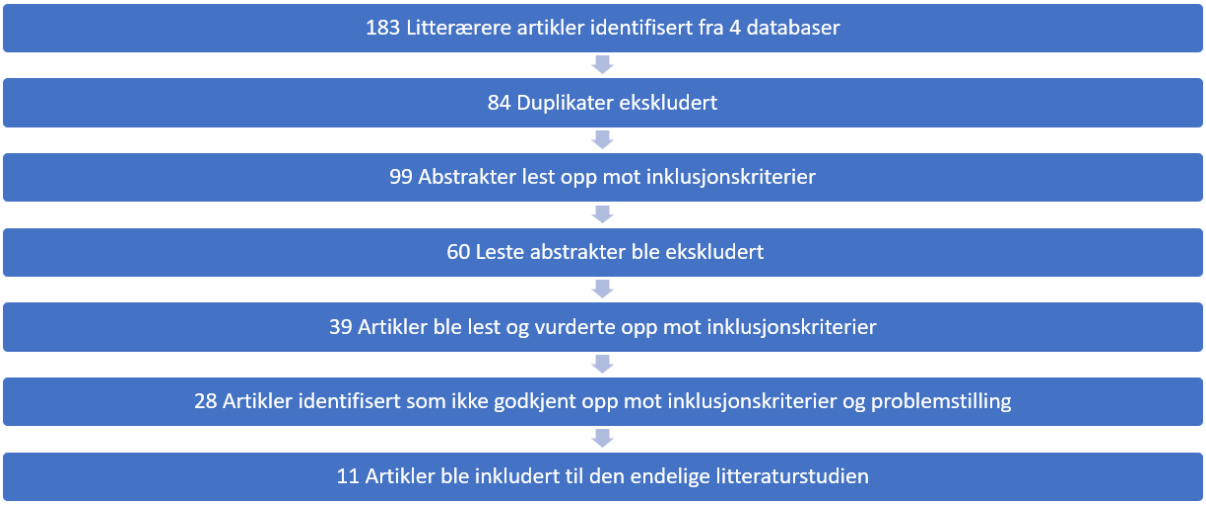
Ridley (2012) argumenterer for å anvende god tid i forberedelsene til litteratursøk slik at man er kjent med muligheter og begrensninger. I gode forberedelser ligger det også å bli godt kjent med verktøy og databaser man skal bruke i litteratursøk, noe som er essensielt for å lykkes med litteraturstudier. Ved å utforske Oria i september 2023 lærte jeg meg hvordan å formulere søk som gav hensiktsmessige treff. Dette dannet grunnlaget for å kunne få tilfredsstillende brede i søkene, samtidig som jeg kunne effektivt og hensiktsmessig avgrense resultatene.

3.5 Flytskjema

Jeg vil i det følgende beskrive hvordan jeg gikk frem i innsamlingen og utvelgelsen av litteratur til denne studien. Først utfyllende med tekst og dernest illustrert ved et flytskjema

ofte referert til som et PRISMA-diagram. Hovedformålet med et slikt diagram er å gi en oversikt over prosessen som ledet til de utvelgelse av artikler inkludert i denne studien (Aveyard, 2014).

Totalt identifiserte jeg 183 artikler i de ulike databasene etter søk med inklusjonskriteriene. Ved gjennomgang av artiklene fant jeg at 84 var duplikater og ekskluderte følgelig disse. Jeg leste så gjennom tittel, nøkkelord og abstrakt på resterende 99 artikler. Etter denne gjennomgangen ekskluderte jeg videre 60 artikler som ble vurdert ikke relevant for studien i henhold til valgt problemstilling og forskningsspørsmål. Deretter leste jeg 39 artikler og endte med 11 artikler som ble vurdert både relevante for problemstilling og forskningsspørsmål samt at de ikke helt eller delvis oppfylte enkelte av eksklusjonskriteriene. Det er disse 11 artiklene som er benyttet som grunnlag for studiens utvalgte empiri og drøfting. Artikler som ble ekskludert i siste runde ble ekskludert da de kvalitativt ble vurdert opp mot problemstilling og relevans for forskningsspørsmålene.



Figur 6 Flytskjema

3.5.1 Eksempler på artikler som er inkludert og ekskludert:

Artikler som ble ekskludert i siste gjennomgang inkluderer Tang et al. (2016) grunnet dens fokus på organisasjonskulturs effekt på informasjonssikkerhetskultur og at case studie bare fokuserte på en bedrift i ett land. Aldulaimi et al. (2023) ble ekskludert grunnet lav kvalitet og artikkelens fokus på kun to land. Alshaikh (2020) ble eksludert grunnet fokus kun i Australia. Her vurderte jeg å inkludere artikkelen ettersom den undersøkte tre ulike selskap i landet, men den havnet etter en totalvurdering av relevans til problemstillingen utenfor. Dhillon et al. (2016) ble ekskludert grunnet artikkelens fokus på sammenslåing av selskap.

Et eksempel på en artikkel som ble inkludert er Da Veiga og Martins (2015) sin case-studie av en internasjonal finansinstitusjon der en information security culture assessment (ISCA) ble gjennomført ved fire intervaller over en periode på åtte år, over 12 land. Artikkelen ble vurdert relevant ettersom den inkluderte 12 land og en lengre tidsperiode i tillegg til at faktorer som påvirker informasjonssikkerhetskultur var en sentral del studien. En annen artikkel som ble inkludert er Da Veiga et al. (2020) som også fokuserer på kjernen i denne studien, nemlig definisjoner av informasjonssikkerhetskultur og hvilke faktorer som påvirker denne. Dette har artikkelen gjort gjennom å se både til teorier i akademia og praktisk bruk hos selskaper.

3.6 Dataens gyldighet og pålitelighet

Studiens forskningsdesign har konsekvenser for undersøkelsenes validitet (Jacobsen, 2016). For å sikre oppgavens validitet må empirien, altså artiklene som samles inn, være gyldige og relevante. Ettersom jeg har valgt litteraturstudie vil jeg ikke ha førstehåndskunnskap om forskningsdataene. Dette resulterer i en risiko for at litteraturen i tilstrekkelig grad besvarer valgt problemstilling. Hadde man valgt et design hvor jeg kunne velge informanter og formulert spørsmål selv kunne jeg spisset disse til å besvare problemstillingen mer konkret. På den andre siden hadde jeg da ikke fått tilgang til samme mengde datamateriale som en litteraturstudie gir. Jeg har derfor søkt å velge ut artikler som i størst mulig grad besvarer oppgavens to forskningsspørsmål, noe som vil øke studiens validitet (Jacobsen, 2016). Som nevnt har jeg også kun valgt artikler som er fagfellevurdert. Dette vil øke oppgavens relabilitet. Jeg har også listet opp antall siteringer for utvalgte artikler som en del av kvalitetssikringen. Med unntak av Arbanas et al. (2021), som bare er sitert 2 ganger, vurderes artiklene å være tilstrekkelig sitert.

I oppgavens empiri-kapittel har jeg samlet funn i tabeller. Dette muliggjøre at andre kan gjennomgå samme litteratur og etterprøve funnene i studien. Det er likevel på sin plass å påpeke litteraturstudiens svakheter. Jeg har eksempelvis oversatt faktorene noe som medfører en mulighet for at andre kan oversette og slå sammen faktorer annerledes enn hva jeg har gjort. Videre kan jeg i valg av søkeord utelatt treff som hadde resultert i flere relevante funn. Jeg har heller ikke i denne litteraturstudien gjennomført en snøballsøk, noe som kunne gitt flere relevante artikler. Jeg kan også ha mistolket informasjon som er relevant for studien. Ved å begrense studien til kun å inkludere fagfellevurderte artikler, kan det ha medført at jeg har oversett annen relevant forskning som er publisert, slik som doktorgradsavhandlinger.

De fleste av de identifiserte artiklene forsøker å løse forskjellige problemer, og de er dermed ikke er direkte sammenlignbare, ettersom de ikke inneholder de samme faktorene. Dette er et problem også Abranas et al. (2021) hadde for sin litteraturstudie. Det er likevel ikke slik at om artiklene har ulikt fokus så kan de ikke brukes. Tematikken informasjonssikkerhetskultur er gjennomgående, og hensikten med denne oppgaven er nettopp å se på spennet for å kunne sammenfatte flere perspektiv på informasjonssikkerhetskultur. Det vurderes derfor som at denne problemstillingen ikke i for stor grad påvirker studiens relabilitet negativt.

Flere av de utvalgte artiklene er skrevet av en forfatter. Da Veiga (2010; 2015; 2018; 2020) er førsteforfatter på tre artikler og eneste forfatter på en fjerde. Det kan være problematisk at en forsker er såpass sterkt representert, men da Da Veiga kun er eneste forsker på en artikkel og ellers samarbeider med andre anser jeg forskningen som gyldig. Det er videre interessant å merke seg vektingen av artikler med forskere tilknyttet Sør-Afrika. Hele 7 av artiklene har overvekt av forskere knyttet til Sør-Afrika selv om Da Veiga et al. (2020) også har en medforfatter knyttet til Russland. Videre er Karlsson og Karlsson knyttet til Sverige, Arbanas et al. (2021) knyttet til Kroatia, Uchendu et al. (2021) og Chen et al. (2015) til USA. Her hadde jeg ideelt sett ønsket en bredere bakgrunn blant forskerne. Det kan være flere grunner til at forskere med tilknytning til Sør-Afrika dominerer utvalget. Eksempelvis kan den Sør-Afrikas nasjonale «Cyber Security Policy Framework (NCPF)» fra 2015 gjenspeile regjeringens prioritet og initiativer som oppmuntrer til forskning i cybersikkerhet, noe som fører til økt publisering på dette området. Forskere fra Sør-Afrika kan også ha en større interesse av å sende inn sine artikler til fagfellevurderte tidsskrifter enn forskere fra andre land. En annen alternativ forklaring kan være knyttet til sårbar infrastruktur, som fører til økt fokus rundt informasjonssikkerhet. Jeg har imidlertid ikke lykkes med å konkludere med hvorfor representasjonen fra Sør-Afrika er så stor i denne studien.

Artiklene er publisert i følgende tidsskrift: *Computers & Security*: 5 artikler, *Information and Computer Security*: 3 artikler, *Computer Fraud & Security*: 1 artikkel, *Aslib Journal of Information Management:* 1 artikkel og *The Journal of Computer Information Systems*: 1 artikkel. Totalt sett vurderer jeg at dette gir en tilfredsstillende variasjon ettersom tidsskriftene kan regnes som anerkjente tidsskrifter og artiklene er fagfellevurdert. Dette kan i noe grad demme opp for Sørafrikansk dominans av forskere.

4 Empiri

Hensikten med denne studien er å belyse hva som skaper og påvirker informasjonssikkerhetskultur og hvilke tiltak som kan føre til forbedring av informasjonssikkerhetskulturen. Forskningsspørsmålene som benyttes omhandler hvordan informasjonssikkerhetskultur defineres, og hvilke faktorer som har størst påvirkning på organisasjoners informasjonssikkerhetskultur. I det følgende vil jeg først oppsummere hvordan artiklene forklarer informasjonssikkerhetskultur med å se på om det presenteres en formell definisjon eller en beskrivelse av informasjonssikkerhetskultur. I oversikten har jeg også inkludert hvor mange siteringer artiklene har ved bruk av Keenious Research Explorer. Dette danner grunnlaget for å besvare forskningsspørsmål 1. Dernest har jeg systematisert alle faktorer som påvirker informasjonssikkerhetskultur som nevnes i artiklene. Dette for å kunne besvare forskningsspørsmål 2. Jeg har valgt å tilstrebe å oversette både definisjoner og faktorer som forskerne benytter. En fare ved å oversette til norsk er at noe av nyansene kan gå tapt og det kan være utfordrende å oversette rett, samt vurdere hvilke faktorer som skal slås sammen. Flere av de engelske begrepene brukes i dagligtale på norsk, eksempelvis «Awareness», «compliance» og «Policy». Jeg har valgt å oversette Awareness med bevisstgjøring og compliance med etterlevelse. Policy i denne sammenheng har vært utfordrende å oversette og er så godt innarbeidet i språket at Språkrådet (u.å) går god for bruken av begrepet. Det er derfor et lite antall faktorer som ikke er oversatt. For å støtte begrunnelsen av å oversette mest mulig tilfører dette oppgaven en bedre flyt og struktur. Samtidig referer jeg til alle oversettelser og faktorer slik at det er mulig å etterprøve oversettelsene.

4.1 Definisjoner og beskrivelser av informasjonssikkerhetskultur

Tabell 3 Oversikt over definisjoner og beskrivelse av informasjonssikerhetskultur

	Definisjoner og beskrivelser av informasjonssikkerhetskultur	Formell definisjon	Beskrivelse	Antall siteringer
1	Arbanas et al. (2021) definerer ikke selv informasjonssikkerhetskultur, men viser til Alhogail & Mirza (2014) og Alnatheer (2014) og påpeker at felles for definisjoner av informasjosnssikekrhetskult er *viktigheten av folks konsistente etterlevese av regler definert i sikkerhetspolicyer* (Arbanas et al., 2021).		X	2

2	Chen et al. (2015) argumenter for at informasjonssikkerhetskultur inkluderer "alle sosio-kulturelle tiltak som støtter tekniske sikkerhetstiltak". Informasjonssikkerhetskultur beskrives som en sub-kultur i organisasjonskulturen hvor målet er økt informasjonssikkerhet. Chen et al (2015) viser til Schein (1999) sin definisjon av organisasjonskultur, som vi så i kapittel 2.1, og sier at om vi bygger på denne definisjonen er informasjonssikkerhetskultur *måten å utføre ting på knyttet til informasjonssikkerhet, inkludert å skape et miljø som fremmer og pleier delte sikkerhetsholdninger, verdier og overbevisninger i en bestemt organisasjon*.	X		72
3	Da Veiga og Eloff (2010) påpeker at informasjonssikkerhetskultur endrer seg over tid men definerer i sin første artikkel informasjonssikkerhetskultur som de *holdninger, antakelser, tro, verdier og kunnskaper som ansatte/interessenter bruker for å samhandle med organisasjonens systemer og prosedyrer på et hvilket som helst tidspunkt. Denne interaksjonen resulterer i akseptabel eller uakseptabel atferd (dvs. hendelser) som blir tydelige i artefakter og kreasjoner som blir en del av måten ting gjøres på i organisasjonen for å beskytte dens informasjonsressurser*.	X		303
4	Da Veiga, & Martins (2015) tilbyr ikke en egen definisjon, men starter med å referer til Information Security Forum (2000) sin definisjon. Videre henviser de til Schlienger og Teufel (2002) som understreker at fokusområdene i informasjonssikkerhetskultur er *artefakter og kreasjoner; kollektive verdier, normer og kunnskap; samt grunnleggende antakelser og tro*. Dette oppsummerer De Veiga og Martins (2015) med å si at informasjonssikkerhetskultur innebærer grunnleggende antakelser knytte til beskyttelse av all informasjon uavhengig av format. Videre hvilke kunnskap ansatte har om informasjonssikkerhet og deres holdninger til etterlevelse av policyer, kontroller og generelt hvordan de håndterer informasjon. Avslutningsvis konkluderer artikkelen med å henvise til Da Veiga & Eloff (2010) sin definisjon som beskrevet ovenfor.		X	78
5	Da Veiga (2018) tilbyr ikke en egen formell definisjon, men en sterk eller positiv informasjonssikkerhetskultur beskrives som *når informasjon blir beskyttet gjennom hele det livsløp og ved alle anledninger hvor ansatte interagerer med informasjonen og hvor ansatte har en felles forståelse av å beskytte informasjonen i tråd med organisasjonens informasjonssikkerhetspolicy*. Også denne artikkelen refererer til Da Veiga & Eloff (2010) som den definisjonen artikkelen tar utgangspunkt i.		X	16
6	Da Veiga et al. (2020) har i denne artikkelen gjennomført en litteraturstudie hvor de blant annet har sett på definisjoner av informasjonssikkerhetskultur. De konkluderer	X		47

	studien med følgende definisjon*: Informasjonssikkerhetskultur er kontekstualisert til menneskers oppførsel i en organisatorisk sammenheng for å beskytte informasjon behandlet av organisasjonen gjennom etterlevelse av informasjonssikkerhetspolicy og -prosedyrer og en forståelse av hvordan man implementerer krav på en forsiktig og oppmerksom måte som innarbeides gjennom regelmessig kommunikasjon, bevisstgjøring, opplæring og utdanningsinitiativer. Adferden blir over tid en del av måten ting gjøres på, det vil si, en naturlig atferd, som et resultat av ansattes antagelser, verdier og tro, deres kunnskap og holdning til og oppfatning av beskyttelse av informasjonsressurser. Informasjonssikkerhetskulturen styres av ledelsens visjon sammen med ledelsesstøtte i tråd med informasjonssikkerhetspolicyen og påvirkes gjennom interne og eksterne faktorer, støttet av et adekvat IKT-miljø, synlig i organisasjonens artefakter og oppførsel vist av ansatte, og skaper dermed et miljø av tillit hos interessenter og etablerer integritet.*		
7	Karlsson og Karlsson (2015) presenterer ikke en formell definisjon av informasjonssikkerhetskultur, men konkluderer med at til tross for at forskere har definert informasjonssikkerhetskultur på litt forskjellige måter av (Dhillon 1997; Da Viega og Eloff 2010; Ilvonen 2011; Schlienger og Teufel 2002), synes det å være en felles forståelse av at det består av et *delt mønster av verdier, mentale modeller og aktiviteter som blir utvekslet blant en organisasjons ansatte over tid, noe som påvirker informasjonssikkerheten*. Studien peker videre ikke direkte på faktorer for informasjonssikkerhetskultur, men er interessant ettersom den gjør en omfattende studie av hva informasjonssikkerhetskultur er som 1 av 4 meta spørsmål.	X	50
8	Nel og Drevin (2019) presenterer ingen definisjon av informasjonssikkerhetskultur, men fremhever at organisasjoner kan redusere sikkerhetsrisiko gjennom å kultivere en informasjonssikkerhets opplyst kultur. Gjennom trening og utdanning kan organisasjoner øke istandsette ansatte til å etterleve policyer innen informasjonssikkerhet. Når det blir naturlig for ansattes å beskytte informasjon ubevist i deres daglige gjøremål kan organisasjoner integrer informasjonssikkerhet i organisasjonskulturen hevder Nel og Drevin (2019).	X	17
9	Thomson et al. (2006) presenterer ikke en egen formell definisjon av informasjonssikkerhetskultur, men bygger artikkelen på Schein (1999) sin definisjon av organisasjonskultur og sier at siden den påvirker ansattes handlinger bør den styres mot å styrke ansattes handlinger innen informasjonssikkerhet. Et annen beslektet	X	139

	begrep de henviser til i artikkelen er «informasjonssikkerhetslydighet» som de definerer som «brukeres de facto oppførsel relatert til etterlevelse av toppledelsens visjoner som definert i organisasjonens informasjonssikkerhetspolicy. Artikkelens fokus er hovedsakelig på hvordan å endre organisasjonskultur, men benevner likevel et par faktorer som er relevant for å forbedre informasjonssikkerhetskultur.		
10	Uchendu et al. (2021) skiller seg ut ved at artikkelen bruker begrepet cyber sikkerhetskultur og tilbyr således ikke en definisjon av informasjonssikkerhetskultur. Det er likevel interessant å se hva artikkelen i lys av valgt begrep i denne oppgaven. Uchendu et al. (2021) analyserer 58 ulike artikler innen informasjonssikkerhetskultur og cyber sikkerhetskultur og konkluderer med at det er klare paralleller mellom definisjoner av kultur for cybersikkerhet og informasjonssikkerhet. Det er også et klart forhold mellom cybersikkerhet og definisjoner av organisasjonskultur. Til tross for disse parallellene, finnes det ingen omforent beskrivelse.	X	21
11	Van Niekerk & Von Solms (2010) tilbyr ikke en formell definisjon av informasjonssikkerhetskultur, men bygger videre på Schein (1999) sin definisjon av organisasjonskultur, nemlig «måten vi gjør ting på her». Da artikkelen advarer mot å forenkle konseptet i for stor grad bygger den videre på Schein sin inndeling av organisasjonskultur i artefakter, verdier og normer og grunnleggende antakelser og legger til kunnskap som et fjerde nivå under grunnleggende antakelser. Dette ettersom de argumenter for at kunnskap, eller mangel på kunnskap, påvirker informasjonssikkerhetskultur. Med fare for at overtolke Van Niekerk & Von Solms kan man si at artikkelen ligger tett på å forklare informasjonssikkerhetskultur som måten vi gjør ting på her, knyttet til informasjonssikkerhet, basert på kunnskapen vi har om emnet.	X	220

4.1.1 Oppsummering av definisjoner og beskrivelser

I tre av de gjennomgåtte artiklene blir det presentert en formell definisjon Da Veiga og Eloff (2010), Chen et al. (2015) og Da Veiga et al. (2020), mens resterende ikke presenterer en egen definisjon. Det er nyanseforskjeller i definisjonene og enkelte hevder at det ikke finnes én allment akseptert og omforent definisjon. Likevel viser artiklene samlet sett at det er en bred enighet om at informasjonssikkerhetskultur involverer holdninger, verdier, kunnskap og oppførsel relatert til beskyttelse av informasjon innenfor en organisatorisk ramme.

4.2 Identifiserte faktorer for informasjonssikkerhetskultur

Under er faktorer som har blitt identifisert i artiklene samlet i en tabell. Denne viser hvilke faktorer som nevnes, hvilke artikler som nevner faktorene og aggregert hvor mange ganger faktorene nevnes totalt.

Tabell 4 Oversikt over faktorer

Faktorer	Totalt	Artikler som belyser faktorene
Trening	7	Arbanas et al. (2021) Chen et al. (2015) Da Veiga (2018) Thomson et al. (2006) Uchendu et al. (2021) Da Veiga et al. (2020) Nel og Drevin (2019)
Utdanning/kunnskap	9	Arbanas et al. (2021) Chen et al. (2015) Da Veiga og Eloff (2010) Da Veiga 2018 Van Niekerk & Von Solms (2010) Thomson et al. (2006) Uchendu et al. (2021) Da Veiga et al. (2020) Nel og Drevin (2019)
Policyer, retningslinjer og prosedyrer	8	Arbanas et al. (2021) Chen et al. (2015) Da Veiga (2018) Da Veiga og Eloff (2010) Thomson et al. (2006) Uchendu et al. (2021) Da Veiga et al. (2020) Nel og Drevin (2019)
Ledelsesstøtte	6	Arbanas et al. (2021) Da Veiga og Eloff (2010) Da Veiga (2018)

		Thomson et al. (2006) Uchendu et al (2021) Nel og Drevin (2019)
Bevisstgjøring.	7	Arbanas et al (2021) Chen et al. (2015) Van Niekerk & Von Solms (2010) Thomson et al. (2006) Uchendu et al. (2021) Da Veiga et al. (2020) Nel og Drevin (2019)
Roller og ansvar	3	Arbanas et al. (2021) Uchendu et al. (2021) Nel og Drevin (2019)
Etterlevelse	3	Arbanas et al. (2021) Thomson et al. (2006) Uchendu et al. (2021) Nel og Drevin (2019)
Adferd/Oppførsel, styring av sikkerhetsadferd og belønning straff av denne	3	Arbanas et al. (2021) Da Veiga et al. (2020) Uchendu et al. (2021)
Tillit	4	Arbanas et al. (2021) Da Veiga og Martins (2015) Da Veiga (2018) Da Veiga et al. (2020)
Etikk	3	Arbanas et al. (2021) Uchendu et al. (2021) Nel og Drevin (2019)
Antivirus	1	Arbanas et al. (2021)
Backup	1	Arbanas et al. (2021)
Autentisering og autorisasjon	1	Arbanas et al. (2021)
Sikkerhetsmonitorering	1	Chen et al. (2015) Da Veiga og Eloff (2010)
Egenvurdering	1	Da Veiga (2018)

Teknologi	3	Da Veiga (2018) Da Veiga og Eloff (2010) Da Veiga et al. (2020)
En rapporteringslinje for sikkerhetshendelser	1	Da Veiga (2018)
Endringsledelse	6	Da Veiga (2018) Da Veiga og Martins (2015) Da Veiga og Eloff (2010) Uchendu et al. (2021) Da Veiga et al (2020) Nel og Drevin (2019)
Informasjonsressursforvaltning (brukernes oppfatninger av beskyttelsen av informasjonsressurser)	3	Da Veiga og Martins (2015) Da Veiga (2018) Nel og Drevin (2019)
Sikkerhetsrisikoer	3	Uchendu et al. (2021) Da Veiga et al. (2020) Nel og Drevin (2019)
Nasjonal kultur	2	Uchendu et al. (2021) Da Veiga et al. (2020)
Politiske og juridiske faktorer	2	Da Veiga et al. (2020) Nel og Drevin (2019)
Økonomiske faktorer	1	Da Veiga et al. (2020)
Sosio-kulturelle faktorer	2	Chen et al. (2015) Da Veiga et al. (2020)
Organisasjonens indre tilstand	1	Da Veiga et al. (2020)
Organisasjonens livssyklustilstand	1	Da Veiga et al. (2020)
Nivået på den overordnede organisasjonskulturen	1	Da Veiga et al. (2020)
Systembeskyttelse for informasjon	1	Da Veiga et al. (2020)
Ressurser	1	Da Veiga et al. (2020)

Ledelse	1	Da Veiga et al. (2020)
Operativ ledelse	1	Da Veiga et al. (2020)
(menneskelige) Personlighet og verdier	1	Da Veiga et al. (2020)
(menneskelige) Behov	2	Da Veiga et al. (2020) Nel og Drevin (2019)
(menneskelig) emosjonell tilstand	1	Da Veiga et al. (2020)
Forpliktelse	1	Uchendu et al. (2021)
Etablert nettverk av «Security champions»	1	Uchendu et al. (2021)
Internkontroll	1	Nel og Drevin (2019)
Forretningskontinuitetsplanverk	1	Nel og Drevin (2019)
Informasjonssikkerhetsprogram	1	Nel og Drevin (2019)
Kommunikasjon	2	Nel og Drevin (2019) Uchendu et al. (2021)
Strategi	1	Nel og Drevin (2019)
ROI (return on investment)	1	Nel og Drevin (2019)
Rettferdig behandling	1	Nel og Drevin (2019)

4.2.1 Oppsummering faktorer

I de 11 artiklene har jeg identifisert 43 faktorer som påvirker informasjonssikkerhetskultur. Faktorene utdanning/kunnskap (9), policyer, retningslinjer og prosedyrer (8), trening (7), bevisstgjøring (7), endringsledelse (6), ledelsesstøtte (6) og etterlevelse (6) nevnes oftest.

Etter å ha identifisert og kvantifisert faktorene ser vi at det er ulike nivåer på faktorene. Nel og Dreven (2019) deler de inn i 3 nivåer. Nivå 1 betegnes som veldig viktige faktorer, men som ofte er vagt definert. Her plasserer de policyer, etterlevelse samt utdanning og trening. Nivå 2 omtaler de som moderat viktig, men mer detaljert enn nivå 1. På nivå 2 plasserer de eksempelvis endringsledelse, altså organisasjonens evne og vilje til å endre seg, revisjoner for å sikre at man jobber på en hensiktsmessig måte samt kontinuitetsplanverk, altså at

organisasjoner har kriseplaner for å kunne jobbe på alternativer måter dersom en hendelse inntreffer. Nivå 3 omtaler de som «sub-nivåer» og som kan plasseres inn under en av de øvrige nivåene. Her nevner de roller og ansvar, strategi og risikovurderinger som eksempler.

Da Veiga et al. (2020) deler faktorene inn på en noe annerledes måte. De deler opp i eksterne og interne faktorer. Videre skilles de interne faktorene inn i organisatoriske, ledelses- og menneskelige faktorer. De bruker også begreper som personlige faktorer som omhandler individuelle aspekter som kan påvirke en persons atferd og beslutninger knyttet til informasjonssikkerhet. Kulturelle faktorer som de formidler fokuserer på hvordan organisasjonskulturen og sosiale normer innenfor en organisasjon kan påvirke informasjonssikkerhet. Til slutt nevnes også kontekstuelle faktorer som tar for seg eksterne eller miljømessige aspekter som kan ha innflytelse på informasjonssikkerhet i en organisasjon. I kategoriinndelingen til Da Veiga et al. (ibid) kan vi se en viss henvisning til perspektiver på kultur. De eksterne faktorene, som nasjonal kultur, er vanskelig å endre, mens ledelsesfaktorene som utdanning, trening og bevisstgjøring er mulig for ledelsen i en organisasjon å styre. Til tross for at flere av artiklene plasserer utdanning og kunnskap i samme kategori hevder Høiby et al. (2022) at forskningslitteraturen setter klare skiller mellom kunnskap, trening og utdanning. Dette forklares ved at det er en reise fra bevisstgjøring til atferdsendring.

4.3 Oppsummering

I dette kapittelet har jeg kartlagt elementer som påvirker informasjonssikkerhetskulturen i organisasjoner. Sentralt i studien har vært å definere informasjonssikkerhetskultur og identifisere de mest innflytelsesrike faktorene. Gjennom en gjennomgang av relevante artikler, deriblant forskning av Da Veiga og Eloff (2010), Chen et al. (2015), og Da Veiga et al. (2020), har jeg identifisert formelle definisjoner og beskrivelser av informasjonssikkerhetskultur. Til tross for ulikheter i detaljer, er det enighet om at kulturen involverer holdninger, verdier, kunnskap og atferd relatert til informasjonsbeskyttelse. Videre ble det identifisert 43 faktorer som påvirker informasjonssikkerhetskultur, knyttet til ulike nivåer og inndelinger. I det neste kapittelet vil jeg drøfte disse funnene ytterligere, og undersøke hvordan de kan anvendes for å forstå og forbedre informasjonssikkerhetskulturen i ulike organisasjoner.

5 Diskusjon

I dette kapittelet vil jeg drøfte de viktigste funnene fra forrige kapittel i lys av teoriene fra kapittel 2. Formålet med diskusjonen er å sette funnene inn i en bredere kontekst, utforske deres implikasjoner og hva som ligger i faktorene. Denne tilnærmingen har som formål å gi en dypere innsikt og forståelse av informasjonssikkerhetskultur, og hvordan studiens resultater kan bidra til videre forskning på tematikken.

5.1 Definisjoner

Av 11 artikler var det bare 3 som presentere en selvstendig formell definisjon av informasjonssikkerhetskultur, mens de øvrige i ulik grad beskrev begrepet. Jeg vil her primært ta utgangspunkt i de 3 formelle definisjonene som gis og fremheve de likheter og ulikheter som ligger i definisjonene. Dette for å utforske konseptets bredde og dybde. Jeg vil prioritere plass til diskusjon rundt faktorer da definisjonene fremstår, om ikke omforente, så ikke direkte motstridene.

5.1.1 Likheter

Alle tre definisjonene påpeker at informasjonssikkerhetskultur er forankret i organisasjonens måte å gjøre ting på, og at den er tett knyttet til holdninger, verdier og tro. Man ser således knytningene til Schein (1999) sin definisjon av organisasjonskultur. Videre antyder likhetene i definisjonene en felles enighet i at informasjonssikkerhetskulturen ikke bare er en samling av regler og prosedyrer, eller artefakter for å bruke Scheins ord. Det fremstår derfor som informasjonssikkerhetskultur innebærer et dypere, mer innebygd aspekt av organisatorisk atferd og tenkemåte, eller en «annen natur» for å bruke Da Veiga et al. sine ord.

Når Chen et al. (2015) legger vekt på et miljø som fremmer og nærer sikkerhetsholdninger, verdier og overbevisninger antydes det at informasjonssikkerhetskultur ikke begrenser seg til individuelle handlinger, men omfatter et kollektivt handlemønster. Da Veiga og Eloff (2010) utvider dette ved å inkludere de faktiske holdningene, antakelsene, troen, verdiene og kunnskapene som ansatte, og interessenter, bruker i sin interaksjon med organisasjonens systemer og prosedyrer. Da Veiga og Eloff legger da større vekt på de menneskelige aspektene av kulturen, hvordan individuelle overbevisninger og kunnskaper former atferden.

Artikkelen til Da Veiga et al. (2020) går enda ett stegg videre og tilbyr den mest omfattende definisjonen. Her kontekstualiseres informasjonssikkerhetskultur til menneskelig atferd i en organisatorisk sammenheng, og legger vekt på etterlevelse av policyer og prosedyrer, samt

viktigheten av kommunikasjon, bevisstgjøring, opplæring og utdanningsinitiativer. De inkluderer også elementer av både miljø og individuell atferd, samt den overordnede styringen og støtten fra ledelsen. Således fremmes flere faktorer som vi identifiserte i kapittel 4.2 også i definisjonen.

5.1.2 Ulikheter

Til tross for grunnleggende likheter, presenterer definisjonene noe ulike vinklinger og fokuspunkter. Mens Chen et al. (2015) fokuserer på dannelsen av et støttende miljø legger Da Veiga og Eloff (2010) større vekt på de individuelle aspektene, som hvordan ansatte og interessenter personlig oppfatter og engasjerer seg i informasjonssikkerhetspraksiser. Senere forener på et vis Da Veiga et al. (2020) disse aspektene, ved å inkludere både individuell atferd og organisasjonsmessige strukturer og prosesser. Det fremstår samlet sett ikke som at definisjonene er direkte motstridene, men heller har utviklet seg over tid om man ser på det i tidsmessig kronologisk rekkefølge. Det er likevel interessant at kun 3 av studiens 11 artikler presentere en egen definisjon og det kan virke som at det enda ikke foreligger en komplett omforent definisjon av informasjonssikkerhetskultur. Likevel fremstår Da Veiga et al. (2020) sin definisjon som en til å omfavne de aspekter som beskriver informasjonssikkerhetskultur i de andre artiklene.

5.1.3 Kort delkonklusjon

Totalt sett viser de ulike definisjonene og de øvrige artiklers beskrivelse av begrepet at informasjonssikkerhetskultur er et flerdimensjonalt konsept som krever både en individuell og organisatorisk tilnærming. Dette bør organisasjoner som ønsker å forbedre informasjonssikkerhetskultur merke seg.

5.2 Faktorer

Faktorene ble identifisert og kvantifisert i forrige kapittel. At en faktor er identifisert flest ganger i utvalget av artikler gjør den likevel ikke automatisk til den viktigste faktoren i informasjonssikkerhetskultur. Ettersom artiklene har ulikt fokus og kunne det vært aktuelt å fokusere på artiklene til Uchendu et al. (2021), Nel og Drevvin (2019) og Da Veiga et al. (2020) som alle tar for seg sentrale faktorer i informasjonssikkerhetskultur. For å benytte bredden i utvalget av artikler tar jeg likevel utgangspunkt i de faktorer som er nevnt i flest artikler som et utgangspunkt for drøftingen. Av totalt 43 faktorer skilte de 7 faktorene utdanning/kunnskap (9), policyer, retningslinjer og prosedyrer (8) trening (7) bevisstgjøring (7) endringsledelse (6) ledelsesstøtte (6) og etterlevelse (6) seg ut som de mest gjengitte.

Når vi har identifisert faktorer som kan skape og påvirke informasjonssikkerhetskultur, faller det naturlig at det er *tiltak* knyttet til disse faktorene som bør iverksettes for å *forbedre* informasjonssikkerhetskulturen.

Faktoren utdanning/kunnskap henger tett sammen med både trening og bevisstgjøring. Ifølge Høiby et al (2022) er det gode grunner for å dele disse opp. Det er altså ikke bare overføring av informasjon som er viktig, men også hvordan denne kunnskapen påvirker ansattes holdninger og forståelse av sikkerhetsrisikoer. Det er sentralt å også se på hvordan utdanning bidrar til både individuell og kollektiv bevissthet om informasjonssikkerhet. Uchendu et al. (2021) har delt faktorene opp i sikkerhetsbevisstgjøring, sikkerhetstrening og kunnskap. I deres litteraturstudie er sikkerhetsbevisstgjøring nevnt i 24 studier, sikkerhetstrening i 21 studier og kunnskap i 11. Sikkerhetsbevisstgjøring og sikkerhetstrening er identifisert som de viktigste faktorene etter toppledelsens støtte og sikkerhetspolicyer. Det er på sin plass å minne om at artikkelen benytter cybersikkerhetskultur som begrep, men ser samtidig, som denne studien, svært store likhetstrekk med informasjonssikkerhetskultur. Da Veiga et al. (2020) har på sin måte samlet utdanning, trening og bevisstgjøring i en faktor. De plasserer faktoren under kategorien ledelsesfaktorer. Nel og Drevin (2019) har på sin side har gått for en mellomting og definert utdanning og trening i en faktor og informasjonssikkerhetsbevisstgjøring i en annen. Nel og Drevin (ibid) plasserer begge faktorene i nivå 1: veldig viktige faktorer. Basert på at faktorene utdanning, kunnskap trening og bevisstgjøring skiller seg ut i kvantitet i denne undersøkelsen og Uchendu et al. (2021) samt nevnes som en ledelsesfaktor av Da Veiga et al (2020) og som veldig viktige faktorer av Nel og Drevin er det sterke indikatorer på at dette er sentrale faktorer i å bygge en sterk informasjonssikkerhetskultur. Arbanas et al. (2021) poengterer at mange organisasjoner tidligere kun målte antall ansatte som fullførte treningsprogram, indikator på kvaliteten til sikkerhetsopplæringen. Høye gjennomføringsrater viste seg likevel ikke nødvendigvis å bety at ansatte hadde forstått og internalisert organisasjonens sikkerhetspolitikk. Kvaliteten på treningen og hvordan denne gjennomføres har altså en betydning på faktoren.

I faktoren Policy (retningslinjer og prosedyrer) ligger det ifølge Nel og Drevin, (2019) at det finnes en definert policy for informasjonssikkerhetskultur som beskriver alle prosedyrer, standarder, retningslinjer og beste praksiser innen informasjonssikkerhet, og alle ansatte er klar over policyen, dens innhold og hvor de kan finne den. Policy beskrives av Nel og Drevin (ibid) som en nivå 1, veldig viktig, faktor Nel og Drevin og er identifisert som den nest viktigste faktoren for informasjonssikkerhetskultur av Uchendu et al. (2021). Policy for

informasjonssikkerhetskulturen kan sies å danne selve grunnlaget for informasjonssikkerhetskulturen ved å etablere klare forventninger og retningslinjer. Ser vi tilbake til Chen et al. (2015) sin inndeling av kulturnivåer for informasjonssikkerhetskultur illustrert i figur 4 er policy noe som manifesterer seg som en artefakt i en informasjonssikkerhetskultur. Da Veiga et al. (2020) plasserer også Policy som en intern ledelsesfaktor som kan styres. I samme artikkel finner vi også igjen faktoren i selve definisjonen av informasjonssikkerhetskultur, nemlig i «*… gjennom etterlevelse av informasjonssikkerhetspolicy og -prosedyrer*». Et sentralt punkt her som kan påvirke informasjonssikkerhetskulturen negativt er dersom organisasjonen ikke klarer å balansere mellom behovet for av å ha strukturerte policyer og behovet for at disse er fleksible nok til å tilpasses endringer. Vi ser altså at det er flere ting som kan undergrave policy som faktor. Det første adresseres av Nel og Drevin (2019), nemlig at ansatte må kjenne til policyen og vet hvor den finnes. Det neste adresseres både i definisjonen av Da Veiga et al. (2020) og som en egen sentral faktor, følgelig etterlevelse. Dersom policyen ikke *etterleves* virker den ikke å tilføre mye til informasjonssikkerhetskulturen, snarere tvert imot. En Policy som ikke etterleves kan virke negativt på informasjonssikkerhetskulturen. I etterlevelse ligger også disiplinere tiltak for å bryte policyer eller på annen måte ikke etterleve de regler som er satt av organisasjonen. Da Veiga et al. (2020) understreker viktigheten av etterlevelse i sine funn og konkluderer med at faktorene informasjonssikkerhetspolicy, bevisstgjøring og disiplinærtiltak for manglende etterlevelse er de tre viktigste tiltakene som organisasjoner flest har innført for å påvirke informasjonssikkerhetskulturen positivt ifølge deres studier. Av Uchendu et al. (2021) identifiseres etterlevelse som den sjette viktigste faktoren og er definert som en nivå 1, veldig viktig faktor av Nel og Drevin (2019). Sistnevnte beskriver etterlevelse som at det er det er tydelige konsekvenser knyttet til manglende overholdelse av sikkerhetsprotokoller. Ansatte er klar over mulige konsekvenser hvis de ikke følger policyen.

Nel og Dreven (2019) beskriver endringsledelse som moderat viktig for informasjonssikkerhetskultur og plasserer følgelig faktoren som en nivå 2 faktor. De skriver at ansatte bør oppmuntres til å være åpne for endringer i organisasjonen og at ledelsen spiller en sentral rolle ved å vise ansatte på lavere nivå at de omfavner endring. Dette er spesielt viktig i organisasjoner der ansatte avviser sikkerhetstiltak fordi det er «for nytt» for dem (ibid, s.14). Vi så i innledningen til denne studien at det teknologiske landskapet har endret seg drastisk de siste tiårene og det vil stilles stadig nye krav til informasjonssikkerhet. Den greske filosofen Heraklit får fra mange æren av å stå bak sitatet «ingenting er konstant, foruten

endring». Det gir dermed mening at endringsledelse er en sentral faktor i å påvirke og forbedre informasjonssikkerhetskultur. Det er derfor sentralt å se på hvordan organisasjoner håndterer motstand mot endring, spesielt når det gjelder å endre grunnleggende antakelser og atferdsmønstre. Uchendu et al. (2021) påpeker at mangelen på dedikert tid prioritert og ressurser med tilstrekkelig kompetanse på endringsledelse ofte står i veien for å utvikle en sterk informasjonssikkerhetskultur.

I sin studie identifiserte Uchendu et al. (2021) ledelsestøtte som den klart viktigste faktoren i å skape en god sikkerhetskultur. Artikkelen bruker begrepene *støtte fra toppledelse, lederskap eller engasjement* og definerer det som støtten og engasjementet fra ledende direktører, toppledere, avdelingsledere i å skape, praktisere og opprettholde en informasjonssikkerhetskultur (ibid). Da Veiga et al. (2020) samt Nel og Drevin (2019) bruker andre begreper knyttet til ledelse, men alle er tydelige på at tonen for informasjonssikkerhetskulturen settes fra toppen. De deler slikt sett seg synet om at organisasjonskultur og deres subkulturer kan styres. Kultur er dermed ikke «bare» noe som vokser frem, men noe som kan påvirkes. Hvordan lederne forholder seg til informasjonssikkerhet påvirker altså de ansatte.

Av de mest gjengitte faktorene finner vi linker til Reasons (1997) nøkkelkomponenter for en god sikkerhetskultur. Etterlevelse kan knyttes opp mot en rettferdig kultur. Policyer kan knyttes opp mot en fleksibel kultur gitt forutsetningen at organisasjoner klarer å balansere behovet for å ha strukturerte policyer og behovet for at disse er fleksible nok til å tilpasses endringer. En rapporterende kultur kan vi se i faktorene tillitt og rapporteringslinje for hendelser, selv om disse ikke var blant de mest gjengitte. Et interessant funn er at erfaringer eller tilsvarende faktor ikke nevnes som kunne knyttes opp mot en lærende kultur. Det kan argumenteres for at utdanning/kunnskap og bevisstgjøring kan knyttes opp mot komponenten. Selv om utdanning og bevisstgjøringskampanjer kanskje bør inkludere konkrete erfaringer organisasjonen har gjort seg, kom dette ikke eksplisitt frem i funnene.

5.2.1 En alternativ inndeling av faktorer

De 43 faktorene som ble identifisert spenner over et bredt spekter av områder relatert til informasjonssikkerhet, inkludert organisatoriske, tekniske, menneskelige, kulturelle og strategiske aspekter. De varierer betydelig i natur og omfang. Eksempelvis fokuserer faktorene utdanning/kunnskap og bevisstgjøring på menneskelige aspekter, mens antivirus og sikkerhetsmonitorering er mer teknisk orienterte. Nasjonal kultur og til dels politiske og

juridiske faktorer er mer knyttet mot en bredere samfunnsmessig og regulatorisk kontekst. Alle disse faktorene kan påvirke hverandre og bør sees i sammenheng. For eksempel kan politiske og juridiske faktorer styrke eller begrense effektiviteten av en organisasjons interne policyer og prosedyrer knyttet til informasjonssikkerhet. Med det vide tilfanget av faktorer som til dels er overlappende kan det være vanskelig å analysere og kategorisere disse. Det vil også være rom for å diskutere sammenslåing og oppdeling av enkelte faktorer. Likevel mener jeg totalt sett at følgende inndeling av faktorer kan foreslås basert på identifiserte faktorer i denne studien.

Tabell 5 En alternativ inndeling av faktorer – De mest gjengitte faktorene er markert i kursiv

Organisasjon og ledelse	*Ledelsesstøtte, endringsledelse*, organisasjonens indre tilstand, organisasjonens livssyklustilstand, nivået på den overordnede organisasjonskulturen, operativ ledelse, forpliktelse, etablert nettverk av «Security champions», internkontroll, strategi
Menneskelige faktorer	*Trening, utdanning/kunnskap, bevisstgjøring*, roller og ansvar, adferd/oppførsel, styring av sikkerhetsadferd, personlighet og verdier, behov, emosjonell tilstand, tillit, rettferdig behandling
Policyer og prosedyrer	*Policyer, retningslinjer og prosedyrer*, *etterlevelse,* forretningskontinuitetsplanverk, Informasjonssikkerhetsprogram, rapporteringslinje for sikkerhetshendelser, Informasjonsressursforvaltning
Teknologiske faktorer	Antivirus, backup, autentisering og autorisasjon, sikkerhetsmonitorering, teknologi, systembeskyttelse for informasjon
Risiko og sikkerhetsstyring	Sikkerhetsrisikoer, egenvurdering, ressurser, kommunikasjon, ROI (Return on Investment)
Eksterne faktorer	Nasjonal kultur, politiske og juridiske faktorer, økonomiske faktorer, sosio-kulturelle faktorer

5.3 Kort oppsummering

Denne studien har lagt til grunn at organisasjonskultur, og dermed informasjonssikkerhetskultur kan og bør styres gitt den teknologiske virkeligheten vi står ovenfor. Studien har utforsket ulike definisjoner og argumentert for at informasjonssikkerhetskultur kan og bør styrkes gjennom målrettede tiltak oppsummert i syv faktorer. Selv om denne studien begrenset seg til de syv mest sentrale faktorene for informasjonssikkerhetskultur betyr det ikke at resterende faktorer er uvesentlige. En faktor som ingen av artiklene omfattet av denne litteraturstudien tok for seg var kunstig intelligens som trolig vil spille en sentral rolle i sikkerhetsarbeid fremover. Det ble heller ikke identifisert en faktor som spesifikt så på organisasjoners erfaring og hvordan jobbe ut fra disse.

6 Konklusjon

Denne studien har hatt som hensikt å identifisere hva som skaper og påvirker en informasjonssikkerhetskultur og hvilke tiltak som kan forbedre denne. Gjennom å studere definisjoner har studien konkludert med at informasjonssikkerhetskultur og cybersikkerhetskultur brukes om hverandre i det daglige av de som praktiserer og jobber med dette i organisasjoner. I akademia er det klarere skillelinjer mellom begrepene, men det er likevel ikke en etablert konsensus rundt definisjoner av og rammeverk for, informasjonssikkerhetskultur og cybersikkerhetskultur. Dette problematiserer en enkel konklusjon på spørsmålet om hva som skaper og påvirker en slik kultur. Samtidig er det i denne studien identifisert syv sentrale faktorer som skiller seg ut som de mest sentrale for å skape og påvirke en sterk informasjonssikkerhetskultur. Disse er faktorene utdanning/kunnskap, policyer, retningslinjer og prosedyrer, trening, bevisstgjøring, endringsledelse, ledelsesstøtte, og etterlevelse. Tiltak for å forbedre informasjonssikkerhetskultur bør følgelig knyttes til disse faktorene. Videre har denne oppgaven påpekt at sikkerhetsarbeid ikke er et produkt, men en iterativ prosess. På samme måte bør videre forskning fortsette å utforske definisjoner, faktorer og rammeverk slik at vi kan bidra til et sikrere samfunn gjennom økt informasjonssikkerhet. Ettersom denne oppgaven fokuserte på å identifisere faktorer kan videre forskning undersøke effektiviteten av faktorene og hvordan tiltak knyttet til disse bør implementeres i praksis. På denne måten kan vi bidra til at mennesket ikke forblir det svakeste leddet i informasjonssikkerhet.

Referanseliste

AlHogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. 2014 World Congress on Computer Applications and Information Systems (WCCAIS), 1–7. https://doi.org/10.1109/WCCAIS.2014.6916579

Alnatheer, M.A. (2014). A conceptual model to understand information security culture, *International Journal of Social Science and Humanity*, Vol. 4 No. 2, pp. 104-107, doi: 10.7763/ IJSSH.2014.V4.327

Aldulaimi, S. H., Abdeldayem, M. M., & Abo Keir, M. Y. (2023). Formulating the Cyber Security Culture in Organizations: Proposing and Arguing Insights. *International Journal of Professional Business Review*, *8*(5), e01660. https://doi.org/10.26668/businessreview/2023.v8i5.1660

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003–102010. https://doi.org/10.1016/j.cose.2020.102003

Alvesson, M. (2002). *Understanding Organizational Culture* (1. utg.). London: SAGE Publications.

Antonsen, S. (2009). *Safety Culture: Theory, Method and Improvement.* Farnham, UK: Chapman & Hall/CRC Press.

Antonsen, S. (2018). *Key Issues in Understanding and Improving Safety Culture.* In: Gilbert, C., Journé, B., Laroche, H., Bieder, C. (eds) Safety Cultures, Safety Models. SpringerBriefs in Applied Sciences and Technology(). Springer, Cham. https://doi.org/10.1007/978-3-319-95129-4_12

Antonsen, S., Nilsen, M,. Almklov, P. G. (2017). Regulating the intangible. Searching for safety culture in the Norwegian petroleum industry. *Safety Science*, 92, 32-240, https://doi.org/10.1016/j.ssci.2016.10.013

Arbanas, K., Spremic, M., & Zajdela Hrustek, N. (2021). Holistic framework for evaluating and improving information security culture. *ASLIB JOURNAL OF INFORMATION MANAGEMENT*, *73*(5), 699–719. https://doi.org/10.1108/AJIM-02-2021-0037

Aveyard, H. (2014). *Doing a literature Review in Health and Social care* (3.utg.). Open University Press.

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

Bostrøm, L. M. E., Grimstad, A., Palmer, A. (2021). *Sikkerhetskultur i politiet*. Masteroppgave ved Høgskolen i innlandet.

Carlsson, Y. (1984). *Du skal ikke stå på krava*. Arbeidsnotat nr.226, Institutt for sosiologi, Universitetet i Oslo

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture. *The Journal of Computer Information Systems*, *55*(3), 11–19. https://doi.org/10.1080/08874417.2015.11645767

Christensen, T., Lægreid, P., Rørvik, K. A (2021). *Organisasjonsteori for offentlig sektor*. Oslo, Universitetsforlaget.

Cooper, Dominic (2001), *Improving Safety Culture. A Practical Guide*. Hull: Applied Behavioural Science

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

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162–176. https://doi.org/10.1016/j.cose.2014.12.006

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713–101723. https://doi.org/10.1016/j.cose.2020.101713

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information and Computer Security*, 26(5), 584–612. https://doi.org/10.1108/ICS-08-2017-0056

Deal, T. E., & Kennedy, A. A. (1982). *Corporate cultures*. Addison-Wesley.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, *56*, 63–69. https://doi.org/10.1016/j.cose.2015.10.001

Digitaliseringsdirektoratet. (u.å). *Hvorfor styring av informasjonssikkerhet*? Hentet 02.10.2023 fra https://www.digdir.no/informasjonssikkerhet/hvorfor-styring-av-informasjonssikkerhet/3145#:~:text=Informasjonssikkerhet%20handler%20om%20tilstrekkelig%20og%20balansert%20sikring%20av,tiltak%20m%C3%A5%20systematisk%20tilpasses%20i%20takt%20med%20utviklingen.

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

Eskeland, B. (2017). *Samfunnskritisk sikkerhet*. Språknytt 2/2017. Språkrådet. Hentet 23.09.2023 fra https://www.sprakradet.no/Vi-og-vart/Publikasjoner/Spraaknytt/spraknytt-22017/samfunnskritisk-sikkerhet/

Fernández-Muñiz, B., Montes-Peón, J. M. & Vázquez-Ordás, C. J. (2007). Safety culture*:* Analysis of the causal relationships between its key dimensions. *Journal of Safety Research*, 38(6), 627-641. https://doi.org/10.1016/j.jsr.2007.09.001

Flakstad, T-E. C. (2019). *Fokus på sikkerhetskultur i organisasjoner*. Masteroppgave ved UiT- Norges Arktiske Universitet Tromsø.

Fladeby, L-E. (2014). *Sikkerhetskultur i Forsvaret: En idé på reise*. Masteroppgave ved UiT-Norges Arktiske Universitet Tromsø.

Forsvaret (2022). *Fokus 2022*. Hentet 28.11.2023 fra https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/fokus-2022

Furøy, C, T. (2023) *Cybersikkerhetskultur – en studie av interne organisatoriske mekanismers påvirkning*. Masteroppgave ved UiT- Norges Arktiske Universitet Tromsø.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors (*Basel, Switzerland), *21*(9), 3267. https://doi.org/10.3390/s21093267

Gjessing, M. (2023, 16. oktober). *Oppretter eget digitaliseringsdepartement*. Digi.no https://www.digi.no/artikler/oppretter-eget-digitaliseringsdepartement/538368

Guldenmund, F. W. (2000). The nature of safety culture: a review of theory and research. *Safety Science,* 34(1), 215-257. https://doi.org/10.1016/S0925-7535(00)00014-X

Guldenmund, F. W. (2010). (Mis)understanding Safety Culture and Its Relationship to Safety Management. *Risk Analysis*, 30(10), 1466-1480. https://doi.org/doi:10.1111/j.1539-6924.2010.01452.x

Halvorsen, K. (2008). *Å forske på samfunnet: en innføring i samfunnsvitenskapelig metode*. Oslo: Cappelen akademiske forlag.

Hart, C. (1998). *Doing a Literature Review: Releasing the Social Science Research Imagination*. London: Sage.

Haukelid, K. (2008). Theories of (safety) culture revisited—An anthropological approach. *Safety Science*, 46(3), 413-426. https://doi.org/10.1016/j.ssci.2007.05.014

Hayden, L. (2015). *People-Centric Security, Transforming Your Enterprise Security*. McGraw Hill

Hudson, P. (2007). *Implementing a safety culture in a major multi-national*. Safety Science, 45(6), 697-722. https://doi.org/https://doi.org/10.1016/j.ssci.2007.04.005

Høiby, M., Vatn, D. M. K., Fiskvik, J., & Thaulow, K. (2022). *Kunnskapsgrunnlag om bevisstgjøringsstrategier som skal motvirke rekruttering av ubevisste innsidere i norske virksomheter*. SINTEF. ISBN: 978-82-14-07977-7.

ISF (Information Security Forum). (2000) *Information security culture - a preliminary investigation*. s.l. 2000.

International Telecommunication Union (ITU). (2008). *ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity 2008*. Hentet 20.11.2023 fra https://www.itu.int/rec/T-REC-X.1205/en

International Organization for Standardization (ISO). (2022). *Information security management systems* (ISO Standard No. 27001:2022). https://www.iso.org/standard/27001

Jacobsen, D. (2016). *Hvordan gjennomføre undersøkelser*. Oslo: Cappelen Damm AS

Jacobsen, D. I og Thorsvik, J. (2021), *Hvordan organisasjoner fungerer*. Bergen, Fagbokforlaget

Karlsen, J. E. (2004). *Ledelse av helse, miljø og sikkerhet* (2. utg.). Bergen: Vigmostad & Bjørke, Fagbokforlaget.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. *Information and Computer Security*, *23*(3), 246–285. https://doi.org/10.1108/ICS-05-2014-0033

Kongsvik, T., Alberechtsen, E., Antonsen, S., Herrera, I., Hvoden, J., & Schiefloe, P. (2018). *Sikkerhet i arbeidslivet*. Bergen: Fagbokforlaget

Kroeber, A. L. & Kluckhohn, C. (1954). Culture, a Critical Review of Concepts and Definitions. *Bulletin de l'Institut de recherches économiques et sociales,* 20(07), 755. https://doi.org/10.1017/S1373971900104433

Laroche, H. (2018). The Commodification of Safety Culture and How to Escape It: Taking Stock and Moving Forward. I C. Gilbert, B. Journé, H. Laroche & C. Bieder (Red.), *Safety Cultures, Safety Models: Taking stock and moving forward* (s. 167). Springer.

Leverage Edu. (2023). *Difference Between Cybersecurity and Information Security*. Hentet 02.10.2023 fra https://leverageedu.com/blog/difference-between-cybersecurity-and-information-security/

Machi, L.A, McEvoy B.T. (2016). *The Litterature Review – Six steps to Success*. Thousand Oaks, Corwin

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1-6. https://doi.org/10.1109/ICRIIS.2017.8002442

Maslow, A. H. (1943). *A theory of human motivation*. Psychological Review, 50(4), 370-396. Doi: https://doi.org/10.1037/h0054346

McKinsey. (2022). *Building a cybersecurity culture from within: An interview with MongoDB.* Hentet fra https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/building-a-cybersecurity-culture-from-within-an-interview-with-mongodb 24.09.2023

Nasjonal Sikkerhetsmyndighet (NSM). (2023). *Nasjonalt digitalt risikobilde 2023*. Hentet 18.11.2023 fra https://nsm.no/regelverk-og-hjelp/rapporter/nasjonalt-digitalt-risikobilde-2023

Nasjonal Sikkerhetsmyndighet (NSM). (2020a). *Skape en god sikkerhetskultur*. Hentet 23.09.2023 fra: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/opprettholde-og-oppdage/skape-en-god-sikkerhetskultur/

Nasjonal Sikkerhetsmyndighet (NSM). (2020b*). Hva er informasjonssystemsikkerhet?* Hentet 03.10.2023 fra: https://nsm.no/fagomrader/digital-sikkerhet/informasjonssystemsikkerhet/hva-er-informasjonssystemsikkerhet/

Nasjonal Sikkerhetsmyndighet (NSM). (2020c). *Grunnprinsipper for IKT-sikkerhet 2.0*. Hentet 03.10.2023 fra: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

National Institute of Standards and Technology (NIST). (u.å). *Cyber Security*. Hentet 03.10.2023 fra https://csrc.nist.gov/glossary/term/Cyber_Security

Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information and Computer Security, 27*(2), 146–164. https://doi.org/10.1108/ICS-12-2016-0095

Norsk senter for informasjonssikring (NorSIS). (2021). *Nordmenn og digital sikkerhetskultur*. ISSN: 2535-7816

NOU 2006:6. (2006). *Når sikkerheten er viktigst — Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Hentet 28.11.2023 fra https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/?ch=1

NOU 2018:14. (2018). *IKT-sikkerhet i alle ledd: Organisering og regulering av nasjonal IKT-sikkerhet*. Hentet 28.11.2023 fra https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037

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

Perrow, C. (2011). *Normal Accidents: Living with High Risk Technologies* - Updated Edition. Princeton University Press.

Peters, T. (1982). *In search of excellence: lessons from America's best-run companies*. New York: Harper & Row.

PwC. (2023). *Cybersikkerhet: Seks råd til ledere som vil unngå cyberangrep*. hentet fra https://www.pwc.no/no/pwc-aktuelt/cybersikkerhet-seks-rad-til-ledere-som-vil-unngaa-cyberangrep.html 24.09.2023

PwC. (2023). *God organisasjonskultur er avgjørende for suksess.* hentet fra https://www.pwc.no/no/tjenester/people-and-organisation/organisasjonskultur.html 24.09.2023

Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot: Ashgate.

Reason, J. (2007). Achieving a safe culture: Theory and practice. *Work & Stress*, (12), 13.

https://doi.org/10.1080/02678379808256868

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

Regjeringen. (2023). *Cybersikkerhetsforordningen*. Hentet 03.10.2023 fra https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2017/nov/cybersecurity-act/id2590048/

Richter, A. & Koch, C. (2004). Integration, differentiation and ambiguity in safety cultures. *Safety Science, 42, 19. DOI:10.1016/j.ssci.2003.12.003*

Ridley, D. (2012). The Literature Review*: A Step-by-Step Guide for Students* (2.utg). Sage Study Skills

Roughton, J.E. & Mercurio, J.J. (2002). *Developing an Effective Safety Culture: A Leadership Approach*. Butterworth-Heinemann

Schein, E. H. (1991). *What is culture? Reframing organizational culture*. (s. 243-253). Thousand Oaks, CA, US: Sage Publications, Inc.

Schein, E. H. (2010). *Organizational culture and leadership* (4. utg). John Wiley & Sons

Schein, E. H. & Schein, P. (2017). *Organizational culture and leadership* (5. utg). Hoboken: Wiley.

Schlienger, T., Teufel, S. (2002). Information Security Culture. In: Ghonaimy, M.A., El-Hadidi, M.T., Aslan, H.K. (eds) Security in the Information Society. IFIP Advances in *Information and Communication Technology, vol 86*. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-35586-3_15

Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management, 34*(4), 1203–1228. https://doi.org/10.1108/JEIM-08-2019-0217

Språkrådet. (ukjent årstall). *Policy på norsk?* Hentet 25.11.2023 fra https://www.sprakradet.no/svardatabase/?CurrentForm.SearchText=Policy+

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management, 17*(2), 179–186. https://doi.org/10.1007/s10799-015-0252-2

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 2006*(10), 7–11. https://doi.org/10.1016/S1361-3723(06)70430-4

Turner, B. (1978). *Man-made disasters*. London: Wykenham Science Press

Turner, B, Pidgeon, N, F. (1997). *Man Made Disasters*, Oxford: Butterworth Heineman.

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

Von Solms, R. & Van Niekerk, J.F. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Westrum, R. (2004). A typology of organisational cultures. *Quality and Safety in Health Care*, 13(suppl 2), ii22-ii27. https://doi.org/10.1136/qshc.2003.009522

Zohar, D. (1980). Safety climate in industrial organizations: Theoretical and applied implications. *Journal of Applied Psychology*, 65(1), 96–102.

Vedlegg

Vedlegg 1 – Søkehistorikk i databaser

Som vedlegg 1 har jeg valgt å inkludere søkehistorikken til litteraturstudien som ble gjennomført i de 4 databasene. Totalt ble søk gjennomført. Vedlagte tabeller viser hvordan inklusjon og eksklusjon av artikler ble vurdert og gjennomført og er lagt ved for å illustrere rent konkret hvordan litteraturstudien ble operasjonalisert og gjennomført.

Database	Oria
Dato	15.10.2023
Søk nummer	1
Søkeord	(informasjonssikkerhetskultur OR cybersikkerhetskultur OR "Cyber sikkerhetskultur" OR "Information Security culture" OR "cybersecurity culture" OR "Cyber security culture") AND (Organizational OR Organisational) AND culture
Antall treff	55

Database	BASE (Bielefeld Academic Search Engine)
Dato	15.10.2023
Søk nummer	2
Søkeord	(informasjonssikkerhetskultur OR cybersikkerhetskultur OR "Cyber sikkerhetskultur" OR "Information Security culture" OR "cybersecurity culture" OR "Cyber security culture") AND (Organizational OR Organisational) AND culture
Antall treff	69

Database	Web of Science
Dato	17.10.2023
Søk nummer	3
Søkeord	(informasjonssikkerhetskultur OR cybersikkerhetskultur OR “Cyber sikkerhetskultur” OR “Information Security culture” OR “cybersecurity culture” OR “Cyber security culture”) AND (Organizational OR Organisational) AND culture
Antall treff	42

Database	Google Scholar
Dato	17.10.2023
Søk nummer	4
Søkeord	(informasjonssikkerhetskultur OR cybersikkerhetskultur OR “Cyber sikkerhetskultur” OR “Information Security culture” OR “cybersecurity culture” OR “Cyber security culture”) AND (Organizational OR Organisational) AND culture AND “peer review*”
Antall treff	17

Vedlegg 2 – Liste over inkluderte artikler

#	Forfatter, årstall og tittel	Tidsskrift	Begrunnelse for inklusjon i litteraturstudien
1	Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs.	Computers & Security	Studien undersøkte 58 artikler for å identifisere sentrale faktorer i informasjonssikkerhetskultur og cybersikkerhetskultur samt definisjoner.
2	Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry.	Computers & Security	Artikkelen samler perspektiver på informasjonssikkerhetskultur fra akademia og næringslivet og gir en omfattende definisjon av begrepet. Artikkelen sammenstiller og kategoriserer også 25 faktorer som kan påvirke informasjonssikkerhetskultur positivt.
3	Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture.	Computers & Security	Artikkelen presenterer et rammeverk for å skape en sterk informasjonssikkerhetskultur basert på en definisjon som forskerne også står bak.
4	Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective.	Computers & Security	Artikkelen er inkluderte da den presenterer en konseptuell modell av informasjonssikkerhetskultur, som integrerer økonomiske prinsipper for å illustrere hvordan ulike variabler i en informasjonssikkerhetskultur påvirker hverandre.
5	Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013.	Information and Computer Security	Artikkelen gir en svært grundig gjennomgang av eksisterende forskning på informasjonssikkerhetskultur fra 2000 til 2013.
6	Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations.	Information and Computer Security	Artikkelen identifiserer nøkkelaspekter ved informasjonssikkerhet og kategoriserer faktorer i ulike nivå. Selv om organisasjonene artikkelen ser på er begrenset til Sør-Afrika vurderes resultatet fra den omfattende litteraturstudien artikkelen gjennomfører som nyttig for å besvare denne studiens problemstilling.

7	Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture.	Computer Fraud & Security	Artikkelen gir en inngående analyse av hvordan ansattes kunnskap, ferdigheter og engasjement direkte påvirker informasjonssikkerheten i en organisasjon. Den presenterer også opp flere faktorer som som besvarer et av denne studiens forskningsspørsmål.
8	Da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture.	Information and Computer Security	Artikkelen presenterer en tilnærming til styring av endringer i informasjonssikkerhetskultur basert på sentrale faktorer.
9	Arbanas, K., Spremic, M., & Zajdela Hrustek, N. (2021). Holistic framework for evaluating and improving information security culture.	Aslib Journal of Information Management	Artikkelen ser på teknologiske, organisatoriske og sosiologiske faktorer for informasjonssikkerhetskultur og fremmer en rammeverk for å forbedre denne.
10	Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture.	The Journal of Computer Information Systems	En av få artikler som tilbyr en definisjon av informasjonssikkerhetskultur. Artikkelen utforsker videre sammenhengen mellom informasjonssikkerhetsprogrammer og sikkerhetskultur. Artikkelens empiriske testing gir innsikt i hvordan spesifikke komponenter som utdanning, trening og bevisstgjøring påvirker sikkerhetskultur.
11	Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study.	Computers & Security	Artikkelen presenterer en case-studie av en internasjonal finansinstitusjon der en vurdering av informasjonssikkerhetskultur ble gjennomført ved fire intervaller over en periode på åtte år, over 12 land. Artikkelen ble vurdert relevant ettersom den inkluderte 12 land og en lengre tidsperiode i tillegg til at faktorer som påvirker informasjonssikkerhetskultur var en sentral del studien.