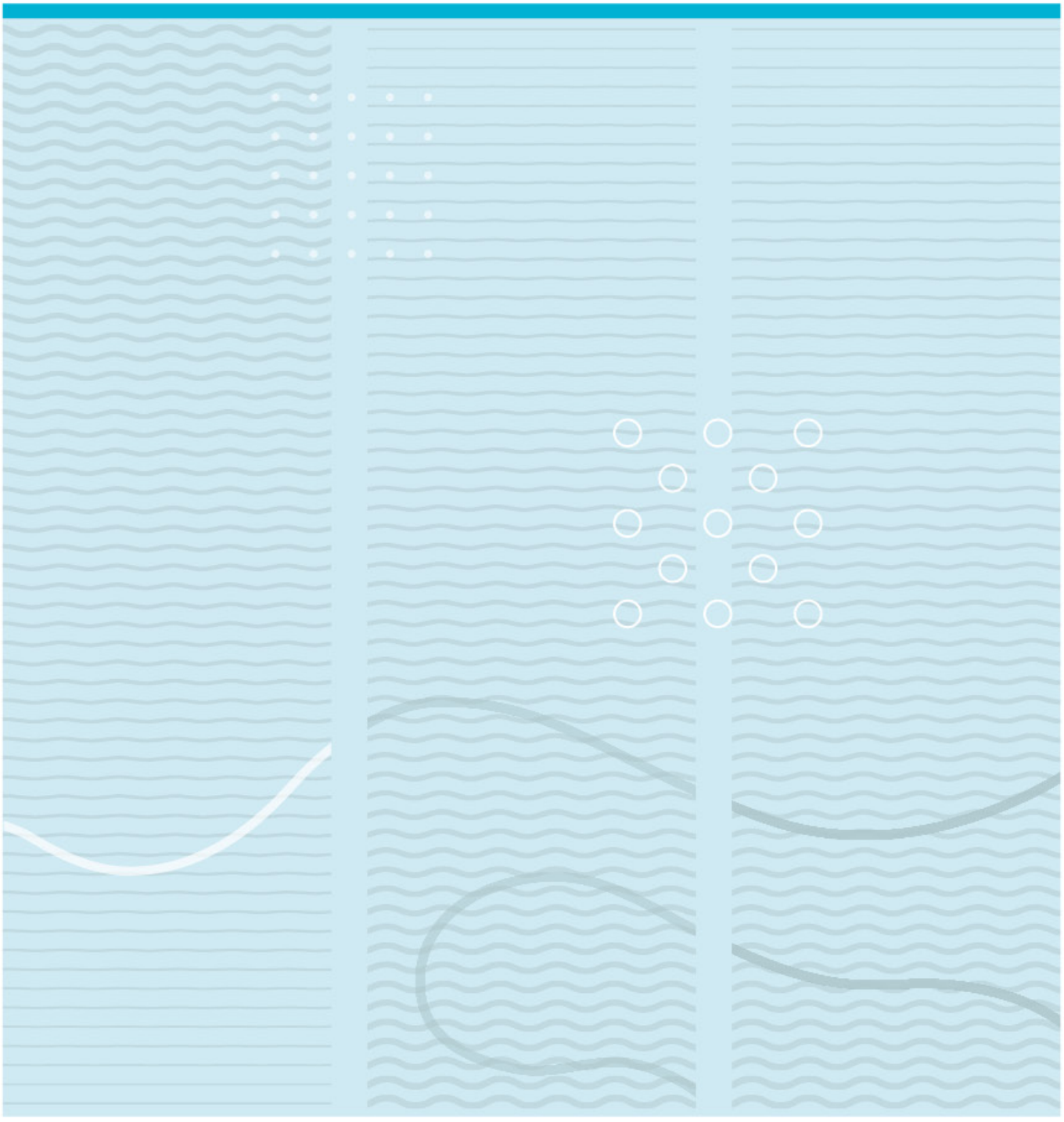
Universitetet i Sørøst-Norge
Handelshøyskolen

Mastergradsavhandling i økonomi og ledelse
Studieprogram: Strategi og kompetanseledelse
**Vår 2020**

Tonje Langelid & Viktoria Røtterud

# Informasjonssikkerhetskultur i bank

En case-studie om leders betydning



# *Forord*

Vi er to studenter som har skrevet denne masteravhandlingen som siste ledd av vår utdannelse i Strategi og kompetanseledelse ved Universitetet i Sørøst-Norge (USN) avdeling Ringerike. Masteroppgaven er skrevet våren 2020 og er et selvstendig arbeid over 22 uker.

Vi vil benytte anledningen til å takke Glenn Kristiansen, vår veileder gjennom hele oppgaven for hjelp og råd. Vi vil også benytte anledningen til å takke banken som har tatt seg tid til å sette av møter med oss over Skype i en hektisk tid med epidemi. En stor takk til informantene i produksjonsstøtteavdelingen og markedsavdelingen som i sin travle arbeidshverdag har tatt seg tid til å øke vår kunnskap om lederstil og informasjonssikkerhetskultur.

Vi vil rette en stor takk til vår kontaktperson i banken for god hjelp og støtte i en krevende tid. Uten vedkommende hadde vi ikke fått kontakt med informantene eller kunnet ferdigstilt avhandlingen.

Avslutningsvis vil vi takke familie og våre samboere for god støtte og forståelse.

Hønefoss, 1 juni 2020.

Tonje Langelid

Viktoria Røtterud

## *Sammendrag*

Den teknologiske utviklingen har ført til endringer i norsk bank- og finansnæring, og har gjort informasjonssikkerhet til en viktig del av arbeidet. Sikkerhetsbruddene har større konsekvenser enn tidligere, og etableringen av en informasjonssikkerhetskultur er nødvendig for å kunne etablere en effektiv informasjonssikkerhetspraksis. Denne oppgaven har derfor som formål å kartlegge informasjonssikkerhetskulturen i to avdelinger i en norsk bank, og hvilken betydning leder har for denne informasjonssikkerhetskulturen. Vår problemstilling er som følger: *"hvilken rolle spiller lederstil for informasjonssikkerhetskulturen i bank?"*

Teori om organisasjonskultur, informasjonssikkerhetskultur og lederstil danner grunnlaget for studien. Undersøkelsen ble gjennomført ved kvalitativ tilnærming, og datamaterialet ble samlet inn gjennom intervju av 16 informanter fra to ulike avdelinger. Informantene besto av to avdelingsledere og ansatte på disse avdelingene. I tillegg ble det gjort bruk av offentlige dokumenter for å få belyst fenomenet informasjonssikkerhetskultur på en bedre måte. Det var ønskelig å få kunnskap om emnet for å kunne bidra til å se hvilken betydning leder har for informasjonssikkerhetskulturen. Dette ville vi gjøre ved å kartlegge informasjonssikkerhetskulturen i avdelingene, samt lederstilen de to avdelingslederen før vi så hvilken rolle lederne kan spille for informasjonssikkerhetskulturen.

Informasjonssikkerhetskulturen fremstår som god i begge avdelingene. Leder i avdeling 2 har flere karakteristikker fra en transformasjonsleder, og ansatte i denne avdelingen er i større grad bevisste på informasjonssikkerhet. Ansatte ble påvirket gjennom positiv innflytelse slik at de forstår konsekvensene ved sikkerhetsbrudd (Avolio, Bass, Berson & Jung, 2003; Da Veiga & Eloff, 2010). Det indikerer at transformasjonsledelse er en lederstil som har en positiv innvirkning på informasjonssikkerhetskulturen (Bass, 1990; Niekerk & Solms, 2010; Safa & Solms, 2016). Transaksjonsledelse fremstår likevel som en lederstil som er viktig for overholdelse av regler og rutiner som vil fremme sikkerhetsatferd (Avolio et al., 2003; Humaidi & Balakrishnan, 2015). Ansatte ble påvirket til å sørge for god etterlevelse av instrukser og rutiner ved at leder følger opp rutiner og instrukser før det oppstår avvik, rutinebrudd eller informasjonssikkerhetsbrudd (Antonakis Avolio & Sivarsubramaniam, 2003; Avolio et al., 2003; Guhr & Breitner, 2018). Sentrale trekk ved transformasjonsledelse er mer fordelaktig for en mer helhetlig tilnærming til arbeid for informasjonssikkerhetskultur på avdelingsnivå. Selvgående og proaktive ansatte som ikke bare følger regler og prosedyrer, kan være aktive bidragsytere i sikkerhetsarbeidet på daglig basis (Guhr & Breitner, 2018).

# *Innholdsfortegnelse*

# *1. Innledning*

I dag påvirker informasjonssystemer nesten alle. De siste årene har digital teknologi gitt enkeltpersoner, organisasjoner og samfunnet nye muligheter (Meyers og Avison, 2002). Det har gitt offentlige og private virksomheter nye muligheter til å samle inn, lagre og administrere informasjon. Når organisasjoner blir mer avhengige av informasjonssystemer for strategisk fordel og drift, blir også spørsmålet om informasjonssikkerhet stadig viktigere (Kankanhalli,Teo,Tan & Wei, 2003). Mens teknologi i økende grad har skapt forskjellige innovasjonsmuligheter i organisasjoner, har disse mulighetene også forårsaket alvorlig risiko forbundet med informasjon. På grunn av denne risikoen har informasjonssikkerhet blitt et stort problem i organisasjoner. Sikkerhetsbruddene har større konsekvenser enn tidligere, og selskaper som er avhengige av å beskytte informasjonen i sine datasystemer opplever store utfordringer (Moon et al., 2018). Virksomheter må derfor investere i informasjonssikkerhet for å forhindre angrep som kan føre til konkurransemessige ulemper (Kankanhalli et al., 2003).

Omfanget av virksomheter som uttrykker bekymring i forhold til deres informasjonssikkerhet er stor. Virksomheter investerer betydelige summer for å redusere potensielle trusler i forbindelse med informasjonssikkerhet. Ifølge International Data Corporation1 anslås det at globale firmaers utgifter til informasjonssikkerhet vil øke fra 83,5 milliarder dollar i 2017 til 119,9 milliarder dollar innen 2021 (Hwang et al., 2019). En undersøkelse gjort av Experis viser at en betydelig del av norske virksomheter har hatt minst ett tilfelle av sikkerhetsbrudd i løpet av et år. Sikkerhetsbrudd skjer stadig oftere, og det ble registrert 40% flere databrudd i 2015 enn året før. Det brukes også stadig mer ressurser for å håndtere sikkerhetstrusler mot datasystemer (Experis, 2019).

Virksomheter konsentrerer seg primært om tekniske tiltak for å forhindre potensielle angripere. Selv om det tekniske aspektet er viktig, er det en dominerende svakhet å sikre informasjon gjennom den enkelte bruker i en virksomhet. Det er spesielt viktig fordi forskere har estimert at nesten halvparten av innbrudd og sikkerhetsbrudd skjer på innsiden av virksomheten (Crossler, Johnston & Lowry, 2013). De menneskelige faktorene som policy, opplæring og utdanning får betydelig mindre oppmerksomhet enn sikkerhetsløsninger som brannmurer, antivirus og inntrengningsdeteksjon. En årsak til dette er at de menneskelige

aspektene på mange måter oppleves som et mer utfordrende problem å tilnærme seg, og fordi det ikke kan målrettes med en produktbasert løsning (Furnell og Clarke, 2012). Cyberkriminaliteten retter seg mot de menneskelige ressursene i virksomheten og øker raskt. Ansatte og ledere blir sett på som det svakeste leddet, og angriperne ønsker å utnytte manglende oppmerksomhet om informasjonssikkerhet (He & Zhang, 2019). De vanligste årsakene til sikkerhetsbrudd er ansatte og lederes mangel på oppmerksomhet (Safa og Solms, 2016). Tre av de vanligste årsakene til at et sikkerhetsbrudd oppstår er relatert til menneskelige feil ved at eksisterende prosesser ikke følges og mangel på sikkerhetsbevissthet hos ansatte (Eriksen, 2018).

Etablering av en informasjonssikkerhetskultur i en organisasjon er nødvendig for å kunne etablere en effektiv informasjonssikkerhetspraksis, og er et samspill mellom organisasjonsmedlemmene, deres sikkerhetsatferd og tekniske sikkerhetstiltak (Da Veiga & Eloff, 2010). Flere forskere mener at leder har en viktig rolle for utviklingen av en informasjonssikkerhetskultur, hvor leder har makt til å endre kultur ved å introdusere nye tiltak og praksiser (Antonsen, 2009; Da Veiga & Eloff, 2010; Niekerk & Solms, 2010; Reason, 1997; Schlienger & Teufel, 2003).). På grunn av rask teknologisk utvikling er det et stadig behov for mer forskning på administrasjon og informasjonssikkerhet (Bongiovanni, 2019; Crossler et al., 2013). Vi ønsker å få mer innsikt på dette området, og vil utforske på hvilken måte leder forholder til informasjonssikkerhet. Derfor vil vi se på forholdet mellom lederstil og informasjonssikkerhetskultur. Vår problemstilling er derfor som følger:

*"Hvilken rolle spiller lederstil for informasjonssikkerhetskultur i bank?"*

I denne avhandlingen presenteres relevant teori i kapittel 2, hvor vi innledningsvis vil foreta en begrepsavklaring av informasjonssikkerhet. I sammenheng med dette vil vi gjøre rede for informasjonssikkerhetsrelaterte lovkrav og praksiser tilknyttet bank. Deretter presenteres et organisasjons- og informasjonssikkerhetskulturrammeverk med tilhørende begrepsavklaring. Lederstilene transformasjon- og transaksjon presenteres før vi vil forklare hvordan fenomenene lederstil og informasjonssikkerhet kan være relatert til hverandre. I kapittel 3 vil vi gi en gjennomgang av metodikken som er benyttet i oppgaven, etterfulgt av en presentasjon av analyse i kapittel 4. I kapittel 5 drøftes studiens funn mot de teoretiske perspektivene før konklusjonen presenteres. Avslutningsvis presenteres begrensninger med studien og forslag til videre forskning.

## *1.1. Avgrensning og presisering av problemstilling*

Vi har valgt å avgrense avhandlingen til å undersøke finanssektoren, nærmere bestemt bankvirksomhet. Årsaken til valg av bankvirksomhet er at de har god kjennskap til informasjonsbehandling og sikkerhet, blant annet fordi dette er pålagt gjennom lover og krav som omtalt i kapittel 2.1. Bransjen har dermed i lenger tid gjennomført programmer rettet mot å utvikle sikkerhetskultur. Grunnet bankvirksomhetenes forhold til sikkerhetskulturbegrepet, samt økt fokus på sikkerhet i bransjen, forventes det at de kan bidra med å gi økt innsikt og forståelse omkring temaet informasjonssikkerhetskultur. Uavhengig av om virksomheten benytter begrepet, kan det tenkes at de i ulik grad arbeider med kulturbygging tilknyttet virksomhetens sikkerhetsarbeid, og kan bidra med relevant kunnskap og informasjon. For å ivareta ansatte og lederes personvern, og av hensyn til virksomheten, har vi valg å sensurere banken og datamaterialet.

Grunnet begrenset forskning om avhandlingens problemstilling, samt at kultur er et krevende forskningsområde, inntar vi en ydmyk tilnærming til temaet. Vi er avhengig av å måle informasjonssikkerhetskulturen i avdelingene for å kunne besvare vår problemstilling. Det er anbefalt å gjennomføre observasjon i forbindelse med kartlegging av kultur (Schein & Schein, 2017). På grunn av begrenset tid til å gjennomføre studiet og Covid-19 situasjonen, var observasjon vanskelig å gjennomføre. Muligheten for å måle informasjonssikkerhetskulturen vil dermed begrenses. I avhandlingen vil derfor informasjonssikkerhetskulturen i avdelingene kartlegges på bakgrunn av ansatte og lederes tolkninger, forståelser og meninger rundt sin respektive kultur.

Videre har vi avgrenset sikkerhet til å gjelde informasjonssikkerhet, og ikke fysisk sikkerhet som brannvern, ran eller personell sikring. Fysisk sikkerhet vil være en del av den totale sikkerheten i virksomheten, og vil derfor være et aspekt av organisasjonskulturen. Dette vil derfor falle utenfor vår problemstilling.

# 2. Teoretisk perspektiv

For å utforske hvilken rolle lederstil kan spille for informasjonssikkerhetskulturen vil vi i det følgende presentere en teoretisk ramme som vår analyse og drøftelse vil bygge på. Temaet for oppgaven er fenomenene lederstil og informasjonssikkerhetskultur. For å få en forståelse av begrepet informasjonssikkerhetskultur må vi se hen til den overordnede organisasjonskulturen. Deretter presenteres relevant teori om lederstilene transformasjons- og transaksjonsledelse, før vi avslutningsvis vil se på hvordan lederstil kan være relatert til informasjonssikkerhetskultur.

## 2.1. Informasjonssikkerhet

De teoretiske perspektivene vil som nevnt innledningsvis være rettet mot bankvirksomhet. Informasjonssikkerhetsområdet vil dermed inneholde det vi mener er de viktigst elementene for bankvirksomhet. Ifølge datatilsynet dreier informasjonssikkerhet seg om å *"håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger"* (Datatilsynet, 2018, s.1). Informasjonssikkerhet gjelder behandling av personopplysninger som er muntlig, papirbasert og digitalbehandling av informasjon. Det omfatter derfor alle typer av informasjon som skal beskyttes på en god måte, uansett om informasjonen lagres eller formidles (Datatilsynet, 2018, s1). Informasjonssikkerheten har fire områder som skal beskyttes:

- Konfidensialitet vil si at informasjonen bare skal være tilgjengelig for autoriserte personer og prosesser. I bankvirksomhet er det slik at det gis tilgjengelighet til dokumenter ved relevant kundebehandling og at denne dataen ikke skal brukes om det ikke er behov.
- Integritet vil si at *"informasjonen ikke blir endret utilsiktet eller av uvedkommende"* (Datatilsynet, 2018, s.1). Det er viktig at informasjonen til enkeltindivider blir ivaretatt slik at personlig informasjon ikke kommer på avveie. I en bank vil det innebære at uvedkommende ikke får tilgang til informasjon som kan føre til alvorlige konsekvenser for banken. På denne måten kan tilliten fra kundene forsvinne. En bank er avhengig av tillit fra sine kunder, og en slik hendelse vil derfor utgjøre en stor trussel.

- Tilgjengelighet er "*at informasjonen er tilgjengelig for autoriserte ved behov"* (Datatilsynet, 2018, s.1). I bank er autoriserte fagfolk avhengig av å innhente informasjon om kundene slik at de kan hjelpe eller forvalte låneavtaler til kunden.
- Robusthet vil si at "*organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser"* (Datatilsynet, 2018, s. 1). Det kan være trusler som for eksempel datasvindel og bankens evne til å gjenopprette normaltilstand ved en slik hendelse.

Sikkerhetsområdene ovenfor blir ofte brukt for beskyttelse av informasjonssikkerhet (Datatilsynet, 2018). Virksomheter opplever stadig nye sikkerhetstrusler og dermed er det viktig at de holder seg oppdatert på nye trusler og sårbarheter, samt tar stilling til om de har etablert tilstrekkelig sikring av informasjonsmidlene (Eriksen, 2018). Ivaretakelse av personvernregelverket er en kontinuerlig prosess og med fokus på de fire sikkerhetsområdene. De fire sikkerhetsområdene er stadig under utvikling og den sikringen banken hadde i fjor, er kanskje ikke gode nok i dag (Datatilsynet, 2018). For å oppnå tilstrekkelig sikkerhet må virksomheten derfor ta hensyn til behandlingens art, formål, omfang og sammenheng. De må undersøke hva som finnes av tilgjengelig teknologi, kostnader ved gjennomføring og få oversikt over sannsynligheten for uønskede hendelser skal inntreffe (Datatilsynet, 2018). Datatilsynet mener at "*informasjonssikkerhet oppnås ved hjelp av tekniske og organisatoriske tiltak"* (Datatilsynet, 2018, s. 1). I det følgende vil vi derfor redegjøre for sikkerhet tilknyttet informasjon og den overordnede sikkerheten i banken i forhold til relevante lover og forskrifter.

### *2.1.1. Informasjonssikkerhetsrelaterte lovkrav*

For å få informasjon om hvordan banken forholder seg til og arbeider med informasjonssikkerhet anså vi det som hensiktsmessig å gjennomføre dokumentinnsamling av interne prosedyrer og policyer. Dette var imidlertid ikke mulig å gjennomføre på grunn av regelverket banken er bundet av. Ved å intervjue IT-avdelingen fikk vi imidlertid et innblikk i interne prosedyrer og policyer, og hvilke risikoer de anser som mest relevante. Vi gjennomførte en dokumentanalyse av lovverk om informasjonssikkerhet i bankvirksomhet som i kombinasjon med intervjuene vil gi et helhetlig bilde på hvordan banken arbeider for informasjonssikkerhet. Lovverket om informasjonssikkerhet i bankvirksomhet vil avgrenses til Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) av 21. mai 2003

nr. 630 (Heretter IKT-forskriften), Lov om behandling av personopplysninger av 15. Juni 2018 nr. 38 (Heretter Personopplysningsloven) og Lov om finansforetak og finanskonsern av 10. April 2015 nr.17 (Heretter Finansforetaksloven). Det finnes flere lover som direkte og indirekte legger føringer for sikkerhet i norske banker, men det er de overnevnte lovkravene som fastsetter de største delene av det regulatoriske rammeverket for informasjonssikkerheten.

IKT-forskriften gjelder blant annet for forretningsbanker, sparebanker, finansforetak og forsikringsselskaper, jf. IKT-forskriften § 1. Denne loven legger føringer for at sikkerhet og dokumentasjon skal ivaretas ved bruk av IKT-systemer. Personvernloven gjelder for behandling av personopplysninger som knyttes til enkeltpersoner, jf. Personvernloven § 2. Finansforetaksloven omhandler finansiell stabilitet som vil si at finansielle systemet er robust nok til å motta og utbetale innskudd og andre tilbakebetalingspliktige midler fra allmennheten, formidle finansiering, utføre betalinger og omfordele risiko på en tilfredsstillende måte jf. Finansforetaksloven § 1. I Finansforetaksloven vil § 9- 6 være mest relevant for informasjonssikkerhet. ISO-27001 er en standard som omfatter organisatoriske krav om hvordan virksomheter bør implementer, ivareta og forbedre sine informasjonssikkerhetsstyringssystemer. Denne standarden gjelder imidlertid ikke for den banken vi undersøker da de ikke er ISO-27001 sertifisert, og vi vil derfor ikke ta for oss denne i den videre redegjørelsen.

Sikkerhetsmål og sikkerhetsstrategi

Virksomheten er pliktige til å fastsette mål, strategier og sikkerhetskrav og det skal foreligge beskrivelse av den enkelte prosess. I dette ligger det blant annet at en bankvirksomhet skal sette sikkerhetsmål for å kunne nå virksomhetens øvrige mål, jf. IKT-forskriften § 2. I tillegg skal ansvaret for administrasjonen, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte, jf. IKT-forskriften §2. Det skal være en ansvarlig med en funksjon eller stilling for de ulike delene av IKT- virksomheten som er definert i banken. Dette skal være tilgjengelig for alle ansatte. Det er viktig at alt med sikkerhetsarbeid avklares under utviklingen av strategier slik at ledelse, driftspersonell og andre ansatte vet hvordan de skal kunne bidra til å nå målene.

Fysisk og logisk informasjonssikkerhet

Banken skal utarbeide prosedyrer som skal sikre beskyttelses av utsyr, systemer og

informasjon av betydning, mot skader, misbruk uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare jf. IKT-forskriften §5. Fysisk sikring av utsyr i bankvirksomhet kan omfatte låsing av skjerm når en går fra datamaskinen sin. Det gjennomføres opplæring i hvordan behandle datamaskinen utenfor arbeidsplassen, som for eksempel at maskinen ikke skal ligger tilgjengelig for uvedkommende. Logisk sikring kan eksempelvis være brannmurer og anti-virus systemer. Det er viktig i den forbindelse at banken utarbeider prosedyrer som skal sikre beskyttelses av utsyr, systemer og informasjon av betydning, mot skader, misbruk uautorisert adgang og endring, samt hærverk, jf. IKT-forskriften § 5.

Under intervjuet med IT-avdelingen kom det frem at det er formulert en sikkerhetspolicy som er godkjent i bankens styre. Det er et forpliktende dokument som tar for seg hvem som har ansvaret for de forskjellige sikkerhetsområdene og hvem som har ansvaret for opplæring. Under policyen er det en rekke rutiner og standarder som er utarbeidet. Standarder er omfattende og inneholder grundige forklaringer, mens rutiner er en oppskrift på hvordan ting skal gjennomføres. Disse er utarbeidet og i samsvar med IKT –forskriften § 5 om at det skal utarbeides prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet.

Personvern og taushetsplikt

Personvern og taushetsplikt er en viktig del av sikring av informasjon i bankvirksomhet. Dette er fastsatt gjennom personopplysningsloven som skal verne om fysiske personer i forbindelse med behandling og om utveksling av personlige opplysninger. Personopplysningsloven gjelder for *"helt eller delvis automatisert behandling av personopplysninger og ved ikke-automatisert behandling av personopplysninger"*, jf. Personopplysningsloven § 2. Ikke automatisert behandling vil eksempelvis være dokumenter som inneholder personopplysninger som sendes per post. Automatisert behandling kan for eksempel være søknader som lagres i en database. Som en del av informasjonssikkerheten vil overholdelse av taushetsplikt ved behandling av personlig informasjon også være et viktig moment. Ansatte plikter å hindre at uvedkommende får adgang eller kjennskap til opplysninger om kunder og andre forretningsmessige eller personlige forhold som ansatte behandler i sitt arbeid med mindre det er hjemmel i lov eller forskrift som tillater det, jf. Finansforetaksloven § 9-6.

Avvik- og endringshåndtering

IKT-forskriften § 9 omhandler avvik- og endringshåndtering og fastsetter prosedyrer for avvikshåndtering som skal omfatte alle avvik som oppstår. Formålet med avviksbehandlingen er å gjenopprette normal tilstand og identifisere årsaken til avvik, hindre gjentagelser og sikre forsvarlig og formell behandling av avviket. Under intervjuet med IT-avdelingen kom det frem at banken benytter en hendelseslogg som tar for seg rapportering av uønskede hendelser og avvik. Prosedyrene for endringshåndtering av de innrapporterte hendelsene skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift, jf. IKT-forskriften § 9.

Kontinuitetsløsning og katastrofeplan

I IKT-forskriften § 10 settes det krav til prosedyrer hvor roller, ansvarsoppgaver og risiko defineres og at dette fremkommer i en oppdatert kontinuitetsplan. Denne kontinuitetsplanen skal inneholde identifisering og vurdering av enkeltelementer som kan svikte. Dermed må det iverksettes tiltak og kriterier for oppstart av reserveløsninger, gjenopprettingsprosedyrer og informasjon til ledelse, ansatte, eventuelle kunder og leverandører. For denne planen er det viktig å gjennomføre opplæring, øvelser og testing som skal gi trygghet for at alt fungerer. Dette skal dokumenteres og resultatet skal vurderes i ettertid. Etter IKT – forskriften § 11 er banken pålagt å ha en katastrofeplan. Ved disse kravene er det slik at det skal minst en gang i året gjennomføres opplæring, øvelser og test slik at en ser at planen fungerer som normalt, jf. IKT-forskriften § 11.

Risikostyring

Virksomheten skal fastsette kriterier for akseptabel risiko, dokumentere prosessen og gjennomføre en risikoanalyse av IKT-systemene, jf. IKT-forskriften § 3. Gjennom risikoanalysen skal det settes opp en akseptabel grense av risiko og dette resultatet skal dokumenteres en gang årlig. I samsvar med IKT forskriften § 3 blir det foretatt risikoanalyser i banken. Under intervjuene med IT-avdelingen kom det frem at banken får hjelp fra organer høyere opp i systemet for å håndtere risikoen, samt at det eksisterer egne fagområder som setter standard for opplæring, utvikling, og hvordan de skal sørge for en god sikkerhetskultur. Risikovurderinger tas av en egen avdeling og der vurderes det nye momenter fortløpende, hvor det også følges med på trender. Dersom det oppdages en risiko vil det vurderes hvilke tiltak som kan iverksettes for å senke risikoen. Det blir gjennomført risikovurderinger

kontinuerlig gjennom hele året, men dersom det oppstår en hendelse eller flere hendelser av samme art vil risikoavdelingen sette det opp som et eget agendapunkt. De risikoene banken selv anser som mest relevante er falske eposter som eksempelvis phishing email som prøver å stjele brukernavn eller passord, men også eposter som krypterer alle filene du har tilgang til når du trykker på en link. Et annet element de anser som en risiko er data på avveie, som eksempelvis vil være personopplysninger som sender i åpne kanaler. Dersom det skulle oppstå sikkerhetsrelaterte hendelser eller mistenksomheter skal dette rapporteres i en hendelsesbase.

Sikkerhetskultur

Det finnes ikke noe direkte lovkrav om sikkerhetskultur i bank. Det er stort sett IKT-forskriften som legger til rette for en sikkerhetskultur i bankvirksomhet gjennom å sette sikkerhetsmål, strategier og drive risikostyring som de må forholde seg til. Det jobbes hele tiden mot en kontinuitetsplan. IT-avdelingen har et stort ansvar ved å holde systemene vedlike og sørge for at medarbeidere klarer å holde risikoen nede ved å følge de instruksene de har fått beskjed om. Det er slik alle ansatte og ledere må forholde seg til IKT-forskriften som omhandler fysisk og logisk sikkerhet. I tillegg må de forholde seg til Personvernloven og Finansforetaksloven som sørger for at informasjonssikkerheten blir ivaretatt for kundene. Det er slik at alle lovene og forskriftene banken må forholde seg til i dag er med på å skape en helhetlig sikkerhetskultur i banken.

Det mest brukte og effektive hjelpemiddelet som benyttes i banken for å skape en informasjonssikkerhetskultur er ved hjelp av korte e-læringskurs som er spisset mot informasjonssikkerhet. Banken foretar risikovurderinger kontinuerlig, og en del av disse kursene er rettet spesifikt mot disse risikoene. I forbindelse med denne spesielle globale situasjonen som vi er i, coronapandemien, er det foretatt risikoanalyser på grunn av endret sikkerhetsbilde og det er identifisert en rekke utfordringer knyttet til dette. Det siste e-læringskurset handlet derfor om hvordan behandle informasjon på en sikker måte ved hjemmekontor. Det kan for eksempel være at det ikke er tillatt å skrive ut konfidensielle papirer på egen printer.

### *2.1.2. Perspektiver på informasjonssikkerhet*

Det presenteres to synsvinkler i litteraturen på hvordan man oppfatter teknologi og organisasjoner på. Den ene måten er å se mennesker eller organisasjoner og teknologi som diskret og uavhengige av hverandre. Den andre måten er å anta at mennesker eller organisasjoner og teknologi er gjensidig avhengig av hverandre gjennom pågående samhandling (Orlikowski & Scott, 2008). Sistnevnte oppfatning vil være slik vi velger å se teknologi og organisasjoner, og kan beskrives som et sosioteknisk perspektiv (Mjølsnes, 2012).

Et sosioteknisk perspektiv på informasjonssikkerhet elementer fra informasjonssikkerhetsprosesser, og samspillet mellom disse elementene. Dette vil være gjennom både uformelle og formelle organisatoriske prosesser. De formelle organisatoriske prosessene vil blant annet omfatte teknologi og administrerende rutineoppgaver gjennom eksempelvis implementering og oppfølging av tiltak gjennom retningslinjer, planer, policyer, risikoanalyse og treningsprogrammer. De uformelle organisatoriske prosessene omfatter organisatorisk atferd, individuell atferd, holdninger, kunnskap og bevissthet. Disse relaterte faktorene skaper et nett av tekniske og ikke-tekniske elementer som per definisjon skal skape et sikkert, pålitelig og tilgjengelig informasjonssystem (Mjølsnes, 2012). Informasjonssikkerhetsstyring i bankvirksomhet kan betraktes som det totale av aktiviteter som utføres for å kontrollere trusler og sårbarheter (Mjølsnes, 2012).

De formelle dokumenterte informasjonssikkerhetsprosessene må være på plass. Uten det vil ikke systematisk og uformell styring vært mulig. Policyer, planer, retningslinjer og standarder vil fungere som en veiledning for informasjonssikkerhetsarbeidet. Imidlertid er det også behov for en utfyllende uformell tilnærming. De formelle prosessene er hovedsakelig relatert til hvordan ting er planlagt utført, mens de uformelle er opptatt av hvordan ting virkelig gjøres i praksis. Det handler altså om hvordan informasjonssikkerhet blir bevart i daglige menneskelige organisatoriske aktiviteter. I en uformell tilnærming til informasjonssikkerhet, finner vi det sosiotekniske perspektivet relatert til menneskelige ressurser, politiske og symbolske perspektiver til en organisasjon som individuell atferd, bevissthet og kunnskap gjennom det som kalles for informasjonssikkerhetskultur (Mjølsnes, 2012).

## 2.2. Organisasjonskultur og informasjonssikkerhetskultur

I det følgende vil vi forklare begrepene kultur og organisasjonskultur. Begrepene kultur og organisasjonskultur er uklare i litteraturen om informasjonssikkerhetskultur. På grunn av denne uklarheten viser mange forskere til teori om organisasjonskultur for å forstå informasjonssikkerhetskultur (AlHogail, 2015; Da Veiga & Eloff, 2010; Guldenmund, 2000; Niekerk & Solms, 2010; Schlienger & Teufel, 2003; Thang, Li & Zhang, 2016; Thomson, Solms & Louw, 2006).

### 2.2.1. Begrepet organisasjonskultur

Den generelle forståelsen av kultur er at det et vidt begrep som går på tvers av mange ulike disipliner, og det finnes ingen universell og bestemt forståelse av begrepet. En utbredt definisjon på kultur er *"the way we do things around here"* (Deal & Kennedy, 1982). Schein (2010) forklarer at kultur skapes av vår interaksjon med andre, formes av vår egen atferd og endres kontinuerlig. Begrepet har blant annet blitt benyttet til å forklare normer og praksiser som utvikles blant menneskene i en organisasjon eller gruppe. Kulturen i en organisasjon kan gi medlemmene en felles identitet, øke stabiliteten i det sosiale systemet som organisasjonen utgjør, og fremme kollektivt engasjement (Schein, 2010).

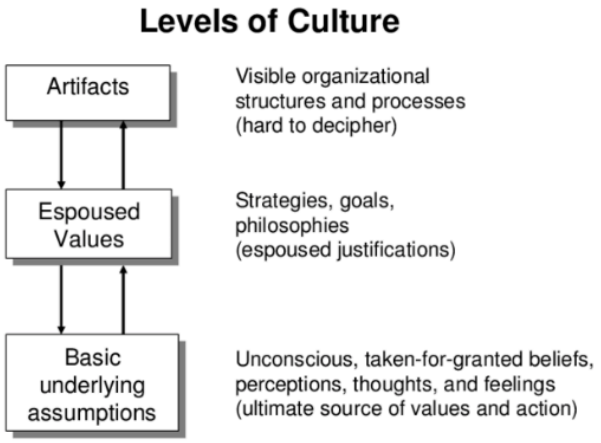
På lik linje med kultur er begrepet organisasjonskultur mye omtalt, og det finnes ingen entydige definisjoner. Skillet mellom den generelle forståelsen av kultur og organisasjonskultur er at sistnevnte oppstår i organisasjoner (Jacobsen & Thorsvik, 2013). En definisjon betrakter organisasjonskultur som *"et system av ideer, symboler og meninger som binder sammen kulturen"* (Bang, 2013, s. 329). Selv om det eksistere forskjellige definisjoner er det likevel én tilnærming til begrepet og forståelsesmodell som har hatt større gjennomslag en andre. Den ble for første gang publisert av Edgar Schein i boken Organizational Culture and Leadership (1987), og har blitt en basis for forståelsen av organisasjonskultur. Edgard Schein (2010) fremhever at organisasjonskultur er mer enn kun det synlige ytre laget i en organisasjon og definerer det som *"a pattern of shared basic assumptions learned by a group as it solved its problem of external adaption and internal integration, which has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems"* (Schein, 2010, s. 18). Denne

definisjonen viser til at kultur ligger på et dypere nivå, utgjør mønstre eller integrering av elementer i et større paradigme som binder de forskjellige elementene sammen.

Schein (2010) forklarer kultur som uhåndgripelig og ubevisst del av en gruppe, og er i liten grad synlig fra utsiden. Når en kultur har utviklet seg er et kjennetegn at den vil dekke hele spekteret av hvordan en gruppe fungerer. Kultur er gjennomgripende og påvirker hvordan en organisasjon takler sine omgivelser, primære oppgaver og interne operasjoner. Ikke alle grupper har kulturer i denne forstand, men kultur assosieres med en gruppes operasjoner på alle organisatoriske nivåer. Schein (2010) forklarer at atferd, verdier, ritualer og klima binder seg sammen til en sammenhengende helhet som stammer fra menneskets grunnleggende behov for å gjøre miljøet vårt mer fornuftig og ryddig. Dette mønsteret eller integreringen er essensen av det vi mener med "kultur". Ledere er opptatt av å utvikle "riktig type kultur", og antyder derfor at kultur har å gjøre med visse verdier som ledere prøver å implementere i organisasjonene sine. I utviklingen av "riktig" kultur ligger det en antagelse om at det eksisterer bedre eller dårligere kulturer, sterkere eller svakere kulturer, og at dette kan påvirke hvor effektive organisasjoner er. Det er vanlig å betrakte en organisasjon bestående av en overordnet organisasjonskultur, og mindre subkulturer i tillegg. Subkulturer er undergrupper av ansatte med kulturelle likhetstrekk (Schein, 2010). Innenfor en slik subkultur vil medlemmene utvikle normer, verdier og virkelighetsoppfatninger som er felles. Det er også slik at organisasjonsmedlemmene kan tilhøre flere subkulturer samtidig (Bang, 2013).

### *2.2.2. Rammeverk for organisasjonskultur*

I følge Schein (1999) er det nyttig å forstå kultur fordi det er et sett med latente og ubevisste krefter som er med på å bestemme verdier, fortolkninger, tankemønstre og individuell og kollektiv atferd. Det er menneskets grunnleggende antakelser som befinner seg "inne i hodet", og det er derfor ikke mulig å studere dette fenomenet direkte. Kultur eksisterer på tre kulturelle nivåer gjennom artefakter, anerkjente verdier og normer og delte underliggende antakelser. De øverste nivåene er mer tilgjengelige og synlige, mens de dypere nivåene er vanskeligere å observere og dermed vanskeligere å vurdere (Schein, 1999).




Figur 1. Levels of culture.
Fra "The corporate culture survival guide: sense and nonsense about culture change," av Schein, 1999, San Fransisco: Jossey-BassInc, s 16.

Artefakter

*Artefakter* er uttrykk for den delen av kulturen som kan observeres. Artefakter kan være både fysiske uttrykk for kultur som for eksempel teknologi, kleskoder og innredning, men også atferdsmessige og verbale uttrykk for kultur. Artefakter vil omfatte synlige organisasjonsstrukturer og prosesser gjennom for eksempel organisatoriske rutiner (Schein, 2010). På dette nivået er kulturen tydelig og har en øyeblikkelig innvirkning for den som observer og kan være både positiv og negativ. Ved å se på artefaktene kan man se hvordan en gruppe konstruerer sitt miljø, og hvilke atferdsmønstre som er synlige blant medlemmene. Likevel er det vanskelig å forstå den underliggende logikken om hvorfor en gruppe oppfører seg slik som den gjør. For å kunne svare på dette spørsmålet må man identifisere hvilke verdier og normer som styrer atferden, og som utgjør det andre nivået i modellen (Schein, 1999).

Anerkjente verdier og normer

Anerkjente verdier og normer er uskrevne regler og prinsipper som er utviklet og fremmet av organisasjonens ledelse. Disse sier noe om hvilken atferd som anses som akseptabel og hva medlemmene anser som viktig (Schein, 2010). Organisasjonens verdier kan eksempelvis bestå av organisasjonens offisielle synspunkter som visjon, kundeløfter, strategidokumenter, personalpolitikk og andre dokumenter som beskriver organisasjonens visjoner, prinsipper verdier og etikk. Et annet eksempel kan være overordnede strategidokumenter som uttrykker

bedriftens samfunnsmessige målsetting og deres ønske om markedsmessig posisjonering. Dette nivået handler ikke om dokumentene i seg selv, og uttrykker dermed ikke selve formuleringene eller de skriftlige dokumentene. Det handler imidlertid om hvordan de ulike verdiene faller sammen i en større helhet hvor alt henger sammen med alt, og dette nivået representeres av summen av disse verdiene. Verdiene reflekterer hvordan bedriften ønsker å fremstå, men det er ikke dermed sagt at organisasjonsmedlemmene handler i henhold til disse (Schein, 1999).

Delte underliggende antakelser

For å virkelig forstå organisasjonskultur og kunne fastslå helheten av gruppens verdier og åpenbare atferd, er det avgjørende at man fordyper seg i delte underliggende antakelsene (Schein, 2010). De delte underliggende antakelsene utgjør selve kjernen i organisasjonskulturen ved at de er avgjørende for medlemmers atferd, holdninger og oppfatninger. Det handler om det som virksomhetens ansatte tar for gitt og som blir betraktet som riktig. Ved å analysere de grunnleggende antagelsene, vil man enklere kunne tyde de observerbare handlingene som organisasjonskulturen gir uttrykk for, og dermed kunne forstå helheten av organisasjonens verdier og atferd. De delte underliggende antakelsene dannes ofte i organisasjonens startfase fordi visse strategier har vist seg å være vellykket. Når strategier basert på spesifikke oppfatninger og verdier fortsetter å være vellykket, vil det gradvis bli tatt for gitt. Verdier, tro og antakelser som har blitt delt og tatt for gitt danner essensen av en organisasjonskultur. Troen, refererer til en gruppe menneskers overbevisning om verden og hvordan den fungerer, mens verdier referer til et samfunns grunnleggende antakelser om hvilke idealer som er verdt å følge. For å beskrive et samfunns grunnleggende antakelser benyttes ofte begrepet "misjon". Dette vekker tanker i retning av livssyn, men er også relevant for andre typer grunnleggende overbevisning som for eksempel hvilke idealer som er verdt å følge (Schein, 1999).

Tilnærminger til kulturbegrepet

Det finnes store variasjoner i tilnærminger til kulturbegrepet, og en rekke kulturforskere er uenige i spørsmålet om kultur er noe en organisasjon *har* eller *er.* Et vanlig skille er å betrakte kulturbegrepet med en funksjonell eller en fortolkende tilnærming. Med en funksjonell tilnærming til organisasjonskultur betrakter man kultur som noe en organisasjon *har*, hvor man antar at kultur kan endres av ledelsen for å tjene organisasjonens interesser. Ønsket med denne tilnærmingen er å finne ut hvordan man kan påvirke og endre kulturen i samsvar med

ledelsesmessige formål (Antonsen, 2009). Schein (1987) kan plasseres innen denne tilnærmingen da hans teori fokuserer på å identifisere underliggende antakelser som påvirker atferden i organisasjonen, for deretter å kunne påvirke kulturen i organisasjonen.

En fortolkende tilnærming betrakter derimot kultur som noe en organisasjon *er*. Det innebærer at organisasjonskulturen skapes gjennom interaksjonene mellom organisasjonsmedlemmene. Denne tilnærmingen handler om hvordan kulturmedlemmene oppfatter verden, fortolker og forstår deres opplevelser. Målet for kulturforskere med en slik tilnærming er å beskrive og tolke kulturen fremfor å endre den, og kritiserer den funksjonelle tilnærmingen for sitt optimistiske syn på kulturell endring. Det er imidlertid få forskere som innehar en ren fortolkende eller funksjonell tilnærming til kulturbegrepet, og de to tilnærmingene representerer derfor to ytterpunkter (Antonsen, 2009). Vår problemstilling handler om hvilken rolle lederstil spiller for informasjonssikkerhetskulturen som medfører at vi til dels inntar en funksjonell tilnærming til kultur.

### *2.2.3. Forholdet mellom organisasjonskultur og informasjonssikkerhetskultur*

Kultur er oppfatninger og verdier som deles av mennesker i en organisasjon (Schein, 1999). Oppfatninger og verdier er begreper som er vanskelig å måle, og det kan derfor være fristende å tenke på kultur som *"måten vi gjør det på her"* eller *"det er det som gjør noen organisasjoner mer suksessfulle enn andre"* (Schein, 1999, s. 15). Imidlertid vil en forenkling av begrepet medføre en manglende forståelse for hva organisasjonskultur er. En bedre måte å se kultur på er derfor å undersøke de forskjellige nivåene som kultur eksisterer på, som forklart i kapittel 2.2.2 (Schein, 1999).

Rammeverket for organisasjonskultur som er presentert i Schein (1987) har blitt bredt akseptert i sikkerhetskulturlitteraturen (Da Veiga & Eloff, 2010; Guldenmund 2000; Niekerk & Solms, 2010; Schlienger &Teufel, 2003; Thang et al., 2016; Thomson et al., 2006). Organisasjonskultur defineres av hvordan ansatte ser organisasjonen og er et kollektivt fenomen som vokser og endrer seg over tid (Schein, 2010). Sikkerhetskultur kan defineres som *"those aspects of the organizational culture that will impact on attitudes and behavior related to increasing or deacreasing risk"* (Guldenmund, 2000, s. 251). Denne definisjonen forklarer at sikkerhetskultur er en del av den overordnede organisasjonskulturen. Alle aktiviteter som gjøres i organisasjonen bør fokusere på informasjonssikkerhet slik at det blir

et naturlig aspekt i den daglige aktiviteten til enhver ansatt. På denne måten kan risikoen forbundet med informasjonssikkerhet minskes. Aktiviteter i den forbindelse kan eksempelvis være at ansatte i banken undersøker og reflekterer over mistenksomme eposter slik at de minsker risikoen for data avveie. En kultur som oppmuntrer ansatte og ledere til å overholde informasjonssikkerhet relatert til å samle inn, bevare, spre og administrerer informasjon kan forbedre informasjonssikkerheten (Thang et al., 2016).

### *2.2.4. Begrepet sikkerhetskultur og informasjonssikkerhetskultur*

Selv om konseptet sikkerhetskultur vokste frem på bakgrunn av Chernobyl-ulykken i 1986 og Piper Alpha i 1988, har det i ettertid blitt omfavnet av sikkerhetslitteraturen for øvrig. Sikkerhetskultur handler om atferd knyttet til sikkerhet, og kan føre til sikkerhetsbrudd som kan være et resultat av individers eller organisasjoners manglende sikkerhetsbevissthet og sikkerhetsatferd. Dette kan skyldes manglende kunnskaper og evne til å foreta riktige beslutninger, eller det kan være handlinger hvor noen bevisst velger å omgå sikkerhetsrutiner og prosesser (Nasjonal sikkerhetsmyndighet, 2014). Litteraturen omtaler begrepene sikkerhetskultur og informasjonssikkerhetskultur om hverandre, og vi vil derfor først redegjøre for ulike definisjoner på sikkerhetskultur, før vi tar for oss informasjonssikkerhetskultur.

Det finnes ingen klar og entydig definisjon av begrepet sikkerhetskultur. De fleste litteraturgjennomganger konkluderer med at konseptet vanligvis refererer til et sett med sikkerhetsrelaterte holdninger, verdier eller forutsetninger som deles mellom medlemmene i en organisasjon (Guldenmund, 2010). I kapittel 2.2.3 om sammenhengene mellom organisasjonskultur og informasjonssikkerhetskultur ble sikkerhetskultur definert som *"those aspects of the organizational culture that will impact on attitudes and behavior related to increasing or deacreasing risk"* (Guldenmund, 2000, s. 251). Dette er en definisjon som er på et mer organisatorisk overordnet nivå. En annen måte er å se sikkerhetskultur som mer spesifikt og menneskelig: *"the product of individual and group values, attitudes, perceptions, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's health and safety management"* (Antonsen, 2009, s. 184). Nasjonale sikkerhetsmyndigheter definerer sikkerhetskultur på en tilsvarende måte som Antonsen (2009): *"summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd"* (Nasjonal

sikkerhetsmyndighet, 2014, s.1). Etter denne definisjonen er sikkerhetskultur et begrep som går på den totale sikkerhetsatferden i virksomheten og inkluderer alle typer risiko.

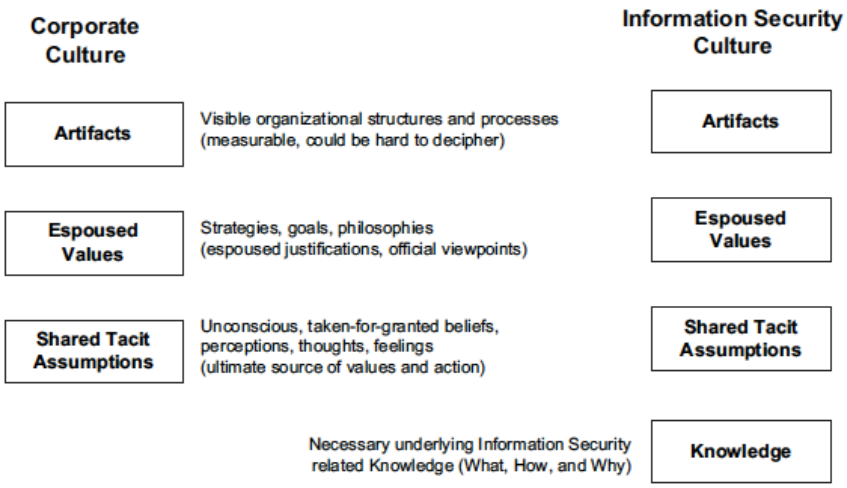
Definisjonene som eksisterer i forhold til informasjonssikkerhetskultur har mange likhetstrekk med definisjonene på sikkerhetskultur, og skillet går i mange tilfeller ved en presisering av at det gjelder informasjon. AlHogail (2015) definerer informasjonssikkerhetskultur slik: *"The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in [an] organization with the aim of influencing employees' security behavior to preserve information security".* Da Veiga og Eloff (2010) forklarer at informasjonssikkerhetskultur utvikler seg på grunn av informasjonsikkerhetsatferd hos de ansatte i organisasjonen, og definerer det som *"the attitudes, assumptions, beliefs, values and knowledge that employees use to interact with the organizations systems and procedures at any point in time. The interaction result in acceptable or unacceptanle behavior (I.e. incidents) evident in artifacts and creations that become part of the way things are done in the organization to protect its information assets. This information security culture changes over time"* (Da Veiga & Eloff, 2010, s. 198). Etter denne definisjonen forklares derfor informasjonssikkerhetskultur som et samspill mellom organisasjonsmedlemmene, informasjonssikkerhetskomponenter og sikkerhetsatferd. Informasjonssikkerhetskomponenter er policyer, retningslinjer, ledelse og styring, og samspillet mellom informasjonssikkerhetskomponenter og atferden til de ansatte vil ha en innvirkning på den resulterende informasjonssikkerhetskulturen. Informasjonssikkerhetskultur tar sikte på å skape en kultur for å sikre informasjonen fysisk og logisk, og omfatter også av lovkrav og forskrifter som går spesifikt på dette med informasjon. Sikkerhetskultur omhandler imidlertid den totale sikkerheten i en virksomhet. Dette vil eksempelvis også inkludere brannvern og ran.

Informasjonssikkerhetskultur kan ses på som en type subkultur ved å si at det er den delen av organisasjonskulturen som retter seg mot informasjonssikkerheten. Organisasjoner har som regel flere subkulturer som eksisterer i ulike grupper i en og samme organisasjon. Sikkerhetskulturen i de ulike gruppene vil kunne være forskjellig, eksempelvis en avdeling. Dette kan belyses med et eksempel. I bankvirksomhet vil kundeservice avdelinge ha en type sikkerhetskultur, mens Compliance avdelingen vil ha en annen sikkerhetskultur. Dette kan blant annet ha noe med påvirkning fra leder og oppfatninger fra ansatte å gjøre, eller forskjeller i arbeidsoppgaver. Ledere har derfor en viktig rolle, ikke bare for å oppnå

organisasjonens vedtatte mål og effektivitet, men også knyttet til sikkerheten på arbeidsplassen. Det betyr at selv om informasjonssikkerheten fremstår som god overordnet i virksomheten, kan det være avdelinger eller grupper som ikke har like god informasjonssikkerhetskultur (Cho, Moon & Amstrong, 2011; Choi, 2016; Da Veiga & Eloff 2010; Guhr & Breitner, 2018; Schein, 1987).

### *2.2.5. Rammeverk for informasjonssikkerhetskultur*

Kulturrammeverket til Schein (1987) forklarer organisasjonskultur generelt. Niekerk og Solms (2010) har derfor bygget videre på dette rammeverket hvor de har lagt til en ny komponent. Nødvendig kunnskap om informasjonssikkerhet kan derfor ses på som et fjerde nivå i Scheins (1987) sitt rammeverk for organisasjonskultur, hvor kunnskap kan skape muligheter for effektiv informasjonssikkerhet. De hevder at tilstrekkelig kunnskaper om hvordan ansatte skal utføre sine normale oppgaver på en sikker måte er et sentralt tema innen informasjonssikkerhet. De understreker også at man ikke kan anta at ansatte har den kunnskapen som er nødvendig for å opprettholde en god informasjonssikkerhet (Niekerk & Solms, 2010).




Figur 2. Level of culture.
Fra «Information security culture: A management perspective,"
av Niekerk, J. F. & Solms, R. V, 2010, Computers & security, s 479.

Artefakter

Artefakter er som nevnt i kapittel 2.2.2 det som faktisk skjer i organisasjonen, og det som er synlig (Schein, 1987). Teknologi er eksempelvis artefakter i denne forbindelse. Disse artefaktene er tydelige som et resultat av informasjonssikkerhetskomponentene som er implementert gjennom for eksempel risikostyring, policyer, retningslinjer, ledelse og styring (Da Veiga & Eloff, 2010). I bankvirksomhet kan for eksempel offentlig nøkkelkryptering identifiseres som en artefakt. Nøkkelkryptering er en teknikk som skal sikre informasjonen mot innsyn eller modifikasjon av uautoriserte (Knapskog & Eilertsen, 2019). Niekerk og Solms (2010) påpeker at uten nødvendige ferdigheter ville det vært umulig å utføre informasjonsrelaterte oppgaver på en sikker måte. For eksempel må de ansatte vite hvordan de skal bruke nøkkelkryptering slik at sensitive personopplysninger er sikret mot innsyn. Organisasjonsmedlemmene må ha tilstrekkelig kunnskap om hvordan de skal utføre arbeidsoppgavene sine på en sikker måte, som en del av arbeidet med å skape en sikkerhetskultur (Da Veiga & Eloff, 2010; Niekerk & Solms, 2010).

Anerkjente verdier og normer

Anerkjente verdier og normer kan som nevnt i kapittel 2.2.2 omfatte strategidokumenter, kundeløfter eller andre dokumenter som beskriver organisasjonens verdier, prinsipper, etikk og visjoner. Disse verdiene og normene vil si noe om hva som er akseptabelt å gjøre og hva organisasjonsmedlemmene anser som viktig. Det handler ikke om dokumentene i seg selv, men den totale verdien (Schein, 1999; Schein, 2010). I forbindelse med informasjonssikkerhet vil anerkjente verdier og normer eksempelvis inkludere utarbeidelse av et policy-dokument. De ansatte må vite hva som skal inkluderes i en slik policy for å kunne adressere organisasjonens sikkerhetsbehov tilstrekkelig (Niekerk & Solms, 2010; Schein, 1999). I banken vil dette eksempelvis inkludere at all programvare som lastes ned fra internett må godkjennes av informasjonssikkerhetsansvarlig, eller at e-poster som inneholder personopplysninger ikke skal sendes i en åpen kanal. De anerkjente verdier er verdier som organisasjonen vil leve opp til, men tolkningen og anvendelsen av disse vil avhenge av et enda dypere nivå av kultur.

Delte underliggende antakelser

Delte underliggende antakelser består som nevnt i kapittel 2.2.2 av ansattes tro og verdier som de deler og som blir tatt for gitt i organisasjonen. Dersom en hendelse kan komme i konflikt med verdiene er det viktig for de ansatte å vite hvorfor en spesifikk kontroll eller

sikkerhetsfunksjon er viktig. Det vil kunne spille en viktig rolle i å sikre etterlevelse av informasjonssikkerheten (Niekerk & Solms, 2010; Schlienger & Teufel, 2003). Delte underliggende antakelser kan representeres gjennom virksomhetens "misjon". For bedrifter som tilsynelatende ikke har annet formål enn å levere økonomisk overskudd, kan "misjonen" være mer skjult. Misjon utgjør de ikke-eksplisitte tankene og følelsene som motiverer og driver individer eller organisasjoner fremover (Schein, 2010). Eksempelvis er kundebehandlere i bankvirksomhet grunnleggende opptatt av service overfor kunden og skape gode økonomiske resultater. Ledere er grunnleggende opptatt av å skape organisatoriske resultater og styringssystemer, mens IT fagarbeidere er grunnleggende opptatt av at systemene som brukes fungerer og er sikre. Det betyr at disse gruppene har ulike misjoner. Bedre samordning må sannsynligvis til for å skape en god informasjonssikkerhetskultur.

Atferd

Etter Schein (1999) sin teori spiller atferd inn på alle de tre nivåene i kulturrammeverket. Atferd handler om hvordan mennesker oppfører seg, deres fysiske handlinger, hvordan de kommuniserer og samarbeider. Dette vil være en ytre presentasjon av virksomhetens indre verdier og prosesser. Atferd består av både det som personer foretar seg fysisk, og gjennom deres synlige tanker, indre refleksjon og følelser. Det å skille mellom personers ytre og indre adferd kan være utfordrende (Schein, 1999). Kulturen utvikler seg på grunn av visse aktiviteter i organisasjonen, for eksempel visjonen vedtatt av ledelsen, og gjennom atferden som ansatte viser på individuelt, gruppe- og organisasjonsnivå (Da Veiga & Eloff, 2010; Robbins, 2001).

Innen informasjonssikkerhetslitteraturen har Da Veiga og Eloff (2010) forankret sin forskning i Schein (1985) og Niekerk og Solms (2010), og tar for seg informasjonssikkerhetskultur med særlig vekt på informasjonsikkerhets atferd. Atferd kan i denne sammenhengen defineres som *"organizational behavior is about what people do in an organisation and how their behaviour affects the performance of the organization* (Da Veiga & Eloff, 2010, s. 198). Informasjonssikkerhetskulturen som utvikles baserer seg på atferden til menneskene som jobber der. Den er tydelig gjennom artefakter som eksempelvis låst dør, verdier som "ansatte er verdifulle ressurser" og mindre tydelig gjennom delte grunnleggende antakelser som eksempelvis kan være at IT-avdelingen er ansvarlige for informasjonssikkerheten i banken (Da Veiga & Eloff, 2010).

Informasjonssikkerhetskomponentene som for eksempel policyer, retningslinjer, ledelse og styring, vil ha en innvirkning på informasjonssikkerhetsatferden i organisasjonen. Sikkerhetsatferden vil i denne sammenhengen være oppførselen som ansatte utviser ovenfor informasjonen de behandler i banken. Målet er å innføre informasjonssikkerhetsatferd som bidrar til beskyttelse av informasjonen basert på bankens informasjonssikkerhetspolicyer, regler og etiske retningslinjer. En slik atferd kan eksempelvis innebære rapportering av sikkerhetshendelser, overholdelse av en klar desk policy eller sikker avhending av fortrolige dokumenter. Med tiden vil denne sikkerhetsatferden utvikle seg til å bli "slik ting gjøres i organisasjonen", hvor det fremmes en kultur der informasjonssikkerhet aksepteres som måten ting gjøres på og en informasjonssikkerhetskultur blir derfor etablert (Da Veiga & Eloff, 2010; Robbins, 2001). Et aktuelt eksempel kan belyse dette. Informasjonssikkerhetspolicyer utarbeidet av ledelsen i banken brukes til å gi ledelsen den nødvendige retning og støtte for informasjonssikkerhet. Målet med en slik policy er påvirke beslutninger, handlinger og atferd hos ansatte. Den spesifiserer videre hvilken atferd som blir sett på som akseptabel og ikke, som for eksempel at en bærbar maskin må være fysisk sikret til enhver tid. Uttalelsen i policyen er rettet mot ansattes oppførsel for å beskytte både den fysiske eiendelen og dataene som er lagret på den bærbare datamaskinen. Målet er å påvirke den ansattes oppførsel når han samhandler med den bærbare datamaskinen for å sikre beskyttelsen. Uten denne erklæringen og lederes håndhevelse av denne, kunne ansatte la bærbare datamaskiner stå usikret. Uten informasjonssikkerhetskomponenter for å dirigere og påvirke ansattes atferd, kan ansatte samhandle med informasjon på måter som kan føre til risiko. Med tiden kan denne potensielt skadelige oppførselen føre til en kultur der svikt blir sett på som akseptabelt (Da Veiga & Eloff, 2010; Robbins, 2001).

For å oppnå et akseptabelt nivå av informasjonssikkerhet, bør organisasjoner sikre at et omfattende og adekvat sett med informasjonssikkerhetskomponenter blir implementert. Dette settet med komponenter hjelper til med å adressere trusler på et menneskelig, prosess- og teknisk nivå som vil fremme etableringen av en informasjonssikkerhetskultur i organisasjonen. Organisasjoner skal videre sikre at medarbeiderens samhandling er i tråd med kravene i informasjonssikkerhetspolicyen og retningslinjene. Disse kravene kan være relatert til handlinger som å ta sikkerhetskopi til serveren på daglig basis, passordbeskyttet informasjon om flyttbare medier eller slette uønskede e-postmeldinger med vedlegg (Da Veiga & Eloff, 2010; Robbins, 2001). Da Veiga & Eloff (2010) forklarer videre at informasjonssikkerhetskomponentene implementeres på individ, gruppe eller organisatorisk

nivå av informasjonssikkerhetsatferd. På det individuelle nivået forholder seg til individer i organisasjonen og deres egenskaper. Egenskapene kan for eksempel være alder eller sivilstand, personlighetskarakteristikker, verdier, og holdninger og grunnleggende antagelser. Disse egenskapene kan påvirke individers oppførsel med hensyn til overholdelse av retningslinjer for informasjonssikkerhet.

Informasjonskomponentene på gruppenivå fokuserer på atferden til mennesker i grupper og hvordan gruppene fungerer. Det er viktig for ledelsen å betrakte ansatte som medlemmer av en gruppe, eksempelvis en avdeling, og å bruke avdelingen til å etablere et akseptabelt nivå for informasjonssikkerhetskultur. På gruppenivå kan en avdelings syn eller press overstyre det individuelle synet. Det kreves et sterkt lederskap for å veilede en avdeling eller annen gruppe til å ta den riktige beslutningen og å overholde selskapets policyer. På organisasjonsnivået legges formelle strukturer til, for eksempel å avgjøre om organisasjonen opererer på en sentralisert eller desentralisert måte (Da Veiga & Eloff, 2010; Robbins, 2001). I en svært sentralisert organisasjonsstruktur vil toppleder ta alle avgjørelser, mens i en desentralisert organisasjonsstruktur vil sakene i større grad avgjøres av ansatte (Jacobsen & Thorsvik, 2013). Disse strukturene implementeres av organisasjonens ledelse og vil påvirke ansattes holdninger og ha en innvirkning på deres atferd. Informasjonssikkerhetskulturen som utvikler seg er forskjellig for hver organisasjon. Det påvirkes både av den overordnede organisasjonskulturen, men også av bedriftsspesifikke informasjonssikkerhetskomponenter. Dersom ansatte synes innholdet i informasjonssikkerhetspolicyen og retningslinjene er vanskelig å forstå eller anser det for ikke å være relevant for deres arbeid, er det ikke sikkert at de overholder det. På denne måten vil Informasjonssikkerhetskomponenten (policy) som er implementert være ineffektiv og slik at ansatte selv kan utgjøre en potensiell trussel for informasjonssikkerheten. I et slikt tilfelle må policyen følgelig justeres (Da Veiga & Eloff, 2010; Robbins, 2001).

Kunnskap

Kunnskap blir lagt til som et fjerde nivå av kultur som er spesifikt for en informasjonssikkerhetskultur. Denne tilpasningen er nødvendig fordi man ikke kan anta at ansatte og ledere har den nødvendige kunnskapen som behøves når den teknologiske utviklingen skjer så raskt. Kunnskap om informasjonssikkerhet vil støtte og påvirke hvert av de tre andre nivåene i Schein (1987) sitt rammeverk, men ved å ha kunnskap som et tilleggsnivå viser man effekten av kunnskap eller mangel på kunnskap kan ha på den

generelle informasjonssikkerhetskulturen. Informasjonssikkerhet kan ikke oppnås uten tilstrekkelige kunnskaper, og dermed må man inkludere kunnskapsnivået (Niekerk & Solms, 2010).

Kunnskap kan defineres som *"information combined with experience, context, interpretation and reflection. It is a higher-value form of information that is ready to apply to decisions and actions"* (Davenport, De Long & Beers, 1998, s. 43). Denne definisjonen forklarer kunnskap som informasjon kombinert med erfaringer, kontekst, tolkning og refleksjon. Dette vil gi informasjonen en høyere verdi som mennesker kan bruke til å ta beslutninger og uføre spesifikke handlinger. Det innebærer at den menneskelige faktoren i informasjonssikkerhet består av to interrelaterte dimensjoner som er kunnskap og atferd. På grunn av sammenhengen mellom disse to dimensjonene er det ikke mulig å ignorere virkningen mangel på kunnskap om informasjonssikkerhet kan ha på en organisatorisk subkultur som informasjonssikkerhet (Niekerk & Solms, 2010).

Ansatte og ledere må ha nødvendig kunnskap for å være i stand til å behandle informasjon på en sikker måte. De må forstå sine roller og sitt ansvar gjennom opplæring i hvordan de skal kunne beskytte informasjonen i organisasjonen. Dermed må informasjonssikkerhets praksiser være en del av organisasjonskulturen, da denne legger begrensninger på aktivitetene og atferden til de ansatte (Thomson, Solms & Louw, 2006). Dette betyr at beskyttelse av informasjon må være en naturlig del av de ansattes og lederes atferd og deres daglige aktiviteter. Det er langt mer effektivt med en kultur som fremmer hensiktsmessig informasjonssikkerhets atferd gjennom kunnskap, artefakter, verdier og antagelser enn å pålegge organisasjonsmedlemmene en viss type atferd gjennom regler. Informasjonssikkerheten er god dersom ansatte og ledere har kjennskap til, forstår og aksepterer de nødvendige forhåndsreglene og tiltakene (AlHogail, 2015). Likevel påpekes det at den menneskelige faktoren blir oversett, og at et av de største problemene når det gjelder beskyttelse av informasjon er mangel på kunnskap, ferdigheter og forpliktelse blant ansatte (Niekerk & Solms, 2010; Thomson et al., 2006).

Kunnskapen ledere og ansatte tilegner seg gjennom opplæring vil påvirke deres bevissthet og atferd forbundet med informasjonssikkerhet (Nikerk & Solms, 2010; Safa & Solms, 2016). Flores & Ekstedt (2016) forklarer at ledere og ansatte kan være bevisst over trusler relatert til informasjonssikkerhet basert på tidligere erfaringer eller interesse, eller ved å gjennomgå

spesifikk opplæring om retningslinjer. Det vil da gjøre de mer oppmerksom på hvordan akseptabel bruk av IT-systemer og tjenester er beskrevet i organisasjonens policy, eller hvordan sensitiv og konfidensiell informasjon skal behandles. Da Veiga og Eloff (2010) påpeker imidlertid at det kan være krevende å få større mengder med informasjon om sikkerhetsretningslinjer. Enkelte ansatte kan oppleve informasjonen som vanskelig å forstå eller lite relevant for deres arbeid. Dermed er det viktig med opplæring av ny teknologi og retningslinjer som ansatte må forholde seg til, slik at de får den oppfølging de trenger. For at ansatte skal tilegne seg riktig kunnskap om informasjonssikkerhet er det også viktig at lederne er klar over det (Da Veiga & Eloff, 2010). Safa og Solms (2016) argumenterer for at sikkerhetsbevissthet er en viktig faktor som kan redusere risikoen forbundet med brudd på informasjonssikkerhet i organisasjoner. Mer kunnskap kan derfor redusere usikkerheten til ansatte slik at de ikke velger lette passord eller trykker på linker de ikke burde fordi de er redde for å miste tilgangen til viktig informasjon (Norsis, 2016, s. 8; Safa & Solms, 2016.). Det å ha lite kunnskap kan også føre til at ansatte bruker samme passord på flere nettsider som krever innlogging. I banken benyttes det e-læringskurs for at ansatte og ledere skal kunne tilegne seg ny kunnskap om informasjonssikkerhet. Poenget med kursene er at ansatte skal bli tryggere på nett og være mer obs på hva de kan møte på i sin arbeidshverdag som kan være en trussel for virksomheten.

I forhold til bedriftens sikkerhetsarbeid og de kontinuerlige forbedringsprosessene er det også viktig at bedriften sørger for innrapportering av avvik. Organisasjonens evne og vilje til å utvikle seg og lære av feil, hendelser og ulykker er essensielt for å oppnå en god informasjonssikkerhetskultur (Reason, 1997). Gjennom sin hendelseslogg som nevnt i kapittel 2.1.1 om informasjonssikkerhet oppmuntrer ledelsen ansatte til å rapportere avvik for å sikre kontinuerlig læring i organisasjonen. Kontinuerlig forbedring kan bety at den underliggende policyen må endres, og det er derfor viktig for banken å forstå årsaken til det som oppleves og få innspill på hva som skal til for å hindre at det oppstår igjen (Reason, 1997).

## *2.3. Leder og informasjonssikkerhetskultur*

I informasjonssikkerhetslitteraturen er det flere som mener at leder har en viktig rolle for utviklingen av en sikkerhetskultur (Antonsen, 2009; Da Veiga & Eloff, 2010; Niekerk & Solms, 2010; Reason 1997; Thang et al., 2016). Transaksjon- og transformasjonsledelse

benyttes i informasjonssikkerhetslitteraturen. Transaksjonsleder handler om at leder identifiserer ansattes behov og bruker belønning for passende innsats og ytelse (Bass 1985). Transformasjonsledelse står i kontrast til transaksjonsledelse, hvor leder kan øke bevisstheten til ansattes tanker om gode resultater og se på deres individuelle behov. Vi vil først ta for oss en begrepsavklaring av ledelse og leder, og deretter ta for oss de to lederstilene (Bass 1985).

### *2.3.1. Definisjon av ledelse og ledere*

Ledelse kan sees på som en av den viktigste faktoren for om en organisasjon lykkes eller ikke lykkes (Bass & Stogdill, 1990). Leder kan defineres som *"en spesiell atferd som mennesker utviser i den hensikt å påvirke andre menneskers tenkning, holdning og atferd"* (Jacobsen & Thorsvik 2013, s. 416). Ledere vil forholde seg til bedriftens hovedmål og sette delmål for de ansatte slik at en skal kunne nå hovedmålet i et langtidsperspektiv. Vi skal se på de menneskelige aspektene ved ledere på mellomleder nivå, og undersøke hvordan de arbeider med informasjonssikkerhet og informasjonssikkerhetskultur (Jacobsen & Thorsvik, 2013; Stogdill, 1950).

## *2.4. Transformasjonsledelse*

Transformasjonsledelse er en del av den moderne ledelsesteorien og har blitt benyttet i forbindelse med informasjonssikkerhetsforskning (Choi, 2016, Flores & Ekstedt, 2016, Guhr & Breitner, 2018). Ledelsesformen transformasjonsledelse ble opprinnelig foreslått av Burns i 1978 for politiske omgivelser. Bass (1985) brukte konseptet til Burns om transaksjonsledelse og transformasjonsledelse om virksomheter. Transformasjonsledelse ble sett på som det motsatte av transaksjonsledelse og bevegde seg utover transaksjoner for å øke bevisstheten til ansattes tanker om gode resultater og for å se på deres behov. Videre oppmuntres de ansatte til å overgå egeninteresse og gjøre det som er best for gruppen (Bycio, Hackett og Allen, 1995). Bass (1985) definerer transformasjonsledelse slik: "*transformational leadership — occurs when leaders broaden and elevate the interests of their employees, when they generate awareness and acceptance of the purposes and mission of the group, and when they stir their employees to look beyond their own self-interest for the good of the group"*(Bass, 1990, s. 21). Dette betyr at lederen skaper bevissthet rundt arbeidsoppgaver og får ansatte til å se konsekvenser. Transformasjonsledelse består av fire grunnelementer som er idealisert

innflytelse, inspirerende motivasjon, intellektuell stimuli og individualisert oppmerksomhet. De fire i´ene tar for seg forskjellige lederansvar, men sammen vil de sørge for at leder kan hjelpe ansatte i sitt arbeid som total sett er best for gruppen, og føre til det beste for virksomheten (Cho et al., 2011; Choi 2016; Da Veiga & Eloff 2010; Guhr & Breitner, 2019). De fire i ´ene kan bidra til en positiv atferdsendring siden de helhetlig legger vekt på hva som motiverer og påvirker ansatte, og ved at lederen går frem som en rollemodell for de ansatte og skaper bevissthet (Avolio et al., 2003; Ghur & Breitner, 2018). Det er viktig å påpeke at det å skape bevissthet på informasjonssikkerhet ved transformasjonsledelse ikke nødvendigvis vil føre til atferdsendringer (Jäger, 2018).

### *2.4.1. Idealisert innflytelse*

Idealisert innflytelse kan også ses på som en type karismatisk ledelse og er et kjent begrep innen transformasjonsledelse (Bass 1985; Burns 1978). Karismatisk handler i denne sammenhengen om å skape tillit til ansatte. Idealisert innflytelse legger vekt på at lederen inspirerer ansatte til å yte mer, og fremstår som en synlig rollemodell (Avolio, Bass & Jung, 1999). Lederen tar hensyn til sine ansatte og lytter til deres behov. Ansattes behov settes ofte foran lederens behov, og dette vil dermed skape tillit, respekt og beundring fra ansatte. Lederen deler risikoen med de ansatte og følger opp med underliggende etiske prinsipper og verdier (Avolio & Bass, 1994; Avolio et al, 2003). I tillegg inspirerer lederen ansatte med ideen om at de kan oppnå store ting i bedriften med ekstra innsats (Bass, 1990). Transformasjonsledelse er preget av karisma og visjon, og vellykkede ledere har en høy evne til å spesifisere viktigheten av å ha en sterk følelse av formål for å vise sin overbevisning i sine idealer, tro og verdier (Thite, 2000). Denne ledelsesformen er i enkelte artikler trukket frem som en god lederstil når en virksomhet skal implementere ny teknologi (Thite, 2000; Cho et al., 2011). Det vil da handle om at lederen går frem som et godt forbilde ved implementering av ny teknologi.

Ledere som er engasjerte i informasjonssikkerhet vil ha et større grunnlag for å skape mer bevissthet rundt sikkerhetssystemer (Bass et al., 2003; Hwang & Wakerfield; Kim & Kim 2019). Det er derfor viktig at lederen gjenkjenner medarbeiderens behov og bygger relasjoner med de ansatte (Bass, 1990). Det er viktig at ledere er gode rollemodeller slik at informasjonssikkerheten kan videreføres til de ansatte (Soomro, Shah & Ahmed, 2016). Implementering av nye informasjonssikkerhetsregler eller policyer kan by på utfordringer for

de ansatte dersom de må gjøre arbeidsoppgavene sine på en ny måte. Dette kan føre til atferd som motarbeidelse og tanker om at man ikke ønsker en slik endring (Leidner & Kayworth, 2006). Det er derfor viktig at lederen klarer å arbeide for å unngå slike motforestillinger mot endring eller sørge for at de ansatte likevel klarer å omstille seg. En sikkerhetskultur utvikler seg ofte på bakgrunn av atferden til de ansatte. Det er derfor viktig med en god relasjon mellom leder og ansatt (Da Veiga & Eloff, 2010). Atferd som leder utviser i forbindelse med informasjonssikkerhet handler ofte om å jobbe med forebyggende tiltak som opparbeidelse av en god sikkerhetskultur (Straub & Welke, 1998).

### *2.4.2. Inspirerende motivasjon*

Inspirerende motivasjon handler om at lederen motiverer de rundt seg ved å skape en mening bak arbeidet og kommer med utfordringer som skaper entusiasme og optimisme. Dette sørger for en individuell drivkraft og en lagånd i forbindelse med arbeidsoppgaver (Avolio et al., 2003; Bass 1985). Disse lederne klarer å uttrykke viktige formål og arbeidsoppgaver på en enkel måte til de ansatte slik at de kan strekke seg mot målene og visjoner for virksomheten (Bass, 1990; Hetland, 2004). En leder som er inspirerende trenger ikke å være karismatisk, da de bygger relasjoner til ansatte gjennom tillitt og positiv tilbakemelding som skaper entusiasme (Avolio et al., 2003; Avolio & Bass, 2004; Bass 1985).

Ifølge Hao og Padman (2016) vil ledere som tar i bruk ny teknologi eller standarder motivere sine kollegaer til å ta det i bruk. På denne måten kan leder gå frem som et godt eksempel og påvirke de ansatte til å gjøre det samme basert på deres relasjon og tillit. I en informasjonssikkerhetskultur er det viktig å holde seg oppdatert ved å tilføre ny kunnskap for både ledere og ansatte. Derfor er det viktige at ledere er optimistiske til nye sikkerhetstiltak og klarer å inspirere de ansatte til å følge de nye tiltakene (Niekerk & Solms, 2010). Det er slik at handlingen lederen gjør for å skape bevissthet og motiverer ansatte vil kunne endre bevisstheten ansatte har til informasjonssikkerheten (Flores & Ekstedt, 2016). På enkelte arbeidsplasser arbeides det ofte i grupper og dermed er det viktig at lederen ser at gruppen forholder seg korrekt til informasjonssikkerhetspolicyer og retningslinjer for å opprettholde informasjonssikkerhetskulturen. Leder må motivere gruppen til å arbeide for virksomhetens sikkerhetsmål. Det er derfor viktig at leder kommer med tilbakemelding når de ansatte følger sikkerhetsmål og retningslinjer, og når de ikke gjør det (Da Veiga & Eloff, 2010). Dette med sikkerhetsmål knyttet til informasjonssikkerhet har vært lite forsket på tidligere (Ghur &

Breitner, 2018; Hu, Dinev, Hart & Cooke, 2012). Det kan være fordi ledere tenker at IT-avdelingen har kontroll på dette område slik at lederen ikke fokuserer på det (Hu et al., 2012).

### *2.4.3. Intellektuell stimuli*

Intellektuell stimuli innebærer at leder stimulerer den ansattes innsats til å være nyskapende og kreativ ved å stille spørsmål om antagelser, omformulerer problemstillinger og bruke gamle situasjoner til å løse nye problemer. Det er ingen latterliggjøring av gruppe eller individuelle feil. Nye ideer og kreative løsninger blir vurdert av medarbeidere som er med på å løse de problemene som skulle oppstå (Avolio et al., 2003; Bass, 1990). Intellektuell stimuli er ikke like følelses preget som de to andre elementene (Bass, 1985).

Under dette elementet er det slik at lederen kan stille spørsmål om hvor mye av organisasjonens ansatte som har av kunnskap om informasjonssikkerhetskultur. Ansatte kan ha mer kunnskap enn nødvendig, kun det som er nødvendig eller mindre enn det som er nødvendig (Niekerk & Solms, 2010). Det kan også være slik at enkelte ansatte stiller spørsmål ved informasjonssikkerheten i organisasjonen og da vil det være viktig at en leder kan bidra med å svare på dette. Det at ansatte er kritiske og stiller spørsmål til informasjonssikkerheten kan være med til å bidra til at sikkerheten i virksomheten blir bedre på lang sikt. Når det kommer nye sikkerhetsregler vil kurs og opplæring av ansatte og ledere være nødvendig (Da Veiga & Eloff, 2010). Under en opplæringssituasjon vil det komme mange spørsmål. Enkelte ledere vil velge å svare på disse spørsmålene med hver enkelt, mens andre ledere velger å ta slike spørsmål plenum. Når spørsmålene blir tatt opp i plenum er det viktig at ansatte føler at de kan spørre om sikkerhetsreglene uten å oppleve å bli hengt ut eller føle på skam på grunn av manglede forståelse (Ghur & Breitner, 2018). I en slik situasjon kan en leder bruke eksisterende kunnskap om sikkerhet for å forklare de nye endringene. Dette kan for eksempel være nye krav om behandling av personopplysninger, men at mye av den gamle måten å gjør ting på eksisterer i den nye. Derfor kan en leder påpeke hva som er nytt og hva som inngår i det nye som er kjent fra tidligere (Bass, 1985).

### *2.4.4. Individualisert oppmerksomhet*

Individualisert oppmerksomhet handler om at lederen tar hensyn til ansattes personlige behov, prestasjon og utvikling. Lederen vil fungerer som en mentor for de ansatte. Et kjennetegn er at alle ansatte behandles likt, og lederen tar hensyn til individuelle behov og ferdigheter. Leder sørger for at ansatte utvikler sitt indre og beste potensial i virksomheten. Det etableres ett støttende miljø der det skapes læringsmuligheter hvor individets ønsker eller behov blir akseptert (Avolio et al., 2003; Bass, 1990; Bass 1985).

Når det kommer nye sikkerhetsregler, kan de være vanskelig å forstå reglene og hvor ansatte ser på innholdet som lite relevant. Dersom reglene er lite relevante vil de ikke overholdes av ansatte. Dermed er det viktig at en transformasjonsleder behandler enkelt individer ulikt avhengig av deres behov og ferdighet (Avolio et al., 2003; Da Veiga & Eloff, 2010). Det er viktig at lederen har en støttende atferd, slik at den ansatte skal kunne tilegne seg kunnskap på deres måte. Ny kunnskap kan for eksempel være nye retningslinjer som kommer i personvernloven. Når det kommer nye regler er det viktig at leder tar dette opp i plenum eller bruker andre metoder for å lære de ansatte om dette. Det er viktig at leder er til stede for ansatte dersom noen er usikre på det som står i reglene eller loven de må forholde seg til. Dersom ansatte skulle bryter loven eller har manglende kunnskap, vil det i verste fall føre til alvorlige konsekvenser for bedriften. Derfor vil det være viktig at en leder er til stede for ansatte og hjelper de som har spørsmål. Atferden til de ansatte vil kunne påvirke informasjonssikkerhet i form at ansatte har forskjellige personlige egenskaper. Noen jobber effektivt og ønsker å få gjennomført mest mulig i løpet av en dag, mens andre ansatte tenker seg ofte flere ganger om de gjør ting (Avolio et al., 2003; Da Veiga & Eloff, 2010).

## *2.5. Transaksjonsledelse*

Transaksjonsledelse står som nevnt i kontrast til transformasjonsledelse (Bass, 1985). Denne lederstilen kan defineres som *"those leaders who identified the needs of their followers and exchanges rewards for appropriate levels of effort and performance were viewed as transactional leaders"* (Allen, Bycio & Hackett, 1995 s. 468; Bass, 1985). Det vil si at lederen identifisere behovene til sine ansatte og gir belønning for passende innsats og prestasjon. Et kjennetegn ved denne lederstilen er at ansatte ofte handler i frykt for straff

(Avolio & Bass, 2004). De sentrale faktorene i denne lederstilen er betinget belønning, ledelse ved unntak (aktivt), ledelse ved unntak (passivt) og Laissez faire (Avolio et al, 2003). Vi har valgt å gå bort fra betinget belønning og vil derfor legge hovedfokuset på de tre andre ledelsesformene. En transaksjonsleder har egenskaper som sørger for overholdelse av regler og rutiner som vil fremme en sikkerhetsatferd hos ansatte (Humaidi & Balakrishnan, 2015).

### *2.5.1. Ledelse ved unntak (aktiv)*

Denne lederstilen kan defineres som *"fokusere på å overvåke utførelsen av arbeidsoppgaven for å ha oversikt over eventuelle problemer som kan oppstå, og korrigere disse problemene for å opprettholde nåværende prestasjonsnivå i virksomheten"* (Avolio, Bass & Jung, 1999, 445). Det vil si at lederen følger med på sine ansatte, og griper inn når det oppstår avvik fra regler og rutiner. Det forventes at lederen aktivt styrer ansatte og spesifiserer viktige standarder eller instrukser som skal overholdes. Dersom disse standardene ikke overholdes, vil den ansatte risikere å bli straffet eller få en advarsel av lederen. Dersom det skulle oppstå avvik eller feil vil leder raskt gripe inn og rette opp feilen (Avolio et al., 2003). En leder med denne lederstilen vil sikre at ansatte følger regler og rutiner, vil gripe inn ved sikkerhetsavvik og få kontroll over en eventuell situasjon (Antonakis et al., 2003; Guhr & Breitner, 2018).

### *2.5.2. Ledelse ved unntak (passiv)*

Det som kjennetegner denne lederstilen er at leder griper inn i situasjoner dersom regler eller standarder ikke blir fulgt. Ledelse ved unntak (passiv) defineres som at lederen *"griper inn når standardene ikke er oppfylt"* (Bass, 1990, s. 22). I sin mer passive form vil lederen vente på at de oppstår problemer før det iverksettes tiltak eller ikke gjøres noe med (Avolio et al., 2003). På grunn av dette kombineres den jevnlig med Laissez-faire lederstilen (Avolio et al., 1999). Essensen med denne lederstilen er at lederen først griper inn når det har skjedd et sikkerhetsbrudd eller et brudd på regler og rutiner i virksomheten (Antonakis et al., 2003). Et annet kjennetegn er at ledere gir mye ansvar til ansatte i bestemmelse av hvilke sikkerhetstiltak de skal foreta seg. Denne lederatferden er forbundet med at ansatte i mindre grad etterlever de organisatoriske informasjonssikkerhetsregler og policyer. Det har vist seg at virksomheter med en mellomledelse som ikke er opptatt av informasjonssikkerhet, må finne

andre måter å kommunisere viktigheten av sikkerhetsatferd til de ansatte (Guhr & Breitner, 2018).

### *2.5.3. Laissez-faire-lederstil*

Laissez-faire omtales også som destruktiv lederatferd. I motsetning til desktruktiv lederatferd omhandler laissez-faire kun det som er forbundet med passivitet. Denne lederstilen kan defineres som en *"unngår ansvar og beslutninger"* (Bass, 1990, s. 22). Et kjennetegn ved denne lederstilen er at leder verken er opptatt av ansatte eller oppgaver (Bass, 1990). Laissez-faire ledere unngår avtaler, avklarer ikke mål eller forventninger til de ansatte. De retter ikke opp i uventede situasjoner som har oppstått, og unngår bevisst å ikke ta ansvar om beslutninger knyttet til deres rolle (Bass, 1990). Det er først når det fremkommer feil eller avvik de velger å gjør noe med problemet. Denne ledelsesformen er ofte sitert som en ikke eksisterende ledelse (Avolio et al., 2003). Lederen unngår å ta beslutninger, sier fra seg ansvar og bruker ikke sin autoritet, og ansatte må selv lære fra sine informasjonssikkerhetsfeil. På denne måten kan det føre til brudd på sikkerhetsreglementet og rutinene (Antonakis et al., 2003).

## *2.6. Leders rolle i informasjonssikkerhetskulturen*

Leder har en viktig rolle for utviklingen av en sikkerhetskultur (Antonsen, 2009; Da Veiga & Eloff, 2010; Niekerk & Solms, 2010; Reason 1997; Thang et al., 2016). Kultur og strukturer er sammensatt og påvirker hverandre ved å identifisere og skape de nødvendige komponentene for deretter å sette de sammen til en helhet (Reason, 1997). Målsetninger, oppfatninger, antagelser og verdier stammer fra kulturen, og det er viktig at leder kommuniserer dette til ansatte. For å kunne formidle målsetninger og verdier må leder være tydelig og vise vei mot organisasjonsmålet (Schein, 1987.; Schein & Schein, 2017). Kultur er noe som endres, og det er viktig at leder går frem som et godt forbilde. Informasjonssikkerhetsregler eller policyer kan gi nødvendige retningslinjer for lederens styring mot en informasjonssikkerhetskultur (Da Veiga & Eloff, 2010). Ledere bør derfor engasjere seg ved å vise støtte og ansvar til informasjonssikkerhet ved lovmessige og dokumenterte policyer (Thomson et al., 2006). En leder som skaper bevissthet rundt regler og policyer kan redusere trusler og reagere om det oppstår uønskede hendelser (Flores & Ekstedt,

2016). Ledere har derfor en viktig rolle for å oppnå organisasjonens overordnede mål, men også tilknyttet informasjonssikkerhet.

Transformasjonsleders rolle til informasjonssikkerhetskultur

Ifølge Choi (2016) kan en sterkt idealisert innflytelse, inspirerende motivasjon, intellektuell stimuli og individualisert oppmerksomhet fra leder føre til at ansatte i større grad etterlever informasjonssikkerhetspolicyer og retningslinjer. Transformasjonsledere vil støtte ansatte slik at de føler seg trygge på informasjonssikkerhet. På denne måten kan transformasjonsledere bedre etterlevelsen av informasjonssikkerhet på arbeidsplassen (Cho et al. 2011). Det å se på andre, og oppfatte at ledelsen deltar aktivt ved implementeringen av nye sikkerhetssystemer eller sikkerhetsregler og går frem som et godt forbilde, vil fungere som en idealisert innflytelse på ansatte og andre ledere. For å få ansatte og andre ledere til å bruke og etterleve systemet eller reglene forsøker lederne å motivere og inspirere de ansatte (Avolio et al., 2003; Hwang et al., 2019). Engasjerte ledere av informasjonssystemer har evnen til å skape et sterke forhold til bevissthet rundt informasjonssikkerhet (Hwang et al., 2019).

Et kjennetegn ved transformasjonsledere er at de er åpne for endring. Når teknologien stadig er under utvikling er det viktig å ha en leder som er åpen for endring av virksomhetens informasjonssikkerhetskultur (Choi, 2016; Guhr & Breitner, 2018; Thite, 2000). Utdanning og opplæring av ledere og ansatte påvirker informasjonssikkerheten positivt. Det argumenteres med at når miljøer innen informasjonsteknologi endres raskt må ledere lære seg de kunnskapene og ferdighetene som er nødvendig for å sørge for en god informasjonssikkerhet ved å unngå nye trusler (Choi, 2016). Siden informasjonsteknologien endrer seg så raskt, kreves det at ansatte og ledere utfører en innsats utover vanlige forventninger (Bass, 1985; Choi, 2016). Transformasjonsledelse har vist seg å være en effektiv lederstil for å endre ansattes atferd etter hvert som informasjonssikkerheten endrer seg. Når leder har egenskaper som kan endre atferd, blir det enklere å oppnå gruppens og bedriftens mål (Guhr & Breitner, 2018). Ledere kan også være nøkkelen til å lykkes med å forhindre eventuelle misbruk av informasjon, og gjennom opplæring kan lederen forebygge slikt misbruk (Choi, 2016; Straub & Welke, 1998). Lederstil kan på denne måten spille en positiv rolle for informasjonssikkerhetskulturen, særlig i forbindelse med å påvirke de delte underliggende antakelsene i kulturrammeverket til Schein (1987). For eksempel er kundebehandlere i bankvirksomhet grunnleggende opptatt av service ovenfor kunden og skape gode økonomiske resultater, det er deres misjon som driver de ansatte fremover (Schein, 2010). Dersom ledere

støtter og hjelper de ansatte til å føle seg trygge på informasjonssikkerhet og motiverer de til å fokusere på dette som en del av arbeidsoppgavene sine og stimulerer de til å bli nyskapende og løse ting på en ny og sikker måte, vil det kunne bli en del av deres misjon (Choi et al., 2016; Schein, 2010).

Transaksjonsleders rolle til informasjonssikkerhetskultur

De tre underelementene av transaksjonsledelse innebærer at leder enten kan overvåke sine ansatte for å unngå sikkerhetsbrudd, gripe inn først etter det har oppstått, eller unngå å gripe inn i situasjonen (Avolio et al, 2003; Guhr & Breitner, 2018). En leder som har kvaliteter av laissez-faire eller ledelse ved unntak passiv forventer at ansatte lærer av sine feil for å forhindre at det samme skal skje igjen. I informasjonssikkerhetssammenheng vil det si at ledere gir ansatte ansvar for å bestemme hvilke sikkerhetstiltak som passer til deres situasjon, og vil på denne måten ikke bidra til etterlevelse av regler og rutiner (Ghur & Breitner, 2018). Dersom ansatte ikke ønsker å lære av sine feil vil det gå utover sikkerhetsstandarden og etterlevelsen av policyer. En leder med kvaliteter av ledelse ved unntak aktiv vil sikre at ansatte følger regler og rutiner, og vil gripe inn ved sikkerhetsavvik og få kontroll over en eventuell situasjon (Antonakis et al., 2003; Guhr & Breitner, 2018). På denne måten vil leder bidra til etterlevelse av regler og rutiner.

Ledere mangler i mange tilfeller kunnskap og bevissthet om hvilke sikkerhetstiltak de kan ta i bruk for å minske risikoen forbundet med informasjonssikkerhet. Risikoer kan styres eller reduseres når ledere er klar over hele risikoområdet som er tilgjengelig, og dermed implementere de mest effektive tiltakene. Ifølge Straub og Welke (1998) mangler imidlertid lederne i mange tilfeller denne kunnskapen, og deres påfølgende handlinger for å takle risiko er derfor mindre effektive enn den kan være. Det underliggende problemet er at mange ledere ikke er kjent med arten av risiko, noe som kan føre til ubeskyttede systemer og dårligere informasjonssikkerhet (Straub & Welke, 1998). Ledere som har en laissez-faire lederstil kan velge å skyve ansvaret over på ansatte, og på denne måten vil de ikke bli kjent med de risikoene som eksisterer (Ghur & Breitner, 2019). Problemet med at mange organisasjoner er lite sikret mot trusler mot deres informasjonssystemer er fordi mange ledere ignorerer problemet og er naive i deres svar på denne økende trusselen (Antonakis et al., 2003; Guhr & Breitner, 2018).

# 3. Metode

Valget på kvalitativ eller kvantitativ forskningsmetode bestemmes ut fra metoden som egner seg best til det du skal undersøke. I en forskningsprosess er det slik at forskningsspørsmålet legger grunnlaget for hvilken metode som er best egnet til å genere informasjon i forskningsprosessen (Creswell & Poth, 2018). De teoretiske rammene adresserer forskningsproblemer som eksempelvis betydningen av enkeltpersoner eller grupper sine sosiale eller menneskelige problem. Kvalitativ tilnærming er derfor nyttig å bruke fordi innsamling av data er en naturlig prosess som tar hensyn til mennesker og stedene som studeres. En dataanalyse er både induktiv og deduktiv som etablerer mønster eller tema. Dataanalysen vil representere informantenes meninger, og vil forme en sammensatt beskrivelse og tolkning (Creswell & Poth, 2018; Creswell, 2013).

## 3.1. Valg av forskningsmetode

Tidligere forskning på informasjonssystemer hadde et teknisk fokus. Dette fokuset flyttet seg på 1980-tallet seg til styring av informasjonssystemer. På 1990-tallet utvidet fokuset seg betydelig fra styring av informasjonssystemer til forholdet mellom informasjonssikkerhet og organisasjoner som helhet. Informasjonssikkerhet har som studieretning blitt utvidet til å omfatte spørsmål som kommunikasjon, samarbeid mellom mennesker og organisasjoner, interorganisatoriske systemer, elektronisk handel og internett (Myers & Avison, 2002; Orlikowski & Scott, 2008). Litteraturen om informasjonssikkerhet, informasjonssikkerhetskultur og lederstil har dannet teorigrunnlaget i avhandlingen. Det skal gi oss og leserne en oversikt over de teoretiske perspektivene som eksisterer på området. I tillegg vil det også gjøre det lettere for oss å oppdage nye momenter eller fenomener som de teoretiske perspektivene ikke nevner.

Kvalitative forskningsmetoder er spesielt passende for å sette forskere i stand til å studere sosiale og kulturelle fenomener. De er designet for å hjelpe oss til å forstå mennesker og de sosiale og kulturelle sammenhengene de lever i. I tillegg påpeker informasjonssikkerhetslitteraturen at det et behov for kvalitativ forskning på informasjonssikkerhet (Crossler et al., 2013; Myers & Avison, 2002). Casestudier kan være en effektiv metode for å skape en forståelse av den faktiske motivasjonen og atferden som

ligger til grunn for informasjonssikkerhetsatferden til individene i organisasjonen (Crossler et al., 2013). Kvantitativ metode forsøker å svare på «hva»-spørsmål, og vil gi en deskriptiv forståelse av fenomenet (Savin-Baden & Major, 2013). For vår problemstilling ville en slik tilnærming kun gitt en overflatisk forståelse av hvordan ledere forholder seg til informasjonssikkerhet i banknæringen i dag. En kvantitativ undersøkelse vil dessuten ikke i like stor grad avdekke underliggende menneskelige elementer om informasjonssikkerhet som kunnskap, atferd, lederstil og kultur.

Avhandlingen tar sikte på å utforske fortolkninger, meninger, oppfatninger og synspunkter rundt leders rolle relatert til informasjonssikkerhetskultur. På grunn av sikkerhetshendelser i ulike virksomheter har argumentet om leders betydning for informasjonssikkerheten blitt løftet frem. En kvalitativ tilnærming ble dermed ansett som egnet for å avdekke dette.
For å oppdage dypere kulturelementer er det nødvendig å snakke med folk for å avklare hvilke normer og verdier de har til felles. De kulturelle nivåene i kulturrammeverket (Niekerk & Solms, 2010; Schein, 1987) vil påvirke hverandre, og når man forstår hva artefaktene betyr kan man forstå de to andre nivåene bedre (Jacobsen & Thorsvik). Det var dermed behov for en åpen og fleksibel tilnærming som kvalitativ metode kan gi, samt oppnå en dybdeforståelse for temaet og på denne måten kunne besvare problemstillingen (Jacobsen 2000). Vår problemstilling er som nevnt innledningsvis: *"Hvilken rolle spiller lederstil for informasjonssikkerhetskulturen i bankvirksomhet?"*

Spørsmålet om man skal ha en stram og mer deduktiv tilnærming, eller løst og mer induktiv tilnærming til det teoretisk rammeverk til Dubois og Gadde (2002) er ikke enten eller, men kan være en kombinasjon. Dersom man ønsker å "avdekke" fenomenet man er interessert i vil en induktiv og utforskende tilnærming være mest passende. Det som kjennetegner en løs tilnærming er at det eksisterer en vek teori, og sentrale begreper er uklare eller manglende (Dubois & Gadde, 2002). Begrepene lederstil, informasjonssikkerhet og informasjonssikkerhetskultur har godt fotfeste i eksisterende teori.
Informasjonssikkerhetskultur er imidlertid et mer umodent begrep i den form at det kun har eksistert i 20 år, og det er derfor naturlig at dette er fenomener som er forsket mindre på enn lederstil. Spørsmålet om man skal ha en induktiv eller deduktiv tilnærming knytter seg derfor til hvordan temaet tradisjonelt har blitt forsket på, og hvilke faktorer som utpeker seg i vår egen studie (Johanessen et al., 2011).

Det finnes to vitenskapsteoretiske hovedretninger, som er positivistisk og fortolkende. Den positivistiske tilnærmingen går ut på å betrakte virkeligheten som ekstern, objektiv og uavhengig av sosiale aktører. Den andre hovedretningen er fortolkende og forklarer virkeligheten som sosialt konstruert, subjektiv, multippel i endring (Savin-Baden & Major, 2013). Et perspektiv innenfor den fortolkende retningen er sosialkonstruktivisme som innebærer at menneskers virkelighetsforståelse betraktes som kontinuerlig formet av sitasjoner de befinner seg i og deres opplevelser som er knyttet til hvem de kommuniserer med. De sosiale fenomenene anses ikke som konstante eller funksjonelle, men gjennom fortolkninger og sosial samhandling vil de formes og omformes (Savin-Baden, 2013). Ettersom avhandlingen forsøker å kartlegge og beskrive informasjonssikkerhetskultur og lederstil i en norsk bank, vil den kunne beskrives som fortolkende. Det vil si at den sosiale verden er tolket og opplevd fra innsiden (Savin-Baden & Major, 2013).

## *3.2. Valg av forskningsdesign og strategi*

Case-studie

En case-studie kan defineres som en *"empirical methode that investigates a contemporary phenomenon within its real-life context, especially when – the boundarioes between phenomenon and contexts may not be clearly evident"* (Yin, 2018, s. 15). Case-studier er spesielt egnet når det stilles spørsmål som "hvordan" eller hvorfor" om et sett av samtidige hendelser som forskeren har lite eller ingen kontroll over (Yin, 2018). Definisjonen legger føring for at case-studier er egnet til å studere fenomenet i en "real life setting" og avdekke mangfold av likheter og forskjeller (Yin, 2018). Vår studie er gjennomført i en bank hvor problemstillingen er basert på lederstil og informasjonssikkerhetskultur. Vi som forskere har liten eller ingen påvirkning eller kontroll over informasjonssikkerhetskulturen i denne banken.

Den største fordelen med case-studier er at de tillater forskeren å gå i dybden av en enhet, og dermed komme frem til detaljerte og inngående beskrivelser av et fenomen (Yin, 2018). Det er viktig å avgjøre hva eller hvem som skal studeres da valg av case i stor grad avhenger av forskningsspørsmål. I en case-studie vil det være hensiktsmessig å benytte etablert teori knyttet til det fenomenet som skal studeres (Yin, 2018). Case-studier kan deles inn i utforskende, forklarende og deskriptive (Yin, 2018). Vi har valgt en kombinasjon av deskriptiv og utforskende case. Deskriptiv case illustrerer og beskriver hva som kjennetegner

transformasjonsledere og laissez faire ledere. Vi har så valgt en til dels utforskende og eksplorerende tilnærming som skal gi oss en forståelse av hvilken rolle lederstil spiller for informasjonssikkerhetskultur (Yin, 2018). Vi stiller dermed en del åpne spørsmål, som vi kommer tilbake til under beskrivelse av datainnsamlingsmetode, men har også brukt en del faktorer vi etter eksisterende teori antar at kan ha en innvirkning. Det som er karakteristisk for en case-studie er at den har fleksibelt design som gjør det mulig å endre forskningsspørsmål og datainnsamlingsmetoder underveis ettersom studien utvikler seg (Yin, 2018).

Embedded single case

Når målet er å studere en helt vanlig case og det representerer en "everyday situation" kan man bruke enkeltcase design (Yin, 2018). Vi ønsker å studere en bank slik fenomenene lederstil og informasjonssikkerhetskultur utspiller seg fra et nåtidsperspektiv. Embedded single case innebærer at man forsker på flere analyseenheter som er en del av casen. Det må med andre ord være en del av den originale casen (Yin, 2018). I vårt tilfelle har vi et samarbeid med en norsk bank som vil representere casen, mens vi vil sammenligne to avdelinger innad i banken. Vi skal forske på informasjonssikkerhetskulturen i en norsk bank, hvor denne kulturen kan utspille seg på ulike måter i de to avdelingene (Schein, 1987).

Triangulering

innebærer at man kombinerer forskjellige perspektiver som kan avdekke svakheter hver for seg. Dersom de ulike perspektivene peker i forskjellig retning er det en indikasjon på at perspektivene har skjevhet, men om de peker i samme retning kan dette indikere at resultatene har høy validitet (Yin, 2018). Typisk vil triangulering involvere bekreftende bevis fra forskjellige kilder for å belyse et tema eller et perspektiv for å se etter mønstre av tanker og atferd (Creswell & Poth, 2018). Ifølge Eisenhardt (1989) vil triangulering føre til at man får sterkere støtte for funnene sine. I vår studie har vi hentet beviser fra ulike kilder. Vi har gjennomført en dokumentanalyse av lover og policyer knyttet til informasjonssikkerhet, i tillegg til å intervjue IT- avdelingen om hvordan de forholder seg til dette. Dette for å kartlegge det første nivået i Schein (1987) sitt kulturrammeverk. Deretter har vi forsøkt å få et bilde på ulike meninger, oppfatninger og tolkninger av begrepene informasjonssikkerhet og informasjonssikkerhetskultur, samt hvilken rolle lederstil kan ha for informasjonssikkerhetskulturen. I den forbindelse intervjuet vi to mellomledere i hver sin avdeling og ansatte i avdelingene. Med dette får vi flere perspektiver på informasjonssikkerhetskulturen i virksomheten og hvordan lederne forholder seg til den. På

denne måten vil vi få bekreftelse eller avkreftelse fra forskjellige perspektiver ved å spørre de samme spørsmålene til forskjellige typer ansatte i virksomheten.

## *3.3. Datainnsamlingsmetode*

### *3.3.1. Dokumentanalyse*

Et startpunkt for datainnsamlingen og som bakgrunn for utarbeidelsen av en intervjuguide kan det være nyttig med en dokumentanalyse. Det kan også gi flere tilleggsopplysninger som er med på å spesifisere og verifisere data. Uten et godt grep om de mulige problemene, kan man gå glipp av viktige ledetråder og ikke vite når et avvik var akseptabelt eller til og med ønskelig (Yin, 2018). Styrker ved dokumenter som kilde er at det er stabil informasjon som man kan ta frem så ofte det trengs, og de inneholder detaljert og eksakt informasjon (Savin-Baden & Major, 2013). I vår studie har det vært relevant å starte med en dokumentanalyse av informasjonssikkerhetsrelaterte lovkrav og standarder. En svakhet ved dokumentanalyse er imidlertid at de er vanskelig å finne og få adgang til (Savin-Baden & Major, 2013). Vi fikk ikke tilgang til bankens egne rutiner og policyer som gjorde det vanskelig å få en fullgod dokumentanalyse. Derfor måtte vi i tillegg til dokumentanalysen intervjue IT avdelingen for å få svar på dette. Formålet med intervjuene og dokumentanalysen var å danne det første nivået (artefaktene) i rammeverket for informasjonssikkerhetskulturen vi forsøker å få en forståelse for. Dette gjorde det enklere å lage gode og relevante spørsmål til intervjuene vi foretok med ledere og ansatte.

### *3.3.2. Intervju*

Ifølge Yin (2018) er det ikke en bestemt måte å samle inn data i casestudier. Når imidlertid nye situasjoner, uforutsette hendelser eller nye momenter kan dukke opp anses intervju som en god innsamlingsmetode. Intervju som metode er kritisert med argument om mangel på standardisering av informasjonen som kan påvirke kvaliteten på forskningen gjennom reliabilitet og subjektivitet. Likevel påpeker andre at strukturen i selve datainnsamlingen ikke avgjør kvaliteten på kvalitativ forskning, men at det er den analytiske strukturen i forskerens hode (Weich, 1989). I denne studien vil intervju gi tilgang til observasjoner, innsikt og kunnskap som kvantitative spørreundersøkelser ikke hadde fanget opp. Intervjuer som

innsamlingsmetode er nødvendig for å få en dyp forståelse av informasjonssikkerhetskulturen og for å unngå misforståelser i forbindelse med personlige meninger (Schlienger & Teufel, 2003). Utfordringer knyttet til intervju som innsamlingsmetode er at vi er avhengig av å stille gode spørsmål som informantene ikke misforstår. Det kan også være slik at informantene kan være forutinntatt, uærlige i sine svar, husker feil, eller svarer det som det som han eller hun tror er forventet (Savin-Baden & Major, 2013). Styrken ved å benytte intervju er at vi får tilgang til mye informasjon på kort tid som gjør det enklere å fokusere direkte på problemstillingen og forskningstemaet. Direkte kontakt med informanten kan gi god innsikt i informantenes erfaringer (Savin-Baden & Major, 2013).

Problemstillingen og forskningsspørsmålet har naturlig nok lagt føringer for valg av teori og således for utarbeidelsen av spørsmål i intervjuene. Vi benyttet åpne individuelle intervjuer som datainnsamlingsmetode. Denne metoden var en egnet metode ettersom vi var ute eller meninger og tolkninger omkring lederstil og informasjonssikkerhetskultur (Jacobsen, 2000). Av hensyn til at vi skulle spørre spørsmål som omhandlet hvordan ledere forholder seg til informasjonssikkerhet anså vi dette som et sensitivt tema. Fokusgruppeintervju ble derfor ansett som mindre egnet for vår problemstilling.

Ifølge Savin-Baden og Major (2013) er det fire forskjellige måter å strukturere en intervjuprosess: strukturert, semistrukturert, ustrukturert og uformell. Strukturerte intervjuer handler om at intervjueren følger et manus der akkurat de samme spørsmålene blir stilt til hver av informanten ved å bruke akkurat de samme ordene. Noen ganger kan spørsmålene være mer åpne, men stort sett er de standardiserte. Denne prosessen kan sette begrensninger på informasjonen vi får fra informantene når spørsmålene er fastsatt. På grunn av dette er det anbefalt å bruke en av de andre prosessene (Savin-Baden & Major, 2013). En ustrukturert prosess har et mål og en plan, hvor intervjueren kan still spontane spørsmål i tilknytning til teorien eller en spesifikk kontekst. Spørsmålene har ofte en tendens til å være åpne om et spesifikt tema som krever stor respons fra informanten. Denne metoden brukes ofte når forskeren har god forståelse om temaene og har en klar agenda. Det kreves ofte flere intervjuer med samme informant som vil ta mye tid. Derfor vil ikke denne være best egnet for oss siden vi har begrenset med tid (Savin-Baden & Major, 2013). Den uformelle prosessen handler om å snakke med mennesker på fagområdet uten en strukturert intervjuguide. Denne metoden tar ikke opp intervjuer på lydbånd, og alt er basert på notater og hukommelse. Denne metoden blir ofte brukt i en observasjonsprosess og når det er lite litteratur på fagområdet. I

vårt tilfelle vil denne metoden være lite relevant siden den er best egnet til observasjon (Savin-Baden & Major, 2013).

Semistruktur handler om at forskeren ikke bare følger fastsatte spørsmål, men også kommer med oppfølgingsspørsmål til informantenes reaksjon eller kommentarer. Intervjueren kan stole på guiden og stiller spørsmål som dekker temaer og kan avvike fra guiden om det skulle være behov. Dataene ble derfor innsamlet ved bruk av semi-strukturerte intervju med åpne spørsmål. Fordelen med semi-strukturerte intervjuer er at det ga oss mulighet til å stille oppfølgingsspørsmål for å få mer utfyllende svar når det var ønskelig (Savin-Baden & Major, 2013). En styrke ved denne metoden er at forskere kan bestemme hvordan de ønsker å bruke den begrensede tiden. Spørsmålene er også åpne nok til at intervjuobjektene kan uttrykke sine perspektiver på et emne eller tema samtidig som det gir rom for å sammenligne data på tvers av informantene. En svakhet ved semistrukturerte intervjuer er at de ikke alltid gir informantene muligheten til å tilby sitt eget unike perspektiv slik som gjennom et ustrukturert intervju (Savin-Baden & Major, 2013). I vårt tilfelle har vi begrenset med tid til å gjennomføre intervjuene slik at denne metoden vil gi oss det beste grunnlaget for å kunne samle inn god data i vår studie. Denne prosessen har selvfølgelig vært med på å forme intervjueguiden i tillegg til å forbedre oss til intervjuene.

### *3.3.3. Utvalg*

For å få en forståelse av bankens informasjonssikkerhetskultur har det vært naturlig å intervjue ledere, ansatte og IT-avdelingen siden kultur er oppfatninger og verdier som deles av mennesker i en organisasjon (Schein, 1999). Utvelgelsen av informanter ble i stor grad gjort ved hjelp av "snøballutvelgelsesmetoden", der vi tok kontakt med enkelte personer i banken som henviste oss videre til personer som de trodde kunne komme med god kunnskap og innsikt omkring fenomenene (Grønmo, 2004). Vi bestemte oss ikke for et bestemt antall informanter i forkant, men vurderte antallet i forhold til dataene vi samlet inn. Når det oppsto "metning" i datamaterialet, det vil si at flere informanter ikke ville generere mer informasjon om fenomenet, var det ikke nødvendig å intervjue flere (Kvale, Brinkmann, Anderssen og Rygge, 2009). Det totale antallet informanter ble til slutt 16 stykker fordelt på tre avdelinger. De tre avdelingene var markedsavdelingen, produksjonsstøtteavdelingen og IT-avdelingen.

## *3.4. Gjennomføring av datainnsamlingen*

Det har vært krevende å få gjennomført studiet på grunn covid-19. Etter en del venting, planlegging og samtaler med banken fikk vi gjennomført studiet. Vi har valgt å dele gjennomføringen inn i forberedelser, gjennomføring, transkribering og dataanalyse. Dette er et kapittel som tar for seg alt vi har gjort.

### *3.4.1. Forberedelser*

Vi hadde et møte med banken tidligere på året der vi avklarte hvordan vi ønsket å gjennomføre studiet og fikk generell informasjon. På grunn av covid -19 fikk vi god hjelp av banken til å komme i kontakt med et utvalg informanter. Vi fikk kontaktopplysninger til de mest relevante kandidatene og sendte raskt ut en e-post med informasjon om forskningen. På grunn av omstendighetene sendte vi ut en samtykkeerklæring (vedlegg 1) på e-post der den ble lest igjennom og underskrevet før Skype intervjuene ble gjennomført. Før vi gjennomførte intervjuene utviklet vi intervjuguiden slik at vi fikk samlet inn dataene på en effektiv måte.

Intervjueguiden

Før vi begynte på intervjuguiden var vi klar over at vi måtte utvikle tre forskjellige spørreskjemaer siden vi skulle intervjue ledere, ansatte og IT-avdelingen. Det er tre forskjellige avdelinger med forskjellig kunnskap. Derfor ble det viktig for oss å lage spørsmål tilpasset de ulike avdelingen slik at det var enklere å forstå og svare på i de forskjellige gruppene. Det var også viktig for oss å formulere spørsmål som kunne gi oss gode data. Vi utformet introduksjonsspørsmål som skulle gjøre informanten komfortabel slik at det ville være enklere å komme med mer kompliserte spørsmål i selve intervjuet (Savine-Baden & Major, 2013). Det som var viktig for oss i utviklingen av intervjuguiden var å bygge tillitt, legge til rette for at informanten skulle kunne åpne seg og komme med egne oppfatninger om informasjonssikkerheten i banken og lederoppgave tilknyttet sikkerheten. Det var viktig for oss å utvikle spørsmål som handlet om informasjonssikkerhetskultur for å få et bilde av hvordan hver informant tenker om teamet. De sentrale kjennetegnene for informasjonssikkerhetskultur som artefakter, anerkjente verdier og normer og delte underliggende antakelser var vesentlig å få med seg i intervjueguiden. Vi formet også sentrale spørsmål om transformasjonsledelse som også ville kunne gi oss svar på transaksjonsledelse.

Vi har blitt inspirert fra Multifactor Leadership Questionnaire på enkelte av spørsmålene Avolio og Bass (2004). Vi ønsket å ha mest mulig åpne spørsmål for å unngå å virke ledende. Vi delte inn i innledningsspørsmål, teamabaserte spørsmål og avsluttende spørsmål. I de temabaserte spørsmålene hadde vi åpne spørsmål og noen detaljerte spørsmål for å kunne se dypere på forståelsen til informanten. Vi forberedte oppfølgingsspørsmål som vi skulle stille dersom vi ønsket mer utdypning eller refleksjon. Avslutningsspørsmål ble stilt hvor hensikten var å få frem informantenes egne erfaringer eller om de forslag til forbedringer tilknyttet informasjonssikkerhet (Savine-Baden og Major, 2013).

### *3.4.2. Gjennomføring*

Intervjuene ble avtalt med informantene og ble gjennomført over Skype business på grunn av covid-19. Dette var praktisk for begge parter og informanten befant seg i trygge omgivelser på hjemmekontor. Dette satte selvfølgelig noen begrensninger for oss ved at det var vanskeligere å foreta observasjoner ved en videosamtale så dette ble i mindre grad vektlagt. Vi opplevde noen ganger å bli kastet ut av Skype business siden vi bare hadde gjestebruker, men vi klarte å fortsette intervjuet etter et lite opphold. Intervjuene varte i gjennomsnitt i 40-45 minutter med avbrudd. Intervjuene bar preg av samtaleform, og spørsmålene ble tilpasset den enkelte informanten og det som opptok informanten. Vi klarte å dekke alle temaene i intervjuguiden gjennom å hoppe litt frem og tilbake avhengig av svarene. Alle intervjuene ble tatt opp på opptak, og ble gjennomført på fire dager. Vi valgte å fordele de 16 intervjuene ved å bytte på som intervjuere annenhver gang, mens den andre tok notater og kom med oppfølgingsspørsmål. Det var lettere for den som ikke ledet intervjuet å stille oppfølgingsspørsmål eller oppdage temaer som informanten ikke snakket om. Den som ikke stilte spørsmålene, fikk også bedre oversikt over hva slags spørsmål som informanten hadde besvarte tidligere. Det var også slik at den personen også hadde bedre oversikt når vi ble kastet ut av Skype business.

### *3.4.3. Transkribering*

Før vi begynte å transkribere utviklet vi en transkripsjonsnøkkel etter Du bois-systemet. Vi har ikke fulgt alt som eksisterer i Du bois-systemet, men det som har vært av vesentlig betydning for oss (Du Bois, 1991). Vi fordelte transkriberingsarbeidet mellom oss, og

systemet ble tatt i bruk for å sikre at vi foretok transkriberingen på lik måte. Det var også viktig å anonymisere personene gjennom å nummere de fra 1 til 16, i tillegg valgte vi å skrive alle intervjuene på bokmål. Vi delte de 16 intervjuene på to og tok fatt på den tidkrevende oppgaven. Noen av utfordringene som dukket opp under transkriberingen var at informanten tok seg lange pauser midt i en setning, hvor noe meningen kunne forsvinne. Vi opplevde også tilfeller av ufullstendige setninger, og at dialekt kunne ha en innvirkning. Gjennom transkriberingen kunne vi øke validiteten ved å kvalitetssikre våre egne tolkninger (Kvale et al., 2009).

## *3.5. Dataanalyse*

Datanalyse handler om å gjøre dataene analyserbare, og redusere risikoen for å miste relevant informasjon. Yin 2018 mener at datanalysen er det vanskeligste aspektet ved case-studier og at det ikke finnes noen standardiserte metoder for å gjennomføre dette. Videre besto dataanalysen av underkategorier, organisering og systematisering av tekstmaterialet (Yin, 2018). Hvilken type dataanalyse som benyttes vil være avhengig av hvilken type casestudie som gjøres og hva som er hensiktsmessig. Yin (2018) presenterer to generelle analysestrategier som vil være relevant for vår avhandling. Den første analysestrategien baseres på å arbeide med dataene du har ved å se mønstre i datamaterialet, og er en induktiv strategi. Den andre vil være en analyse som er basert på de teoretiske antakelsene og er en deduktiv strategi. Denne studien er basert på en kombinasjon av disse to strategiene. Dette vil i analysen gi oss mulighet til å knytte data til de teoretiske antakelsene, og finne nye ting vi eller teorien ikke har tenkt på forut for studien.

<u>Koding og kategorisering</u>

Koding er en teknisk øvelse som går ut på å redusere informasjonen som er innhentet fra intervjuene (Savin-Baden & Major, 2013). I kodingsprosessen er formålet å hente ut den viktigste informasjonen som skiller seg ut i datamaterialet. Det er viktig å være fleksibel i kodingsprosessen slik at det ikke blir en mekanisk prosess der kategoriene er for lite reflektert (Johannesen, Christoffersen & Tufte, 2011). Faren ved å redusere data gjennom koding er at data blir løsrevet fra den konteksten de er samlet i, skapt i eller utviklet fra. Data fra case-studier kommer fra kontekster og dataene er uløselig knyttet til disse, og i utgangspunktet nedfelt i en bestemt sammenheng (Creswell & Poth, 2018). I Embedded case-studie er det

vanlig å begynne med åpen koding og deretter ta for seg axial koding (Creswell & Poth, 2018). Kodene kan være enten datadrevne eller teoridrevne, eller en kombinasjon. Åpen koding vil være datadrevne og vil gradvis dukke opp under datainnsamlingen, mens axial koding vil være teoridrevne og basere seg på det konseptuelle rammeverket (Miles, Huberman & Sadana, 2014). I vår analyse har derfor vi benyttet åpen koding etterfulgt av axial koding. Vi valgte å bruke NVivo 12 i kodingsprosessen, som gjør kategoriseringen av datamateriale enklere og mer effektivt.

I en åpen koding vil forskeren gå gjennom datamaterialet linje etter linje, og krever en konseptualisering av alle relaterte hendelser som resultere i flere konsepter. Åpen koding er første runde hvor begreper og kategorier identifiseres i datamaterialet (Savin-Baden & Major, 2013). Det første vi gjorde i kodingsprosessen var å se etter kategorier eller temaer som skilte seg ut i datamaterialet. Ettersom vi finner kategorier eller tema tildeles dataene en beskrivende etikett som fanger betydningen av hvert datasegment. Dette gjør det lettere å sammenlikne og identifisere mønster som vil forenkle analyseprosessen. Forskere repeterer normalt prosessen for alt av relevant data som blir markert med samme etikett (Savin-Baden & Major, 2013).

De kategorier som utpekte seg gjennom åpen koding tas videre under axial koding for å identifisere sentrale fenomener. Deretter må det identifisere hva som kan forårsake fenomenet, og se på den spesifikke konteksten og de mellomliggende forholdene i fenomenene (Creswell & Poth, 2018). Det finnes en rekke måter å lage en spesifikk kode, og hvordan forskeren velger å kode kan være basert på flere ulike tilnærminger. Koder kan eksempelvis være deskriptive, fortolkende eller mønster. Deskriptive koder tilordner etiketter til data for å oppsummere i et ord eller en kort setning (Miles et al., 2014). Mønsterdrevne koder er koder som reflekterer forklaringer, slutninger, sammenhenger og identifiserer sentrale temaer (Savin-Baden, 2013).

## *3.6. Kvalitet*

Bevissthet rundt etiske dilemmaer, og håndtere kilder og datagrunnlag på en grundig måte er viktig i kvalitativ forskning. Kvaliteten på forskningen knyttes til troverdighet og overførbarhet (Thagaard, 2013). I mange forskningsprosjekter er det ikke mulig å gjenta

studiet på eksakt samme måte og validitet er derfor et stort metodisk problem. En av årsakene til at studiene ofte ikke kan gjentas er fordi fenomenene forandrer seg, samt at resultatene fra forskningsprosessen er formet av forskerens subjektive fortolkninger og utvelgelse av empiri (Yin, 2018). I det følgende vil det redegjøres for reliabilitet, begrepsvaliditet, intern validitet og ekstern validitet. Forskerrollen og etiske vurderinger forbundet med studien vil også redegjøres for.

### *3.6.1. Relabilitet*

Reliabilitet knytter seg til om forskningen er utført på en pålitelig og tillitsvekkende måte. Det referer seg til spørsmålet hvorvidt en annen forsker som anvender samme metode, ville kommet til samme resultat (Thagaard, 2013). I case-studier betyr det at man studerer samme case om igjen, og ikke bare replikerer resultatet av originalcaset ved å studere ett nytt case (Yin, 2018). Det forankrer seg i nøyaktigheten av undersøkelsens data, hvilke data som brukes, den måten de samles inn på og hvordan de bearbeides (Johannesen et al., 2011). En god retningslinje for å gjøre case-studier er derfor å gjennomføre forskningen slik at en annen i prinsippet kan gjenta prosedyrene og forhåpentligvis oppnå samme resultat (Yin, 2018). Vi har forsøkt å sikre reliabiliteten ved å redegjøre for hvordan dataene har blitt utviklet i løpet av forskningsprosessen. Videre har vi gitt en inngående beskrivelse av konteksten som vi ønsker å oppnå ved å presentere oss selv og studien vår.

Når vi spør informantene spørsmål som handler om informasjonssikkerhet og informasjonssikkerhetskultur, kan det være de svarer ut fra hvordan de ønsker å fremstå, og ikke hvordan de egentlig ville håndtert en situasjon. Spørsmålene som handler om leders rolle relatert til informasjonssikkerhet kan for enkelte virke som sensitive. Dette har vi forsøkt å unngå ved å skape en samtale med en god atmosfære som gjør at informanten svarer med egne meninger. Det er også en mulighet for at informantene misforstår ett eller flere spørsmål. Spørsmålene tilknyttet begrepene kan være vanskelig for informantene å svare på, og det er grunn til å regne med at informasjonssikkerhetskultur er et begrep enkelt ansatte ikke har hørt om. Dette har vi forsøkt å løse ved å forklare hva vi legger i begrepene for dem slik at de har anledning til å svare. Dessuten har vi testet intervjuene på utenforstående for å se etter muligheter for forskjellige tolkninger av spørsmålene. Dette er mulige feilkilder ved metoden som kan påvirke reliabiliteten i avhandlingen, som gradvis kan gå ut over validiteten

(Thagaard, 2013). Reliabilitet eller pålitelighet er en forutsetning for å sikre validitet eller troverdighet som vi skal redegjøre for i det følgende.

### *3.6.2. Validitet*

Begrepsvaliditet

Begrepsvaliditet knytter seg til hvor troverdig forskningen er (Thagaard, 2013). Begrepsvaliditet handler om å skape troverdighet rundt datainnsamlingen og den empirien man finner. Enkelt case-design har sin styrke i form av høy intern validitet. Det er derfor viktig at vi ivaretar validiteten gjennom forskningsprosessen. Kritikken om casestudier omhandler at forskeren feiler i å utvikle et tilstrekkelig operasjonelt sett med tiltak, og at forskerens "subjektive vurderinger", de som har en tendens til å bekrefte forskere forutinntatte forestillinger. Vi har benyttet oss av allerede eksisterende definisjoner av de sentrale begrepene for å sikre begrepsvaliditeten. En god begrepsvaliditet vil si at vi og informantene samt de som skal lese oppgaven vil få samme forståelse av begrepene (Thagaard, 2013). Ved å definere de sentrale begrepene i teorifundamentet har vi gjort rede for hva vi legger i begrepene slik at det blir forståelig for leseren. Vi har sørget for dette ved å definere begrepene slik at det passer med formålet bak studien, samt funnet måter vi kan måle konseptene våre på (Bass, 1985; Niekerk & Solms, 2010; Schein, 1987). I tillegg har vi presentert var forståelse for de enkelte begrepene for informantene i intervjuene etter at de selv gir en redegjørelse for begrepene. Med dette sikrer vi at alle legger samme forståelse til grunn for begrepene informasjonssikkerhet og informasjonssikkerhetskultur. Kvaliteten på de svarene vi har fått vil påvirke reliabiliteten i denne undersøkelsen.

Ekstern validitet

Ekstern validitet vil si at man vil etablere funn som kan bli generalisert til andre lignende tilfeller. Det behandler problemet med å vite om funnene til en studie er generaliserbare utover den umiddelbare studien. Ekstern validitet innebærer at den forståelsen vi utvikler innenfor vår oppgave, også kan være relevant i andre situasjoner. Målet med oppgaven er at tolkningen skal være relevant utover det enkelte prosjektet (Thagaard, 2013). Det er utfordrende å sikre god ekstern validitet eller generaliserbarhet i kvalitati v forskning, fordi det ved enkeltcasedesign kun forskes på en virksomhet eller en gruppe. Vi har kun 16 informanter fordelt på flere analyseenheter og en enkelt case og det kan dermed være vanskelig å anse undersøkelsen som overførbar til andre casestudier (Creswell &Poth, 2018).

Thagaard (2013) mener derimot at hvordan case-studier utformes har en sammenheng med muligheter for at resultater av studien har gyldighet i andre sammenhenger. Vi har blant annet forsøkt å sikre ekstern validitet gjennom å sørge for reliabilitet (Thagaard, 2013).

### *3.6.3. Etiske vurderinger*

I løpet av forskningsprosessen må forskere vurdere hvilke etiske spørsmål som man kan møte, og planlegge hvordan disse problemene må adresseres (Creswell & Poth, 2018). Særlig i forbindelse med datainnsamlingen vil etiske problemstillinger være viktig å tenke på, da det berører mennesker (Johannessen et al., 2011). I det følgende vil det gjøres rede for forskningsetiske og juridiske retningslinjer som anses som relevante for denne studien.

I denne studien studerer vi et samtidsfenomen, og som forskere har et vi ansvar for å beskytte informantene (Yin, 2018). Når en begynner er det viktig å forklare formålet med studien for deltakerne. Dette har vi sørget for ved å sende et informert samtykke til hver informant i forkant av intervjuprosessen hvor vi gjorde rede for hva intervjuet ville innebære, at det var frivillig og uten risiko for deltakeren (Creswell & Poth, 2018). En god forsker skal strebe etter de høyeste etiske standardene mens han forsker. En feil som kan gjøres i forbindelse med casestudier er at man i forskerrollen forsvarer en bestemt orientering til problemene, eller en bestemt holdning til det som skal studeres (Yin, 2018). Det kan eksempelvis innebære at man som forsker farges av sine tidligere antakelser eller kunnskap om emnet, og lar det påvirke svarene fra informantene. Det kan innebære at man som intervjuer ser bort fra noe en informant sier fordi man tror ordene blir uttalt utydelig, men egentlig så er det slik at det ikke gis nok oppmerksomhet fordi de ikke passer til forestillingene (Yin, 2018). I fasen under analysen av dataene er det viktig å ikke avsløre bare de positive resultatene, men få med alle perspektivene slik at det komplekse bildet av det sentrale fenomenet kommer frem. Videre er det ved rapportering av dataene viktig å sørge for at bevis, funn og konklusjoner er korrekte som blir kommunisert på en tydelig måte, og uten å røpe informasjon som kan skade informantene (Creswell & Poth, 2018).

# 4. Analyse

Dette er en enkeltcasestudie med to analyseenheter hvor problemstillingen er *"hvilken rolle spiller lederstil for informasjonssikkerhetskulturen i banken"*. Studiet gjennomføres ved en bank i Norge, som av hensyn til informantene er sensurert. Dette kapittelet presenterer analysen av casestudiet. Det er ønskelig å se forskjellen mellom avdelingene, derfor vil vi begynne med å presentere markedsavdelingen (avdeling 1) etterfulgt av produksjonsstøtteavdelingen (avdeling 2). Det første fokuset i analysen er å få en oversikt over hvilke tanker, refleksjoner og meninger ansatte og ledere har omkring informasjonssikkerhetskulturen i banken. Analysen har deretter fokus på hvordan lederne jobber for informasjonssikkerhetskulturen. Denne kulturen kan være forskjellig i de to avdelingene som omtalt i kapittel 2.1.3, og vi ønsker derfor å se på i hvilken grad lederstil kan være en grunn til denne forskjellen. Dersom lederne i de to avdelingene har forskjellig lederstil, vil vi se hvordan denne forskjellen kan være med på å belyse hvilken rolle lederstil spiller for informasjonssikkerhetskulturen. For å kunne beskrive dette var det hensiktsmessig å få frem meninger fra forskjellige ansatte. Analysen bærer derfor preg av forskjellige synspunkter. Hensikten er få frem hva lederne mener om seg selv om sitt arbeid for informasjonssikkerhetskulturen og hva ansatte mener om sin nærmeste leder. Analysen ble delt inn i tre hovedtemaer: informasjonssikkerhet, informasjonssikkerhetskultur og lederstil.

## 4.1. Beskrivelse av case - markedsavdeling og produksjonsstøtteavdeling

Markedsavdelingen (avdeling 1) består av kundebehandlere og kunderådgivere. Kundebehandlerne ekspederer kunder, mens kunderådgiverne hovedsakelig jobber med lån og forsikringer. Intervjuene med markedsavdelingen består av seks ansatte og én mellomleder. Produksjonsstøtteavdelingen (avdeling 2) jobber på back office og på kredittstøtte. De åpner nye privatkunder og bedriftskunder og utbetaler lån. De jobber med bakenforliggende arbeid og fungerer som en støtteavdeling. Intervjuene fra produksjonsstøtteavdelingen består av fem ansatte og én mellomleder. I det følgende vil vi analysere svarene fra informantene. Vi skiller avdeling 1 og 2, og presenterer informantenes meninger under hvert tema.

## *4.2. Informasjonssikkerhet*

Med dette temaet ønsker vi å belyse hva informantene legger i begrepet informasjonssikkerhet. Hensikten er å komme frem til i hvilken grad informantenes oppfatninger av begrepet stemmer overens med de teoretiske perspektivene i kapittel 2. Informasjonssikkerhet har i tillegg fire områder som skal beskyttes, som er konfidensialitet, integritet, tilgjengelighet og robusthet (Datatilsynet, 2018). Disse vil også være en del av begrepsforståelsen, og vi ønsker å se om informantene forklarer noe rundt dette. En begrepsavklaring vil kunne si noe om forståelsen ansatte og ledere har om informasjonssikkerhet, og gi en indikasjon på kunnskapsnivået deres.

**Markedsavdeling - avdeling 1**

Vi ser av svarene fra intervjuene at det er ulik forståelse for begrepet, og at det til en viss grad samsvarer med datatilsynets definisjon som vi har benyttet i denne oppgaven. To informanter forklarer informasjonssikkerhet som håndtering av informasjon som eksempelvis sitatet under viser.

> *"Det må jo være hvordan vi håndterer vår … jaa all vår informasjon rundt kunder og alt mulig"* (Sitat fra informant 2, avdeling 1).

Tre av informantene i avdeling 1 får også frem at det gjelder behandling av personopplysninger. Sitatet under bekrefter dette.

> *"Jeg forstår det på den måten at det har med sikkerhet hvordan vi håndterer informasjonen blant annet. Vi har mye informasjon om mange som vi må beskytte på en eller annen måte eller på mange måter".* (Sitat fra informant 4, avdeling 1).

To informanter forklarer informasjonssikkerhet som taushetsplikt og én nevner at informasjonen ikke må komme på avveie. Dette er således i samsvar med to av de fire områdene som skal beskyttes, om at informasjonen skal være konfidensiell og ha integritet.

Én informant forklarte informasjonssikkerhet som sikkerhet i forhold til "datagreier", og én forklarte at det er hvordan lederne formidler beskjeder til ansatte på en trygg måte. Svarene til

disse to informantene samsvarte i mindre grad med definisjonen som ble lagt til grunn i kapittel 2. Lederinformanten for denne avdelingen forklarte informasjonssikkerhet som informasjon som kun tilflyter de riktige personene, eller de som har et relevant behandlingsgrunnlag for informasjonen.

**Produksjonsstøtteavdeling - avdeling 2**

Informantenes i avdeling 2 sin forståelse av begrepet informasjonssikkerhet samsvarer i stor grad med datatilsynets definisjon, og samtlige i denne avdelingen forklarer at informasjonssikkerhet handler om informasjon og behandling av personopplysninger. Av svarene fremgår det at flertallet av informantene ga en mer detaljert beskrivelse av hvilke tanker de hadde om begrepet.

*"At man bare sender informasjon som er nødvendig å sende og at vi må være sikre på at det ikke kommer på avveie og at det ikke blir lagret mer enn nødvendig, eller i henhold til GDPR, og at vi ikke går inn og snoker og glaner på kunder vi egentlig ikke har noe med å se på, og at vi tier still om all den informasjonen vi vet om kundene"* (Informant 12, avdeling 2)

*"Informasjonssikkerhet ja, det må jo gå på hvordan vi håndterer informasjonen både internt og ut mot kundene da vil jeg tro. Og at vi på en måte har noen sikre mailer når vi oppgir personopplysninger og sånne ting"* (Informant 10, avdeling 2).

Videre er samtlige informanter inne elementer som samsvarer med at informasjonen skal være konfidensiell og ha integritet. Lederinformanten i denne avdelingen forklarte informasjonssikkerhet som sikkerhet tilknyttet alle opplysningene som behandles i banken, og at det i hovedsak dreier seg om å beskytte personopplysninger.

## *4.3. Informasjonssikkerhetskultur*

Dette hovedtemaet består av en rekke underelementer som gjorde seg gjeldende under studiet. For å få en bedre innsikt og forståelse av hvor bevisst informantene var på informasjonssikkerhetskulturen var det viktig å få en forståelse av hva de la begrepet. Målet med dette var å komme frem til i hvilken grad informantenes oppfatninger av begrepet stemmer overens med de teoretiske perspektivene i kapittel 2. Det ble deretter stilt en rekke

spørsmål rundt bankens verdier, policyer, regler og instrukser. Vi stilte også spørsmål om informantenes atferd og kunnskap om informasjonssikkerhet. På bakgrunn av informantenes tanker, refleksjoner og meninger om disse temaene vil vi forsøke å kartlegge informasjonssikkerhetskulturen i de to avdelingene. I det følgende skal vi gjennomgå en begrepsavklaring, etterfulgt av en beskrivelse av avdelingenes synspunkt, kunnskap og atferd relatert til informasjonssikkerhet i banken.

**Markedsavdeling - avdeling 1**

I resultatene fremgår det at informantene synes det var vanskelig å forklare hva som ligger i begrepet informasjonssikkerhetskultur. Samtlige, forklarte at dette var et begrep de ikke benyttet seg av i det daglige sikkerhetsarbeidet. Det indikerer derfor at informasjonssikkerhetskultur ikke er noe informantene i avdeling 1 bevisst jobber for. To av informanten forsøkte likevel å gi en forklaring.

*"Litt sånn hva, hvordan banken har jobbet for å oppnå … gjennom kanskje flere år. Det her med sikkerhet da. Så å følge de retningslinjene en skal og ikke minst det innarbeidet hos oss hvordan vi skal jobbe for å nå det her målet"* (Informant 1, avdeling 1).

*"Det er hvordan alle medarbeidere på en arbeidsplass … får inn sikkerhetsinformasjon og hvordan de utfører det og at man da, om det er ok å gå fra pc ulåst og la sensitiv informasjon ligge åpen på pulten eller om man låser det ned … for eksempel"* (Informant 3, avdeling 1).

Generelt ser vi at det ikke er noen som benytter seg av begrepet eksplisitt, til tross for at flere benytter det aktivt i sitt sikkerhetsarbeid. Heller ikke lederinformanten benytter begrepet eksplisitt, men forklarer det som et kontinuerlig arbeid for at informasjonen skal tilflyte riktige personer. Siden mange synes det var vanskelig å svare på dette spørsmålet, valgte vi å forklare definisjonen som ligger til grunn i denne oppgaven. På denne måten sørget vi for at informantene fikk samme forståelse av begrepet.

**Produksjonsstøtteavdeling - avdeling 2**

Når vi spurte informantene om de var kjent med begrepet informasjonssikkerhetskultur svarte samtlige at dette var et begrep de ikke benyttet seg av i det daglige. Det betyr at også at denne avdelingen ikke bevisst jobber for en informasjonssikkerhetskultur. Det var likevel flere i denne avdelingen som forsøkte å gi en forklaring ved å beskrive hvordan de jobber med

informasjonssikkerhet og deretter koblet det til kultur. Vi forklarte hva vi la i begrepet for denne avdelingen også slik at vi sørget for at alle hadde samme forståelse for begrepet før vi gikk videre med intervjuene.

*"Jeg tenker altså i forhold til kultur det som er satt for bedriften da, det er sånn vi gjør det, og det er faste ting og det er sånn vi gjør det og alle skal være informert og kan noe om"* (Informant 7, avdeling 2).

Lederinformanten forklarte også på lik linje som de ansatte at begrepet ikke blir benyttet i det daglige, men forklarte at det skal være en kultur for hvordan opplysningene håndteres i arbeidshverdagen i banken.

### *4.3.1. Informasjonssikkerhetskulturen i banken*

Finansbransjen er i utgangspunktet en bransje som er sikkerhetsbevisste, og er bundet av en rekke lover og regler som skal sørge for god informasjonssikkerhet blant bransjens virksomheter. Informantene ble derfor bedt om å forklare hvordan de synes informasjonssikkerhetskulturen er i banken. Hensikten med dette spørsmålet var å se hva slags tanker og refleksjoner de gjorde seg om informasjonssikkerhetskulturen.

**Markedsavdeling - avdeling 1**

Samtlige informanter svarer at de synes informasjonssikkerhetskulturen i banken er bra. De forklarte at informasjonssikkerheten er god fordi de følger rutiner som er satt på området, og fire informanter nevner taushetsplikt som særlig viktig å overholde. Tre informanter nevner at informasjonssikkerhetskultur er noe som blir tatt på alvor i banken.

*"Stort sett veldig bra. Vi jobber i en bransje hvor dette har blitt tatt på alvor i all tid, at vi har hatt gode rutiner på alt fra noe så enkelt som taushetsplikt til type handler fra jeg begynte i banken hvor alt var papirbasert"* (Informant 3, avdeling 1).

*"Den er i grunn god syntes jeg, vi har jo rutiner på plass … Og er litt på hverandre".* (Informant 2, avdeling 1).

Lederinformanten er også enige i at banken har en god informasjonssikkerhetskultur. Lederen forklarte at det alltid har vært stort fokus på informasjonssikkerhet gjennom behandling av sensitive opplysninger. Det samme gjelder fokus på å unngå at viktig informasjon kommer på avveie.

**Produksjonsstøtteavdeling - avdeling 2**

Fire av informantene i avdelingen synes informasjonssikkerhetskulturen i banken var god. Mange år med rutiner, oppfølging og fokus på informasjonssikkerhet i banken forklares som årsaker til den gode informasjonssikkerhetskulturen. To informant beskriver det som å følge normer, lover og regler som legger føring for hva slags informasjon som er lov å sende og hvordan det skal behandles. Én informant var imidlertid mer beskjeden i sin forklaring og mente at banken hadde en "grei" sikkerhetskultur.

*"Jeg tror den er … er ganske grei. Jeg tror de fleste holder seg stort sett innafor det… de skal gjøre…det men selvfølgelig kan det skje glipper i enkelte situasjoner sikkert…men jeg føler stort sett at informasjonen…informasjonssikkerheten er ganske grei i banken her da"*(Informant 11, avdeling 2).

Lederinformanten er enig i at informasjonssikkerhetskulturen er god i banken. Etter de nye lovendringene i forhold til personvern og aktivt fokus på informasjonssikkerhet de siste fire årene har det blitt bedre.

### *4.3.2. Personvern og taushetsplikt*

Personvern og taushetsplikt er en viktig del av sikring av informasjon i bankvirksomhet. Det skal verne om fysiske personer i forbindelse med behandling og om utveksling av personlige opplysninger. Personvern og taushetsplikt var konsepter som informantene snakket mye om. Vi spurte ingen direkte spørsmål tilknyttet dette, men det ble nevnt av informantene i forskjellige kontekster. Ettersom informasjonssikkerhet også inkluderer informasjon som ikke er elektronisk vil sikkerhetskultur være viktig. Sikring av muntlig og fysisk informasjon må derfor løses på andre måter enn gjennom tekniske sikkerhetstiltak.

**Markedsavdeling - avdeling 1**

Samtlige informanter påpekte at de var bevisste i forhold til dette med personvern og taushetsplikt. Enkelte nevnte at personvern og taushetsplikt gjaldt både elektroniske dokumenter, fysiske dokumenter, mens én informant nevnte muntlig informasjon. Enkelte påpekte viktigheten av dette i forhold til bankens omdømme.

*"Vi har opplevd eller opplever at det blir et mer og mer viktig område fordi at informasjonsbiten er så stor og det er så mye som foregår elektronisk og det er GDPR i forhold til personvern sikkerhet ikke sant, og det har på en måte blitt strengere regler og mye mer fokus på det sånn generelt i samfunnet og at vi i den forbindelse, at vi da (...) trenger å ha et høyt kompetansenivå blant alle i banken"* (Informant 4, avdeling 1).

*"Vi er aktsomme med å sende sensitive opplysninger i åpne kanaler. Vi sender jo, hvis det skal deles, sensitive opplysninger sendes jo det primært (..) via post hvis du kan si at det er noe mer sikkert en epost, eller så sender vi det jo via nettbank hvor det krever innlogging, (..) og hvor sikkerheten er bedre. Det er klart at det er en stor omdømmerisiko hvis det skal gjøre det. Det er jo nettopp derfor det brukes mye tid og ressurser på, på at vi skal være nøye på sånne ting, og det er vi"* (Informant 2, avdeling 1).

Én informant nevnte at brudd på informasjonssikkerheten for eksempel kunne være når ansatte lar papirer med konfidensielt innhold ligge åpent på pulten, og forklarte at banken hadde strenge retningslinjer for å unngå dette. En annen informant forklarte at man ikke skulle sitte i kantinen å snakke om kunder, og unngå å nevne navn dersom saker ble diskutert. Lederinformanten forklarte på generelt grunnlag at unødvendig informasjon av sensitiv karakter ikke må tilflyte de uten behandlingsgrunnlag. Det ble forklart videre at dette gjaldt spesifikt i kundesituasjoner.

**Produksjonsstøtteavdeling - avdeling 2**

Samtlige informanter forklarte at de er påpasselige med håndtering av personopplysninger og sensitiv informasjon. Flere informanter nevnte blant annet at informasjon som skal sendes i åpne kanaler må krypteres, og på denne måten sørge for å holde personopplysninger skjult. To informanter nevnte også at når man begynner i jobben skriver man under på en taushetserklæring som vil ligge til grunn for alt man foretar seg.

*"Når vi begynner så skriver vi under en sånn taushetserklæring og det er liksom det som ligger i bunn og at man må være forsiktig med, det gjelder jo både ut og internt at man må være litt forsiktig når man håndterer de opplysningene og det er jo mye forskjellige opplysninger som kan være i forskjellige saker"* (Informant 7, avdeling 2).

Lederinformanten forklarte at personvern og taushetsplikt er noe som alltid ligger i bakhodet, men også fremme i panna.

### *4.3.3. Kjennskap til policy, regler og instrukser*

Kjennskap til policy, regler og instrukser er med på å utgjøre det første nivået i informasjonssikkerhetskulturrammeverket (Schein, 1987; Niekerk & Solms, 2010). Når vi stilte informantene spørsmål om de er kjent med bankens sikkerhetspolicyer eller sikkerhetsmål svarte de fleste at de ikke er kjent med dette. Vi hadde en samtale med IT avdelingen, som i kombinasjon med datainnsamlingen skulle gi oss økt kunnskap om hvordan banken arbeider for å nå informasjonssikkerhetsmålene. Informasjonssikkerhetspolicy eller sikkerhetsmål er i utgangspunktet ikke noe som ansatte eller mellomledere i banken skal kunne noe om. Disse er satt overordnet i banken, og arbeides med av bankens IT avdeling, compliance avdeling og toppledergruppen. Vi valgte likevel å spørre de om dette. Hensikten med spørsmålet er at det blir trukket frem i teorien at alle i en virksomhet bør kjenne til de overordnede sikkerhetspolicyene og hva som er virksomhetens mål i henhold til dette. Vi hadde dette i bakhodet og ønsket å høre på avdelingsnivå hvilke tanker ansatte og lederne hadde omkring dette, og om leder hadde nevnt noe eksplisitt.

**Markedsavdeling - avdeling 1**

På spørsmålet om informantene er kjent med bankens sikkerhetspolicyer eller sikkerhetsmål, nevnte de fleste det daglige sikkerhetsarbeidet som omhandler rutiner og hvordan personopplysninger og sensitiv informasjon håndteres. En informant forklarte at måten de jobber med informasjonssikkerhet på er godt innarbeidet, og ligger i "ryggmargen". Informantene påpekte at de har gode rutiner for å sørge for at sensitive opplysninger ikke sendes i åpne kanaler, men enkelte antydet at de tror at det kan forekomme. Lederinformanten var ikke kjent med om banken har sikkerhetspolicy eller sikkerhetsmål.

*"Det er ikke noe sånn som vi har oppe på agendaen så ofte egentlig da, men … i det daglige. Det ligger liksom litt i ryggmargen da"* (Informant 1, avdeling 1).

Vi spurte også informantene om de fulgte instrukser og regler om informasjonssikkerhet. De fleste svarte bekreftende på dette, hvor enkelte nevnte at de sikkert kunne bli enda flinkere. Et eksempel på regel eller instruks som ansatte i bankvirksomhet må følge er å ikke sende eposter i åpne kanaler. En informant forklarte at det i enkelte situasjoner var fristende å be kundene sende informasjon på epost fordi det var enklere, men at det likevel ikke ble gjort på grunn av strenge regler på området. En informant kunne ikke med sikkerhet kunne si at instruksene eller reglene ble fulgt når vedkommende ikke kunne gjenfortelle dem når vi stilte spørsmålet. Lederinformanten forklarte at datadisiplinerklæringen som underskrives ved ansettelse ligger til grunn for alt som ansatte foretar seg. Rutiner og regler er utarbeidet for det meste som gjøres i banken.

*"Jeg kan ikke si at jeg ikke følger den helt og holdent når jeg ikke helt akkurat veit åssen … at jeg kan gjenfortelle den for deg. Men jeg nok ganske sikkerhetsorientert og forsiktig person i … det meste jeg gjør … Både dobbelt sjekker det meste så jeg tenker at jeg følger"* (Informant 5, avdeling 1).

Deretter spurte vi om instruksene eller reglene forbundet med informasjonssikkerhetsarbeidet i banken var enkle å forholde seg til. Hensikten med spørsmålet var å se hvorvidt det kunne være en årsak til eventuelt at regler eller instrukser ikke følges. Samtlige informanter svarte at de synes det var enkle å følge og forholde seg til, og at de reglene som var satt i stor grad baserte seg på rutiner.

*"Ja jeg følger nok de fleste, også er det nok eksempelvis det med lagringstid på informasjonen på papir, det er det jo veldig fort gjort å bryte, og en har for mye papirer det står informasjon på. Vi låser det jo inn på kvelden, men det er liksom ja"* (Informant 4, avdeling 1).

Rutiner var en organisatorisk faktor som samtlige informanter nevnte, både som direkte og indirekte omhandler informasjonssikkerhet i banken. Det ble nevnt i forskjellige kontekster, men det meste av arbeidet som gjøres i forbindelse med informasjonssikkerhet er gjennom

organisatoriske rutiner som er utarbeidet av IT avdelingen. Rutiner og prosedyrer henger sammen med flere andre faktorer.

Informantene var enige i at etterlevelse av rutiner ble godt nok gjennomført og hadde høy prioritet. Ved spørsmål om de rapporterer uønskede hendelser og avvik kom det frem at enkelte ikke gjør det, og at det på denne måten kan oppstå svikt.

*"Vi har hatt gode rutiner på alt fra noe så enkelt som taushetsplikt til type handler fra jeg begynte i banken hvor alt var papirbasert. Hvor vi alltid hadde gode rutiner på oppbevaring og makulering og sånne ting, til hvordan vi nå håndterer elektronisk dokumentasjon (..) og hvordan vi kommuniserer med kundene"* (Informant 2, avdeling 1).

**Produksjonsstøtteavdeling - avdeling 2**

På spørsmålet om informantene er kjent med bankens sikkerhetspolicyer eller sikkerhetsmål svarte også alle i denne avdelingen at de ikke er kjent med dette. De forklarte likevel hvordan de arbeider med informasjonssikkerhet på daglig basis. De nevnte også her rutiner, personopplysninger og taushetsplikt. Én informant nevnte at opplæringskursene er noe alle ansatte er pålagt å ta, og på denne måten kan ses på som et sikkerhetsmål som banken bør oppnå. Én informant nevnte at eneste målene vedkommende er kjent med er salgsmål. En informant forklarte også at de jobber tett med IT avdelingen, og at om det dukker opp noe vil de på en enkel måte få hjelp. Lederinformanten i denne avdelingen var heller ikke kjent med om det foreligger sikkerhetspolicyer eller sikkerhetsmål i banken.

*"På avdelingsnivå hos meg så går jo det på veldig mange plan for så vidt, for det går på både det med behandling av dokumenter og de kanalene vi sender dokumenter i er sikre"* (Informant 12, avdeling 2).

Når vi spurte informantene om de har regler eller instrukser for informasjonssikkerhet svarte de fleste mer utfyllende på det første spørsmålet som ble stilt, om de var kjent med sikkerhetspolicy eller mål. Flere svarte bekreftende på at dette er noe de har, og én informant forklarte hvor disse instruksene ligger. Flere informanter nevnte at dette dreier seg om rutinene som er satt på de forskjellige områdene, som i stor grad legger føringer for hva som skal gjøres for å opprettholde informasjonssikkerheten. Lederinformanten forklarte at de har datadisiplinerklæringen og IKT forskriften, og at disse omfattes av bankens interne rutiner.

På spørsmål om informantene fulgte instrukser og regler om informasjonssikkerhet svarte samtlige at det var noe de gjorde. Samtlige svarte også at de synes instruksene og reglene var enkle å forholde seg til. Reglene de forhold seg til omfattes i stor grad av rutiner som er utarbeidet av IT avdelingen, og fungerer som oppskrifter som kan brukes gjennom et oppslagsverk.

Informantene i denne avdelingen var enige om at etterlevelse av rutiner ble gjennomført på en god måte. Rutinene utarbeides av IT avdelingen og revideres ved behov etter en vurdering som gjennomføres en gang i året. Ved uønskede hendelser eller avvik blir det foretatt endringer for å unngå at dette skal skje igjen, som nevnt under punkt 4.3.5. Flere av informantene nevnte at det finnes en rutine for enhver handling, og påpekte derfor at så lenge disse er gode og ansatte følger dem vil informasjonssikkerheten være god. Lederinformanten forklarte at rutinene som er satt på de forskjellige områdene fungerer som et verktøy, og skal sørge for at arbeidet gjennomføres på en sikker måte. Rutinene omfatter reglement som banken er pliktig til å følge som eksempelvis IKT-forskriften og personopplysningsloven.

### *4.3.4. Kunnskap*

Kunnskap om informasjonssikkerhet er nødvendig. På grunn av rask teknologisk utvikling kan det ikke antas at alle ansatte har den nødvendige kunnskapen som behøves. Vi stilte derfor spørsmål om informantene synes at de hadde nok kunnskap til å vurdere hva som er trygt å utrygt å gjøre relatert til informasjonsbehandling.

**Markedsavdeling - avdeling 1**
De fleste informantene svarte at de hadde nok kunnskap, men én informant fremhevet at kriminelle ofte er i forkant og at man derfor ikke være helt trygg.

*I grove trekk !ja, men det er klart atte kjeltringene de er (..) de er alltid i forkant. Det er jo de som på mange måter driver masse ting videre med en fantastisk kreativitet" (*Informant 2, avdeling 1).

Et inntrykk vi fikk gjennom intervjuene var at enkelte ansatte lente seg på IT avdelingen i enkelte situasjoner. Flere informanter forklarte at IT avdelingen har den nødvendige kompetansen på området, og om de ansatte lurte på noe var det derfor enkelt å ta kontakt for å få hjelp. Etter samtalen med IT avdelingen forsto vi at det var meningen at det skulle være korte linjer og enkelt å få hjelp. Lederinformanten mente også at den nødvendige kunnskapen om informasjonssikkerhet er tilstede.

*"Alt det jeg trenger for å gjøre jobben min selvfølgelig er jo viktig. Men så klart blir vi ikke så veldig gode. Vi har jo en egen avdeling for alt på IT så er jo bare å knipse i fingrene så står de jo der"* (Informant 1, avdeling 1).

Videre spurte vi informantene om de var bekymret for to typiske hendelser som kan oppstå i forbindelse med informasjonssikkerhet. Det første vi spurte om var hvorvidt de var bekymret for at de ble utsatt for phishing emails som fremsto som vanlige eposter. Det var varierende svar, men de fleste informantene opplevde ikke noen bekymring relatert til en slik hendelse. En informant forklarte at det kanskje hadde noe med kunnskapsnivået å gjøre. Lederinformanten var ikke bekymret for at en slik hendelse kunne oppstå, men var bekymret for konsekvensene dersom det skjedde.

*"Nei! Det er sånn jeg ikke tenker på overhode. Det er kanskje fordi jeg ikke har nok kunnskap. Nei, det tenker jeg ikke på. Men det ser jeg jo på det private der det kommer inn så mye. Det er veldig fort gjort å bli lurt, men også har jeg fått de ett par ganger så tenkt at jeg har blitt skeptisk på alt. Fordi de er ganske gode på å kopiere … logoer og ja. Jeg skjønner man kan bli lurt"* (Informant 1, avdeling 1).

Den andre hendelsen vi stilte spørsmål om var en typisk hendelse tilknyttet bank, og omhandlet hvorvidt de var bekymret for at kundens personopplysninger skulle komme på avveie. En informant uttrykte ikke bekymring for at det skal hende på grunn av sitt eget kunnskapsnivå, men ytret bekymring i forhold til kollegaer som kan la seg lure i større grad. De andre informantene uttrykte noe forskjellig grad av bekymring for at en slik hendelse skulle oppstå. Lederinformanten var bekymret og tok en slik hendelse på alvor. Lederen forklarte at det var grunnen til at de har strenge regler for hvilke type opplysninger som sendes på mail og ikke.

*"Det er jeg litt mer bekymret for så der er jeg litt mer påpasselig. Så der har vi et ansvar da"* (Informant 8, avdeling 1).

*"Klart det er jo … alltid en… som jeg sa ista så føler jeg at jeg ikke sender noe med sensitiv informasjon ut på, men dessverre er det jo slik at det er en del kunder som … som føre vi får sukk for oss har send*t (Informant 5, avdeling 1).

*"Ja jeg føler en bekymring på det. Litt av det vi har vært inne på tidligere, altså bekymret for at ting kanskje skal komme ut at vi har sendt ting feil eller ikke sant sendt en mail feil (..) eller at det dukker opp ting i forbindelse med makulering eller sånne ting"* (Informant 4, avdeling 1).

Håndtering av avvik og uønskede hendelser blir fremhevet som utfordringer i informasjonssikkerhetsarbeidet. Enkelte informanter fortalte for eksempel at de tror at mange hendelser forblir urapportert. Uønskede hendelser skal registreres i en egen base på intranettet til banken. To informanter vet ikke hvor de skal rapportere inn uønskede hendelse, men forklarte at dersom det hadde oppstått en situasjon ville vedkommende sendt en mail til IT eller snakket med sin nærmeste leder. Fire informanter vet hvor hendelsene skal registreres, mens ingen av informantene har hatt behov for å registrere noe.

*"Uønskede hendelser. Så må det meldes inn da … og der tror ikke jeg at det meldes inn så mye saker kanskje sånn som de som sitter med ansvaret skulle ønske"* (Informant 1, avdeling 1).

*"Det er nok ikke vær gang en uønsket hendelse blir rapportert"* (Informant 3, avdeling 1).

**Produksjonsstøtteavdeling - avdeling 2**

Informantene synes generelt de har nok kunnskap til å vurdere hva som er trygt å utrygt å gjøre relatert til informasjonsbehandling i banken. Tre informanter forklarte at de antakeligvis burde hatt mer kunnskap, men beskrev kunnskapsnivået sitt som godt nok for å håndtere de ulike arbeidsoppgavene på en trygg og sikker måte. Flere av informantene forklarte også at de føler seg trygge på at de får den hjelpen de trenger fra IT avdelingen dersom det skulle oppstå situasjoner hvor de føler seg usikre. Lederinformanten forklarte at oppveksten i stor grad var preget av teknologi og følte seg derfor svært trygg.

*"Jeg har nok greie på hva jeg kan gjøre, men det er sikkert mer jeg kunne gjøre enn det jeg gjør også likevel hadde vært trygt det veit jeg ikke, men jeg føler vi får god informasjon på jobben av hva vi kan og hva vi ikke kan"* (Informant 12, avdeling 2).

Når vi spurte hvorvidt de var bekymret for å bli utsatt for phishing emails svarte tre informanter at det var lite bekymret for dette. To informanter utrykte til dels bekymring rundt en slik hendelse, og begrunnet det med at de som gjennomfører slike ting alltid er et "hakk foran". De gikk likevel ikke rundt til daglig og bekymret seg for dette. Lederinformanten var ikke bekymret for en slik hendelse.

*"I utgangspunktet er ikke det noe sånn jeg tenker på. Det er det ikke, men det er klart at jeg vet jo at det oppstår innimellom, men akkurat det med løsepenger ligger veldig langt vekk fra min svære"* (Informant 10, avdeling 2).

Ved spørsmål om de var bekymret for at personopplysninger skulle lekke svarte fire informanter at de ikke var bekymret fordi de stoler på rutinene og sikkerhetssystemene. Enkelte forklarte at det likevel lå i bakhodet at slike hendelser kunne oppstå, og uttrykte bekymring for eventuelle konsekvenser av en slik hendelse. Én av informantene forklarte at de jobber kontinuerlig for å unngå slike hendelser, og at alle vet hva de skal gjøre og ikke gjøre relatert til informasjonssikkerhet. En annen forklarte at bakgrunnen for at de krypterer mye informasjon er for å unngå slike situasjoner, og var derfor ikke bekymret for at det skulle skje på sine egne vegne. Én informant uttrykte imidlertid bekymring. Lederinformanten var ikke særlig bekymret for en slik hendelse. Gode systemer og dataleverandører og internt fokus på det gjør at det skal mye til, men forklarer at det kan skje menneskelige glipp.

*"Selvfølgelig en stor bekymring, en må jo hele tiden hver eneste dag være bevisst på hva en sender og ikke og hvilken kanal en sender det i. Man må liksom på en måte hele tiden være bevisst i hver enkelt sak hva en opplyser og hva vi sender fra oss, så det er jo noe som ligger mer i topplokket hver dag liksom og at en har det framme i panna"* (Informant 7, avdeling 1).

*"Det er jeg heller ikke bekymret for, du sender jo aldri det om den enkelte kunde, hvis vi skal sende noe så går det jo i nettbanken til kunden eller så"* (Informant 12, avdeling 2).

Samtlige informanter i avdeling 2 vet hvor og hvordan de skal håndtere avvik og uønskede hendelser. Flere informanter forklarte at det finnes forskjellige måter å melde fra om hendelser, men basen for uønskede hendelser blir nevnt oftest. Samtlige hadde også kontaktet IT direkte dersom det ble ansett som hensiktsmessig.

*"Ja da, vi har en sånn link på innsikt her hvor vi kan…sånn som gjeler rapport av uønskede hendelser kan du si da… eller at en spør nærmeste sjef som er på plass …Først da…det er og en mulighet"* (Informant 9, avdeling 2)

*"Ja, og det har vi også oppskrift for også for å si det sånn. Det har vi rutiner på, så da ville jeg slått opp i rutina og sett ordentlig på den, (..) men i utgangspunktet så har vi flere veier til mål der, men IT som sagt der har de en egen epost adresse (..) som vi melder til om det er noe vi lurer på. Også ligger det som sagt avviksrutiner på sånne uønskede hendelser, det ligger mot kontrollerne våres, så det og har vi oppe i dagen"* (Informant 10, avdeling 2).

*"Eh ja, da har vi en sånn egen base for uønskede hendelser hvor vi melder inn ting det, ellers er det sånn direkte kontaktgruppe til IT da, men det spørs jo selvfølgelig litt hva det er, men det går jo an å melde det inne begge steder da"* (Informant 7, avdeling 2).

Lederinformanten forklarte at den viktigste oppgaven han har som leder er å avdekke kunnskapen til de ansatte og tette hullene. Det kan være ved å tilby opplæring eller en oppfriskning. Lederen påpekte også at det å gå frem som et godt eksempel er det mest effektive.

### *4.3.5. Læring*

Den største opplæringsfasen i forbindelse med informasjonssikkerhet utføres hovedsakelig ved nyansettelse. Banken driver jevnlig med informasjonssikkerhetsopplæring av ansatte ved hjelp av e-læringskurs. Det er korte kurs som kommer jevnlig på mail med opplæringsvideoer og spørsmål. Vi spurte informantene om de hadde fått bedre kunnskap og ferdigheter om informasjonssikkerhet etter opplæringen.

**Markedsavdeling - avdeling 1**

Samtlige informanter utenom én svarte bekreftende på dette, og begrunnet det med at kunnskapen allerede var der. Lederinformanten var også enig i at opplæringen hadde vært nyttig. Jevnlig oppdatert informasjon som kan underbygge bevissthet og forståelse for informasjonssikkerhet er derfor svært nyttig.

*"Vi får jo de ganske fort, ganske fortløpende, det liksom ikke en sånn engangshendelse men det blir liksom en del av jobben. Så da øker jo kunnskapsnivået og ikke minst at vi får det litt lenger fremme i panna enn vi har hatt fordi at vi gjør det hele tiden"* (Informant 4, avdeling 1).

*"Ja egentlig ja, fordi det er ganske dagsaktuelt når det kommer"* (Informant 2, avdeling 1).

Videre spurte vi informantene om de kunne tenke seg mer opplæring. De fleste ønsket mer opplæring, men enkelte svarte at det kun var ønskelig én gang i året. Dersom det ble for ofte forklarte enkelte at det ville oppleves som slitsomt, og begrunnet med at de hadde mye annet å gjøre også. Det indikerer derfor at informasjonssikkerhet ikke er det største fokuset til informantene. Lederinformanten forklarte at mer kunnskap kunne vært nyttig.

*"Det hadde sikkert ikke skadet å tatt noe mer informasjon om det…en gang i året… altså hatt litt mer… det du må hele tilegne deg selv kan bli slitsomt i lengden fordi det er ikke bare det vi blir oppdatert på, på en måte…Men…Så absolutt... jeg tenker sånn att…en gang i året kunne det ha vært nyttig"* (Informant 5, avdeling 1).

Feil og uønskede hendelser bør skape læringssløyfer og kunnskapsdeling med medarbeider, og på denne måten øke kunnskapen og bevisstheten rundt sårbare situasjoner relatert til informasjonssikkerhet. I forbindelse med dette spurte vi derfor om det var en kultur for å lære av feil og uhell. Samtlige informanter svarte bekreftende på at de lærte av feil og uhell i banken. Det meste av nyttig informasjon legges ut på intranettet til banken hvor informantene forklarte at de holder seg oppdatert. Her legges det ut generell informasjon, men også når det oppstår nye situasjoner som er viktig å informere alle ansatte om. En svakhet med intranettet er at ansatte selv må aktivt inn for å innhente informasjon og kunnskap. Lederinformanten var enig i at de hadde en kultur for å lære av feil og uhell i banken.

**Produksjonsstøtteavdeling - avdeling 2**

Når vi spurte informantene i avdeling 2 om de synes de hadde fått bedre kunnskap og ferdigheter etter opplæringen svarte alle bekreftende på dette. Én informant presiserer at det likevel har vært et kontinuerlig arbeid fra de startet i jobben, og at det har vært innprentet som viktig å følge regler og rutiner på området. Lederinformanten synes opplæringen er nyttig og opplevde at hukommelsen på enkelte ting ble frisket opp.

*"Vi får i hvert fall frisket opp igjen det du har hørt tidligere og får en liten sånn reminder på atte åja det må vi huske på. For det varierer jo veldig fra dag til dag"* (Informant 12, avdeling 2).

*"Ja jeg synes det altså, for man blir liksom litt mer sånn bevisst i hverdagen og man får det på en måte litt mer fremme i panna, eh når det (..) både er det quizene vi får og den informasjonen vi får og det er lett å finne tilbake til"* (Informant 7, avdeling 2).

*"Det blir jo sånn at du får frisket opp hukommelsen litt da på enkelte ting… Så jeg syntes det er nyttig … og viktig at vi gjør det også… Det er ikke bare fordi at det gir en revisjonsrapport skal se fint ut at det at alle bankens ansatte har gjennomgått … e-læring på det og det. Det har jo en nytte det også fordi at vi behandler disse opplysningene … hele tiden og det er en viktig del av hverdagen våres og omdømme til banken er jo svært viktig for at vi skal ha en arbeidsplass. Så … jeg tror det … det er ganske knyttet godt i pannen på de fleste her"* (Lederinformant, avdeling 2).

Fire av informantene kunne tenke seg mer opplæring om informasjonssikkerhet.
Én informant forklarte at det ikke var nødvendig med mer opplæring så lenge det kom opplæring i forbindelse med nye systemer eller om det dukket opp nye hendelser. Lederinformanten mener opplæringsopplegget er godt nok som det er, og begrunner det med at de korte kursene som kommer med jevnlig mellomrom ikke stjeler for mye oppmerksomhet.

*"Jeg tenker at det er noe man aldri blir utlært på, så påfyll er bare helt supert, som sagt så er det stadig noe nytt og det er dessverre mye sånne som ligger hakket foran så det vil føle at det er noe som utvikles hele tiden, og påfyll er supert"* (Informant 7, avdeling 2).

Samtlige informanter er klare på at det er en kultur for å lære av feil og uhell som skjer i banken. Det blir påpekt at hensikten med basen for uønskede hendelser er at det som meldes inn skal benyttes for å unngå at liknende hendelser skal skje igjen. Flere informanter forklarer at det på bakgrunn av denne hendelsesbasen at blir gjort endringer i rutiner, og at dette vurderes en gang i året.

*"Ja det mener jeg vi gjør. Vi har for så vidt en rutine på det med uønskede hendelser, (..) og den kontrollen den tar vi i alle fall om vi har noen endringer på den rutinen, den har vi endringer på minimum en gang i året, så det må jo være en eller annen lærdom i det for da finner vi jo gjengangere og må sette oss inn i dem igjen og tenke på hva kunne vi gjort annerledes, og hva må vi gjøre neste gang. Så det vil jeg påstå at vi har"* (Informant 10, avdeling 2).

*"Vi prøver jo det da, og det er jo litt av det som er vitsen med den derre uønskede hendelsesbasen som vi har atte når det skjer noe så blir det tatt tak i og (..) enten om det er systemer som blir endret eller folk som får opplæring eller det blir satt inn doble kontroller eller det kommer jo litt an på hva slags hendelse som har inntruffet da"* (Informant 12, avdeling 2).

*"Ja, absolutt. Hvis man er borti noe liksom sånn så er jo sånn at man melder inn som uønsket hendelse for eksempel da, også blir det tatt litt sånn generelt at nå har vi hatt en sak sånn og sånn og da blir man jo enda mer bevisst på det hvis man har vært borti et tilfelle da. Så ja, absolutt, lærer av feil og ting som skjer"* (Informant 7, avdeling 2).

Lederinformanten forklarer at det er leders ansvar å følge opp hvordan informasjonen behandles, og avdekke avvik. Avvik blir tatt i plenum i avdelingen for å finne ut av hva som har skjedd og for å unngå at det samme skjer igjen. Lederen forklarer at det er en åpen kultur rundt det å lære av hverandres feil.

### *4.3.6. Atferd*

Atferd kommer til uttrykk som et helhetsbilde basert på mange av svarene vi har fått fra informantene, da det handler om hvordan de oppfører seg, hvordan de kommuniserer og samarbeider. En god beskrivelse av informantenes atferd er imidlertid ikke mulig å få til, da

det gjøres best gjennom observasjon. Vi spurte informantene to spørsmål direkte tilknyttet deres informasjonssikkerhets atferd. Det første vi spurte om var om de undersøker link, nettside eller epost før de bruker eller åpner den.

**Markedsavdeling - avdeling 1**

Informantene hadde delte svar om hvorvidt de undersøker link, nettside eller epost før de bruker eller åpner den. To informanter sa at dette ikke er noe de gjør, hvor den ene antar at alle eposter er trygge. To informanter svarte tydelig ja på at dette er noe som undersøkes, og to informanter svarer at de gjør en viss vurdering, særlig i forbindelse med jobb. Lederinformanten var klar på at han alltid undersøker, og at det hender det blir sendt til IT avdelingen slik at de kan kontrollere linker.

*"Eh, i forhold til jobb så gjør jeg vel det (...) altså jeg gjør jo ikke det med hver eneste epost jeg får, men jeg gjør jo en vurdering, altså hvis det er noe jeg ikke kjenner igjen så er gjør jeg en vurdering som er liksom er mer nøye enn hvis jeg får en mail fra en kunde jeg kjenner da"* (Informant 4, avdeling 1).

Deretter spurte vi informantene hvordan deres forhold er til bruk av passord. To informanter svarte at det kunne vært bedre, og beskriver seg selv som sløve på bruk av passord. Likevel setter systemet en rekke krav som tvinger dem til å gjennomføre de viktigste endringene. Det er derfor bruk av ulike passord informantene er "sløve" på. Fire informanter svarer at de er bevisste på bruk av passord. Én informant er konsekvent på å ikke bruke passord hjemme som brukes på jobb, og bruker tid på å lage sikre passord. Lederinformanten har også et bevisst forhold til passordbruk.

*"Ganske konsekvent på å ikke bruke noe på jobb som jeg bruker privat. Også ikke velge noe som er veldig enkelt å gjette"* (Informant 3, avdeling 1).

**Produksjonsstøtteavdeling - avdeling 2**

De fleste informantene i avdeling 2 forklarte at de har opparbeidet seg en del forståelse og kunnskap omkring tegn ved både nettsider, linker og eposter som er mistenksomme, og velger å sjekke over en ekstra gang. Én informant svarte at det nok ikke var alltid det ble undersøkt, men at dette i større grad gjaldt utenfor jobben. Samtlige informanter svarte at de i jobbsammenheng ikke benytter arbeidsdatamaskinen til annet enn jobb, slik at usikre nettsider

sjeldent vil være et problem. Linker og eposter er de imidlertid mer observante på. Lederinformanten var også bevisst på denne problemstillingen, og var særlig påpasselig med linker.

*"Linker sjekker jeg, men vanlige nettsider, eeh jeg bruker aldri jobb pc-en til noe annet enn (..) det hender jo at en kan gå på nettavisen eller VG eller sånn, men jeg går aldri inn på nettsider som jeg, som ikke er sånn allment kjente via jobbpcn"* (Informant 12, avdeling 2).

Ved spørsmål om informantenes bruk av passord svarer samtlige at de har et bevisst forhold til dette. De har kontroller i systemet som bestemmer hvor ofte det må byttes, og de forsøker å lage så trygge passord de kan. Mange bruker egne passordoppskrifter, og det benyttes forskjellige passord til de forskjellige tjenestene. Lederinformanten har også et bevisst forhold til passord, og skiller konsekvent passord som brukes privat og passord i tilknytning til jobben.

### *4.3.7. Bevissthet og fokus*

Bevissthet var et konsept flere informanter nevnte særlig i forbindelse med opplæring. De mente at kurs og opplæring ville gjøre dem mer bevisste på informasjonssikkerhet. Konseptet dukket også opp når vi spurte informantene om de kunne reflektere litt rundt hva som skulle til for at informasjonssikkerhetskulturen i banken kunne bli bedre.

**Markedsavdeling - avdeling 1**
Flere nevnte at lederen i større grad kunne hatt mer fokus på informasjonssikkerhet, og at dette ville gjøre de ansatte mer bevisste på det.

*"Man får den påminnelsen om ting man … egentlig kan … Men litt bevisstgjøring ikke sant, det å holde fokus med det alt man gjør ikke sant"* (Informant 1, avdeling 1).

*"Litt lite fokus på det egentlig, at det burde vært tatt mer i møter, at min nærmeste leder kanskje burde vært litt mer involvert i det ja. Ikke bare komme på innsikt og intrantett men at kanskje han lederen som snakker med oss hver dag, hatt litt mer fokus på det"* (Informant 8, avdeling 1).

Én informant forklarte at fokuset ikke var på det med informasjonssikkerhet når vi spurte om de synes de hadde fått bedre kunnskap og ferdigheter etter kursene.

*"Det er ikke det vi går og tenker på. Har fokus på. Vi tenker at det er sikkert å greit og bruker litt sunn fornuft her"* (Informant 1, avdeling 1).

**Produksjonsstøtteavdeling - avdeling 2**

Informantene i avdeling 2 påpekte også at bevissthet rundt informasjonssikkerhet har blitt større gjennom opplæring og de fleste følger med på utviklingen på området.

*"Handler jo om det å være bevisst på den informasjonssikkerheten hele tiden og følge med og være oppdatert på det som er av både regler og muligheter og farer for å si det sånn da i denne digitale verden. Jeg tenker er at det er viktig å ha fokus på det og det er viktig å ha litt sånn repetisjon innimellom så vi får dratt fokuset litt opp igjen for i en hektisk hverdag er det jo det du har mest med å styre med akkurat der og da, det er jo det som tar fokuset ditt, så det å ha litt fokus innimellom og litt repetisjon på de viktigste reglene rundt informasjonssikkerhet er for så vidt selvfølgeligheter, men som nevnt i en hektisk hverdag så kan det glippe så. Fra tid til annen så kommer det jo nytt regelverk om hva som er lov og ikke lov og hva som er sikkert og (..) så det å avlære, det trengs litt repetisjon for å kunne avlære gammel kunnskap*" (Informant 12, avdeling 2).

### *4.3.8. Hjemmekontor*

På grunn av Covid-19 har en rekke ansatte i norsk og utenlandsk næringsliv måtte ta med seg arbeidet hjem. Ansatte forsøker å gjøre den samme jobben som før bare at det nå foregår hjemmefra. Dette betyr at behandling av informasjon ikke er beskyttet av de samme systemene og prosessene som eksisterer på arbeidsplassen. Dette medfører en del nye og uforutsette utfordringer. Dette preget intervjuene våre i stor grad, og mange av informantene påpekte denne utfordringen under intervjuene.

**Markedsavdeling - avdeling 1**

*"Det med informasjonssikkerhet er kanskje litt vanskeligere å ivareta på et hjemmekontor enn til vanlig"* (Informant 8, avdeling 1).

**Produksjonsstøtteavdeling - avdeling 2**

*"Vi stadig får sånne kurs som vi får tilsendt på mail til alle ansatte som vi må gjennom i løpet av året. Det kan være alt fra på en måte hvordan man skal håndtere hvordan man er hjemme nå for eksempel, i forhold privat mail, i forhold til passordbytter"* (Informant 7, avdeling 2).

*"Nå har vi jo fått en litt spesiell situasjon med at vi er veldig mange som sitter hjemme og jobber og det har jo ikke vi vært vant til før og da får vi jo også veldig mange flere påminnelser om dette med endring av passord og passe på at vi har eh (..) passer på at vi oppfører oss riktig i forhold til de som er her hjemme osv, og dette her får vi jo nesten daglige påminnelser om, og det vil jeg jo påstå at er å etterleve reglene og være opptatt av det, og få med ansatte på det også for å si det sånn"* (Informant 10, avdeling 2).

Lederinformanten forklarte at banken har gode krise og kontinuitetsplaner, og at disse blir testet på grunn av Covid-19. Det er andre utfordringer når ansatte er spredt på 9-10 lokasjoner, mot å sitte sammen på 100 kvm kontor.

## *4.4. Lederstil*

Med dette temaet ønsker vi å belyse hva informantene mener om sin nærmeste leders arbeid for informasjonssikkerhet i banken, samt hva leder selv mener om sitt eget arbeid. Spørsmålene vi stilte til lederne måtte følgelig omformuleres fra de vi stilte til ansatte. Vi har stilt spørsmål som er spesielt for en transformasjonsleder og transaksjonsleder. En leder kan ha kvaliteter fra både transformas- og transaksjonsledelse. Til mer positive svar vi får på spørsmålene tilknyttet transformasjonsledelse, til mer vil den lederen kjennetegnes som en transformasjonsleder. Det betyr at lederen kan i større eller mindre grad oppfylle flere eller alle kvalitetene en transformasjonsleder har. Det samme vil gjelde for transaksjonsledelse.

Vi spurte innledningsvis hva lederne selv synes var deres viktigste lederoppgaver. Leder for avdeling 1 svarte at det var å sørge for at ikke unødvendig informasjon av sensitiv karakter tilflyter folk som ikke har noe behandlingsgrunnlag for å jobbe med det. Leder for avdeling 2 svarte at det innebærer å avdekke kunnskap som mangler hos de ansatte, veilede og hjelpe med å tette kunnskapshull. Det innebærer å tilby opplæring eller friske opp kunnskapen hos

enkelte der det er behov. Leder for avdeling 2 forklarte også at en av de viktigste oppgavene er å gå foran som et godt eksempel.

### *4.4.1. Transaksjonsledelse*

I det følgende har vi analysert spørsmålene hvor hensikten har vært å kartlegge om lederne i de to avdelingene kan ha en eller flere kvaliteter av en transaksjonsleder. En transaksjonsleder kjennetegnes som en som identifiserer behovene til sine ansatte og gir belønning for passende innsats og prestasjon. Innflytelse utøves ved at det er i ansattes egen vilje å gjøre som de vil. Spørsmålene vi stilte er knyttet opp til de tre underliggende elementene i transaksjonsledelse som er ledelse ved unntak (aktivt), ledelse ved unntak (passivt) og Laissez faire (Avolio et al., 2003). Denne lederstilen innebærer at leder kan følge med på å lete etter avvik fra regler og rutiner, og korrigere avvik. Det kan også innebære at leder kun griper inn i situasjoner dersom regler ikke blir fulgt, eller unngår ansvar og avgjørelser. Derfor vil spørsmålet om en leder kan karakteriseres som en transaksjonsleder også kan leses ut fra svarene vi har fått på andre spørsmål i intervjuene.

**Markedsavdeling - avdeling 1**
Vi stilte informantene spørsmål om de synes lederen tar informasjonssikkerhet på alvor. Samtlige informanter svarte bekreftende på dette, og flere nevnte at lederen er flink til å følge opp opplærings- og sikkerhetstiltakene som er satt av IT avdelingen.

*"Ja. han passer på at vi blant annet går gjennom de opplæringstiltakene som er satt opp fra banken"* (Informant 4, avdeling 1).

Deretter spurte vi informantene hvordan de synes sin leder er til å følge opp regler og rutiner, og til å gi tilbakemeldinger på sikkerhetstiltak. Informantene hadde ulike svar, hvor én sa at det er fokus fra leder i perioder. En annen informant sa at det ikke er så mye snakk om det fordi det er noe alle kan og er godt innarbeidet hos de fleste. Flere informanter svarte at leder har fokus på rutiner gjennom å påpeke viktigheten av å beskytte sensitiv informasjon. Enkelte svarte at leder sa fra dersom reglene eller rutinene ikke ble fulgt. Når vi spurte lederen det samme spørsmålet ble det forklart at dersom det er nødvendig ble det gitt tilbakemeldinger direkte til den det gjelder.

Vi spurte så hvordan informantene synes lederen jobber med å skape bevissthet omkring risiko forbundet med informasjonssikkerhet. Samtlige informanter svarte at de ikke umiddelbart kan påpeke at det er noe leder jobber med. Enkelte forklarte at de har en kultur på å være bevisste på slik risiko og at de sitter i "ryggmargen".

**Produksjonsstøtteavdeling - avdeling 2**

Når vi spurte informantene om de synes lederen tar informasjonssikkerhet på alvor svarte samtlige ja. Informantene forklarte at de har et tett samarbeid med lederen, og at de har ukentlige møter hvor det ofte snakkes om informasjonssikkerhet. Flere beskrev lederen som bevisst og godt oppdatert på risikoer forbundet med informasjonssikkerhet. Flere forklarte også at lederen går foran som et godt eksempel og beskrives som en pådriver for informasjonssikkerhet.

*"Han er veldig bevisst på det han driver med og veldig flink til å utnytte både mulighetene og det som ligger i disse systemene våre, og han er flink til å minne oss på ting og ikke minst lære oss nye måter å bruke systemene på som gjør at vi får en enklere hverdag og en forsåvidt tryggere flyt med mindre papirer som ligger på pultene som vi heller på logge oss på for å få se"* (Informant 12, avdeling 2).

Når vi spurte informantene hvordan de synes sin leder er til å følge opp regler og rutiner, og til å gi tilbakemeldinger på sikkerhetstiltak svarte samtlige informanter at leder er god på det. Enkelte informanter forklarer at leder er flink til å gi tilbakemeldinger når de også har gjort positive ting. Når vi spør lederen det samme spørsmålet svares det at det er fort å glemme å gi tilbakemeldinger når ansatte har gjort noe positivt, fordi det ligger en forventning om at de skal gjøre det. Det er enklere å huske å gi tilbakemelding de gangene det er gjort feil. Svarene til ansatte i avdelingen på dette spørsmålet og svaret til lederen indikerer at dette er noe leder har fokus på.

Når vi spurte informantene hvordan de synes lederen skaper bevissthet rundt informasjonssikkerhet svarte samtlige informanter at lederen er god på dette. De forklarte at lederen er god til å bruke tid på å hjelpe hver enkelt dersom de har spørsmål eller lurer på noe. Når noen har opplever problemer eller lurer på noe tar lederen det opp med hele avdelingen og på denne måten gir rom for kunnskapsdeling.

*"Det er om ikke daglig så ofte så har vi noen spørsmål eller er vi i tvil så er det alltid noen svar der som er veldig konkret og enkelt å forholde seg til så det føler jeg er noe som sitter inn hele tiden kan du si da, at det er liksom noe som er med på å bevisstgjøre oss hver eneste dag da på de oppgavene vi har"* (Informant 7, avdeling 2).

### *4.4.2. Transformasjonsledelse*

Vi har analysert spørsmålene hvor hensikten har vært å kartlegge om lederne i de to avdelingene kan ha en eller flere kvaliteter av en transformasjonsleder.
En transformasjonsleder skaper bevissthet rundt arbeidsoppgaver og får ansatte til å se konsekvenser. Spørsmålene vi stilte er knyttet opp til de fire grunnelementer av transformasjonsledelse som er idealisert innflytelse, inspirerende motivasjon, intellektuell stimuli og individualisert oppmerksomhet. En leder trenger ikke ha alle grunnelementene, men hvis noen er tilstede vil lederen gå i retning av å være en transformasjonsleder.

Idealisert innflytelse
Vi ønsket å se hvorvidt lederne inspirerer ansatte til å yte mer, fremstår som synlig rollefigur og lytte til ansattes behov. Vi stilte derfor spørsmål om lederen involverer informantene i sikkerhetsarbeidet, og spurte lederne hvilke mål de har om å ivareta informasjonssikkerheten.

**Markedsavdeling - avdeling 1**
Fem av informantene svarte at de ikke synes at han hadde spesielt fokus på dette med informasjonssikkerhet, men sørget for at de gjorde det de skulle. Én informant svarte at leder fulgte opp at arbeidet ble gjort på en sikker måte, og i den forstand var involverende.

*"Vi har ikke så mye fokus på informasjonssikkerhet i den forstand så på det nei"* (Informant *3, avdeling 1).*

*"Nei, jeg gjør vel ikke det, ikke noe annet enn at han passer på at vi går gjennom det vi skal*" (Informant 4, avdeling 1).

*"Jeg kan ikke akkurat si det… når jeg ikke egentlig føler at det er så mye fokus på det (latter). Det er liksom ikke han som har fokusert …det er som regel de kursene stort sett som vi har fått…så…Han minner oss på det at de skal svares på da"* (Informant 5, avdeling 1).

Informantene ble bedt om å se for seg at de lurte på noe eller trengte hjelp i forbindelse med informasjonssikkerhet. Vi spurte så om de trodde leder ville forklare og hjelpe dem på en god måte. Samtlige informanter var tydelige på at dette var noe lederen ville hjulpet dem med.

*"Ja jeg tror egentlig at det er ganske stor åpenhet i vår avdeling så jeg tror egentlig det"* (Informant 2, avdeling 1).

Når vi spurte lederinformanten om han har satt egne mål for å ivareta informasjonssikkerheten svarte han nei, men forklarte at et slikt mål må innebære å sørge for at alle følger regelverket som er satt. Når vi spurte hvordan lederen kunne være en rollemodell for de ansatte i forhold til informasjonssikkerhet svarte vedkommende at det vil være å oppdage og påpeke brudd, og selv gå frem som et godt eksempel.

**Produksjonsstøtteavdeling - avdeling 2**

På spørsmål om informantene opplever at leder jobber for å involvere dem i sikkerhetsarbeidet svarer alle informantene ja. De forklarer at lederen er glad i å lære bort, komme med råd og tips på måter som kan forenkle arbeidet på en sikker måte. Én informant forklarer at lederen ikke involverer enkeltpersoner, men tar det generelt med hele avdelingen slik at alle får det med seg.

*"Ja, han er på en måte veldig flink til å ta ting med oss så fort det kommer noe nytt eller hvis noe har oppstått så tar han det liksom med oss alle, og om vi har noe, det er liksom alltid noe tips eller noe å komme med så er det alltid åpenhet på en måte så vi føler at vi løser ting i fellesskap det gjør vi absolutt"* (Informant 7, avdeling 2).

Samtlige informanter svarte også at lederen ville forklart dem på en god og enkel måte dersom de ikke forsto et sikkerhetsmål som var satt.

Når vi spurte om lederen hadde laget egne mål for å ivareta informasjonssikkerheten forklarte vedkommende at det ikke var satt egne mål. Lederinformanten forklarer at kravene som er satt og vedtatt i forhold til rutinene skal etterleves. Etterlevelsen av regler og rutiner må avdekkes, følges opp og korrigeres i enkelte tilfeller. Når vi spurte hvordan lederen kan være

en rollemodell ble det forklart at det betyr å etterleve de lover og regler som er satt, og følger rutinene, og går frem som et godt eksempel.

Individualisert oppmerksomhet

En leder som tar hensyn til ansattes personlige behov, prestasjon og utvikling er en egenskap som er positivt relatert til ansattes atferd og tilegning av ny kunnskap om informasjonssikkerhet. Vi spurte derfor informantene om de opplever at lederen veileder dem til å ta informasjonssikkerhet på alvor, og spurte lederne selv hvordan de gjør det.

**Markedsavdeling - avdeling 1**

De fleste informantene forklarte at leder ikke oppfordrer til å ta informasjonssikkerhet på alvor direkte, men som en informant forklarte så følger de reglene og rutinene de er pålagt. Det ligger en forventning fra leder sin side at alle ansatte skal ta det på alvor. Én informant synes at lederen oppfordret til dette, men var noe usikker og synes spørsmålet var vanskelig. Lederinformanten forklarte på dette spørsmålet at det ble oppfordret til å ta kurs og oppdateringer.

*"Nei, eh, nei. Ikke noe sånn (..) litt på det at han forventer nok at folk holder seg oppdatert på det ja"* (Informant 2, avdeling 1).

*"Vi tar det på alvor på en måte. Har det innebygd, men oppfordrer kanskje ikke til det. Det blir på en måte tatt på alvor allikevel. Det ligger der"* (Informant 3, avdeling 1).

Videre spurte vi informantene hvordan de synes tilliten mellom seg og leder var dersom det oppsto et sikkerhetsproblem, og om de fikk tilbakemeldinger fra leder når det var nødvendig. Samtlige svarer bekreftende på dette, og nesten samtlige er veldig fornøyd med tilliten mellom seg og sin leder. Lederinformanten forklarer at han håper at de ansatte har den tilliten, og at de samarbeider tett med IT avdelingen slik at de har muligheten til å henvende seg til han som leder eller til IT avdelingen.

**Produksjonsstøtteavdeling - avdeling 2**

Når vi spurte informantene om de tar informasjonssikkerhet på alvor svarer alle at leder veileder dem til dette. Flere informanter forklarte at det er jevnlig diskusjoner om informasjonssikkerhet ved at det oppstår nye saker eller at det gis påminnelser. På dette

spørsmålet forklarte lederinformanten at han følger de retningslinjene som er satt, og prøver å gå foran som et godt eksempel. Videre forklarte lederinformantene at det blir satt av tid til spørsmål og blir fulgt opp i plenum eller med enkeltpersoner, og at det varierer etter hva som er nødvendig. Lederinformanten forklarer at han tilpasser seg hver enkelt avhengig av den enkeltes behov.

*"Ja, det føler jeg han gjør… absolutt"* (Informant 9, avdeling 2).

*"Ja absolutt. Det liksom hele tiden med de småkursene som kommer at det blir informert om at det nå, husk på de kursene, at dere tar de kursene for nå gjelder det det og det og sånne ting, eh også er det konkrete enkeltsaker hvor det begrepet ligger i hvor man på en måte husk på det og vær obs på det som vi snakket om sist og, det er liksom hele tiden gitt i en eller annen setning da på det så man blir bevisst på det"* (Informant 7, avdeling 2).

Informantene i avdeling 2 var også veldig fornøyd med tilliten mellom seg og leder dersom det dukket opp informasjonssikkerhetsproblemer. De forklarte også at lederen er flink til å gi tilbakemeldinger. Flere av informantene konstaterte også at leder stadig oppfordrer til å innrapportere uønskede hendelser, avvik eller skader. Én informant forklarte at ulike hendelser diskuteres i avdelingen. Lederinformanten forklarte at tilliten oppleves som god, og at det har med den kulturen de har i avdelingen. Lederen har brukt tid på å innarbeide at basen for uønskede hendelser skal brukes som et læringselement i avdelingen.

<u>Inspirerende motivasjon</u>

En leder som er ønsker å holde seg oppdatert og er optimistisk til nye sikkerhetstiltak, vil kunne inspirere ansatte til å følge de nye sikkerhetstiltakene. Vi spurte derfor de ansatte om de synes det var viktig at leder motiverer dem til å fokusere på informasjonssikkerhet, mens vi spurte leder om det var viktig å motivere til å fokusere informasjonssikkerheten.

**Markedsavdeling - avdeling 1**

Fire informanter påpekte viktigheten av motivasjon fra leder. Flere forklarte at dette kan føre til et større fokus slik at de ikke glemmer det bort i en hektisk hverdag. Én informant mente at dette burde være et fokus fra de ansattes side uavhengig av leder, mens en annen informant nevnte at IT avdelingen er den viktigste motivatoren i den forbindelse. En informant mente at det er ansattes eget ansvar å holde informasjonen oppe i forhold til sikkerhetsarbeid.

Lederinformanten sa at det var essensielt og veldig viktig at leder motiverte ansatte til å fokusere på informasjonssikkerhet.

*"Det er jo viktig … det er jo viktig i mange bransjer … særlig i vår. Jo altså han går foran som et godt forbilde på et vis. Ikke sant. Ha litt fokus på det slik at det ikke blir glemt bort på en måte som er hans viktigste oppgave da"* (Informant 1, avdeling 1).

Deretter spurte vi informantene om de opplevde at lederen var engasjert for at de skal gjennomføre kurs og opplæring om informasjonssikkerhet. Samtlige informanter påpekte at lederen sørger for at de kursene som må tas blir tatt og følger opp dette i stor grad. Lederinformanten forklarte at kursene som skal tas følges opp, men nevnte ikke noe utover dette.

**Produksjonsstøtteavdeling - avdeling 2**

På spørsmål om de ansatte synes det er viktig at leder motiverer dem til å fokusere på informasjonssikkerhet svarte alle at dette er en viktig lederoppgave. Én informant forklarte at når en har arbeidet lenge i bransjen ligger mye innunder huden, er det viktig å bli påminnet så det ligger langt fremme i panna i den vanlige hverdagen. Flere informanter nevnte at det er viktig at leder motiverer slik at alle ansatte har fokus på informasjonssikkerhet. En informant nevnte at motivasjon vil påvirke andre ansatte slik at informasjonssikkerheten vil smitte innad i avdelingen. Lederinformanten var enig i at motivasjon er viktig. Dersom ansatte fokuserer på kostnadselementet vil eksempelvis det å sende en epost være billigere enn å sende brev, eller at enkelte av rutinene som skal ivareta sikkerheten kan være tidkrevende. Lederen forklarte at derfor vil motivasjon ved at de ansatte ser at arbeidshverdagen blir enklere og tryggere for både dem selv og kunden vil være vesentlig.

*"Det er superviktig at man blir motivert og informert om ting da så man får det inni den vanlige arbeidsdagen da så det ligger fremst, fordi det er såpass viktig" (*Informant 7, avdeling 2).

Informantene forklarte at lederen sørger for at de gjennomfører de kursene de er pålagt til å ta som kommer fra IT avdelingen og ledelsen. Lederinformanten forklarte at han engasjerer de ansatte ved å ha informasjonssikkerhet på agendaen relativt ofte. Det skal ikke bare være et tema de gangene det har skjedd noe galt, men også når det har skjedd gode ting. Lederen

forklarte videre at det vises til konkrete eksempler, og skaper engasjement ved å ha det oppe som et tema litt oftere enn én gang i året.

Intellektuell stimuli

Intellektuell stimuli innebærer at leder stimulerer den ansattes innsats til å være nyskapende og kreativ ved å stille spørsmål om antagelser, omformulerer problemstillinger og bruke gamle situasjoner til å løse nye problemer. I den forbindelse spurte vi hvordan ledere arbeider for å opprettholde informantenes kompetanse og forståelse i forhold til sikkerhetstiltak og prosedyrer.

**Markedsavdeling - avdeling 1**

Informantene svarte stort sett at dette ikke var noe leder gjorde, og begrunnet det med kursene som kom fra IT avdelingen. Én informant nevnte at det ikke var noe leder gjorde bevisst, men at det ble tatt fortløpende om det oppsto hendelser. Deretter spurte vi informantene hvordan lederen utfordret dem med tanke på tilegning av ny kunnskap om informasjonssikkerhet. Samtlige informanter svarte at dette ikke var noe lederen utfordret dem på.

*«Nei, det utfordrer meg vel egentlig ikke på det. Jeg har ikke noe fokus på det»* (Informant 3, avdeling 1).

Lederinformanten forklarer at dette primært gjøres ved påminnelser om kurs, og at det i utgangspunktet var prisgitt IT avdelingen og andre lenger opp i systemet. Lederen forklarte også at han ikke utfordret de ansatte i noen særlig grad på tilegning av ny kunnskap utover det som kommer fra IT avdelingen og toppledelsen.

**Produksjonsstøtteavdeling - avdeling 2**

Flere informanter forklarer at de opprettholder sin kompetanse og forståelse om sikkerhetstiltak og prosedyrer ved at lederen følger opp dersom det kommer noe nytt. Én informant forklarte at leder tar ting direkte med de ansatte i forhold til de ulike opplæringssituasjonene som er fastsatt av ledelsen høyere opp i systemet. Flere av informantene nevnte at leder er nær og tilgjengelig, og at dette i stor grad påvirker og opprettholder deres kompetanse og forståelse for informasjonssikkerhet. Lederinformanten forklarte at han i stor grad sørger for at de ansatte tar kurs, og følger opp når det kommer noe nytt.

Samtlige informanter synes leder utfordrer dem til å tilegne seg nye kunnskap om informasjonssikkerhet. Én informant forklarte at leder er tilgjengelig og ser hver enkelt ansatt som et selvstendig individ. På denne måten kan lederen oppdage hva hver enkelt trenger for å jobbe med informasjonssikkerhet på en enda bedre måte. En annen informant forklarte at leder følger opp rutinene og vurderer endringer i fellesskap med de ansatte. En annen forklarte at når det kommer noe nytt blir de inkludert av leder, og finner ut hvordan det kan løses i fellesskap. Lederinformanten forklarte at de har en implementeringsløype i banken, og når banken får nye tjenester og produkter vil de også få nye arbeidsverktøy. Lederens oppgave er derfor å sørge for at ansatte klarer å bruke de nye verktøyene, og ikke faller tilbake på de gamle.

# 5. Drøftelse

I denne studien ønsker vi som nevnt å undersøke hvilken rolle lederstil kan spille for informasjonssikkerhetskulturen i en norsk bank. Vi vil drøfte hvorvidt transformasjonsledelse kan bidra til informasjonssikkerhetskultur gjennom de fire i-ene. Det samme vil vi gjøre med transaksjonsledelse og de tre elementene, og se om de påvirker til etterlevelse av regler og rutiner. I dette kapittelet vil vi diskutere funnene mot de teoretiske perspektivene. Vi vil først drøfte hvordan informasjonssikkerhetskulturen er i banken, før vi deretter vil drøfte hvilken rolle lederstil kan spille for denne informasjonssikkerhetskulturen. Avdelingene vil aktivt bli sammenlignet i drøftelsen. Deretter vil vi presentere studiens konklusjon før vi til slutt vil diskutere implikasjoner for teori og praksis.

## 5.1. Informasjonssikkerhetskultur

Informasjonssikkerhetsarbeid i bank er et komplekst område som omfatter lovverk, systemer, og menneskelige forhold. I det følgende vil drøfte hvordan informasjonssikkerhetskulturen er i banken. For å kartlegge informasjonssikkerhetskulturen har vi benyttet oss av dokumentanalyse av gjeldende lovverk og regler som bankvirksomhet er forpliktet til å følge. Vi har også gjennomført intervjuer med IT avdelingen for å få mer utfyllende svar. Disse svarene, i tillegg til dokumentanalysen, har i hovedsak dannet det første nivået i informasjonssikkerhetskulturrammeverket som omhandler artefakter (Niekerk og Solms, 2010; Schein, 1987). Vi gjennomførte intervjuer med ledere og ansatte for å kartlegge de dypere nivåene av informasjonssikkerhetskulturen, som er anerkjente verdier og normer og delte underliggende antakelser. Kunnskapsnivået blir lagt til som en fjerde komponent som er spesielt for en informasjonssikkerhetskultur (Niekerk og Solms, 2010), og baserer seg derfor på all tilgjengelig informasjon. Dette nivået vil støtte og påvirke hvert av de tre andre nivåene i informasjonssikkerhetskulturrammeverket (Niekerk og Solms, 2010; Schein, 1987).

### *5.1.1. Begrepsforståelse*

Informasjonssikkerhet

Analysen viste at det var ulik forståelse rundt begrepet informasjonssikkerhet. I avdeling 1 forklarte to ansatte og lederen at informasjonssikkerhet handlet om håndtering av informasjon. Fire ansatte fikk frem at informasjonssikkerhet handler om integritet og konfidensialitet ved å forklare at informasjonssikkerhet handler om håndtering av informasjon, behandling av personopplysninger og hindre at det kommer på avveie (Datatilsynet, 2018). I avdeling 2 forklarte samtlige ansatte og lederen at informasjonssikkerhet handlet om håndtering av informasjon og behandling av personopplysninger, og fikk dermed frem at informasjonssikkerhet handlet om integritet og konfidensialitet (Datatilsynet, 2018). På grunnlag av det er de ansattes forståelse av begrepet sammenfallende med datatilsynets definisjon som vi har lagt til grunn i kapittel 2.1. Ingen ansatte eller ledere i de to avdelingene forklarer at informasjonssikkerhet dreier seg om å håndtere risiko, eller at det handler om tilgjengelighet eller robusthet (Datatilsynet, 2018). Selv om disse elementene ikke nevnes, kan vi ikke trekke ut noen elementer som vi kan se på som motstridene i forhold til de teoretiske perspektivene. I avdeling 1 er begrepet vagt beskrevet slik at det er lite sammenfallende med definisjonen som er lagt til grunn i kapittel 2.1.

Informasjonssikkerhetskultur

I analysen fremgår det at samtlige ansatte og ledere synes det var vanskelig å forklare begrepet informasjonssikkerhetskultur. Alle forklarte at dette var et begrep de ikke benyttet seg av i det daglige sikkerhetsarbeidet. Enkelte ansatte forsøkte å definere det, men forklarte kun hvordan de arbeider med informasjonssikkerhet. Da Veiga og Eloff (2010) forklarer at informasjonssikkerhetskultur er handlingene, antakelsene, troen, verdien og kunnskapen som de ansatte bruker for å samhandle med systemer og prosedyrer.
Informasjonssikkerhetskulturen kan på denne måten resultere i ulike type atferd som kan være akseptabel eller uakseptabel. Denne atferden vil være tydelig i det som er skapt i banken, og blir en del av måten ting gjøres for å beskytte informasjonsmidlene i banken, og at en slik kultur kan endres over tid. Ingen i avdelingene har vært inne på noen av disse elementene. Enkelte nevnte imidlertid at informasjonssikkerhetskultur handlet om hvordan de jobbet med informasjonssikkerhet og at det var noe som formet seg etter flere år. Dette samsvarer dermed

ikke med definisjonen som legger til grunn om at kulturen kan endres over tid. Det indikerer derfor at informasjonssikkerhetskultur ikke er noe avdelingene bevisst jobber for.

Flere ansatte i begge avdelingene blandet begrepene informasjonssikkerhetskultur og sikkerhetskultur. Informasjonssikkerhetslitteraturen viser også at skillet mellom disse begrepene ikke er stort, som beskrevet i kapittel 2.1.4. Informasjonssikkerhetskultur omhandler informasjon spesifikt og sikkerhetskultur omfatter den totale sikkerheten i virksomheten (AlHogail, 2015; Antonsen, 2009; Da Veiga & Eloff, 2010; Nasjonal sikkerhetsmyndighet, 2014). Etter hvert som vi stilte flere spørsmål ble de fleste mer klar over at dette gjaldt informasjon spesifikt og ikke generell sikkerhet. Selv om ingen i de to avdelingene egentlig vet hva informasjonssikkerhetskultur er, var alle enige i at informasjonssikkerhetskulturen er bra i banken. Ansatte og ledere i begge avdelingene forklarte at informasjonssikkerheten er god fordi rutiner og regler som er satt på området fungerer og følges. Lederne mener at det alltid har vært et stort fokus på informasjonssikkerhet gjennom behandling av sensitive opplysninger, og unngå at viktig informasjon kommer på avveie.

### *5.1.2. Artefakter*

Artefakter utgjør det første nivået i informasjonssikkerhetskulturrammeverket (Niekerk & Solms, 2010; Schein, 1987). Artefakter er det som kan observeres, og er det som Da Veiga & Eloff (2010) omtaler som informasjonssikkerhetskomponenter. Disse komponentene inkluderer policyer, retningslinjer, ledelse og styring. Uten informasjonssikkerhetskomponenter for å rettlede og påvirke ansattes atferd, kan ansatte samhandle med informasjon på måter som kan føre til risiko (Da Veiga & Eloff, 2010). I det følgende vil vi drøfte ansatte og lederes kjennskap til sikkerhetspolicy- og mål, regler, instrukser og personvern og taushetsplikt. Dette vil utgjøre det første nivået i informasjonssikkerhetskulturrammeverket, og vi vil se om det er en forskjell mellom avdelingene.

<u>Kjennskap til sikkerhetspolicy og sikkerhetsmål</u>

I analysen kom det frem at ingen av lederne eller ansatte er kjent med om banken har informasjonssikkerhetspolicy eller sikkerhetsmål. Informasjonssikkerhetspolicyen i banken er utarbeidet av ledelsen, og brukes til å gi ledelsen den nødvendige retning og støtte for

informasjonssikkerhet. En informasjonssikkerhetspolicy har til hensikt å påvirke beslutninger, handlinger og atferd hos ansatte. Den spesifiserer hvilken atferd som blir ansett som akseptabel og ikke. For eksempel nevnte flere av ansatte og lederne at det var viktig å låse datamaskinen når man gikk fra den. Dette er i samsvar med policyen som eksempelvis sier at en datamaskin må være fysisk sikret til enhver tid. Uttalelsen i policyen er rettet mot ansattes atferd for å beskytte både den fysiske eiendelen og dataene som er lagret på datamaskinen. Dersom det ikke fantes en policy som kunne fastsette at dette måtte gjøres, og uten leders håndhevelse, ville det ført til at ansattes datamaskiner ville stått usikret. Dersom dette pågår over tid uten at for eksempel leder griper inn kan det føre til en kultur der svikt blir sett på som akseptabelt (Da Veiga & Eloff, 2010).

Selv om hverken de to lederne eller ansatte var klar over sikkerhetspolicyen, fikk vi vite av IT-avdelingen at dette i utgangspunktet ikke er noe som de skal kunne noe om. Informasjonssikkerhetspolicyen er utarbeidet på et mer overordnet nivå som fastsetter hva som må gjøres for å sikre en god informasjonssikkerhet i banken. En av IT-avdelingens arbeidsoppgaver er å utarbeide konkrete instrukser og rutiner som skal dekke denne policyen. Informasjonen som legges ut på bankens intranett skal sammen med rutinene og instruksene dekke det viktigste policyen fastsetter. Det betyr at IT avdelingen sørger for at ledere og ansatte følger bankens informasjonssikkerhetspolicy uten at de vet det direkte. De vil følge denne policyen indirekte gjennom etterlevelsen av rutiner og instrukser.

Kjennskap til regler og instrukser

Analysen viste at ansatte og ledere i begge avdelingene mente de fulgte regler og instrukser om informasjonssikkerhet. Enkelte nevnte at de sikkert kunne være enda flinkere. Dersom ansatte og ledere følger disse reglene og instruksene i praksis betyr det at informasjonssikkerhetspolicyen også følges. Et eksempel på regler eller instruks som ansatte i bankvirksomhet må følge er å ikke sende eposter i åpne kanaler. En ansatt i avdeling 1 forklarte at det i enkelte situasjoner var fristende å be kundene sende informasjon på epost fordi det var enklere, men at det likevel ikke ble gjort på grunn av strenge regler. Lederen i avdeling 1 forklarte at datadisiplinerklæringen som underskrives ved ansettelse ligger til grunn for alt som ansatte foretar seg. Rutiner og regler er utarbeidet for det meste som gjøres i banken. Flere ansatte i avdeling 2 forklarte at reglene og instruksene som er satt på de forskjellige områdene som legger føringer for hva som skal gjøres for å opprettholde informasjonssikkerhet.

Rutiner var et konsept som både ansatte og ledere snakket mye om. De etableres for å avverge brudd på informasjonssikkerhet og er en viktig prioritering i banken. Lederen i avdeling 2 forklarte at rutiner og prosedyrer henger sammen med flere andre faktorer. De blir gjerne etablert og oppdatert på bakgrunn av risikoanalyser og etterlevelse blir sikret ved at banken foretar intern og ekstern revisjon. Flere ansatte i begge avdelingene påpekte at disse rutinene ligger i "ryggmargen". Et grunnleggende skille mellom avdelingene var at lederen i avdeling 1 hadde en forventning om at ansatte selv sørget for å følge disse rutinene. Leder for avdeling 2 mente at det var en leders oppgave å følge opp og sørge for at de ansatte fulgte rutinene. Ansatte og ledere i begge avdelingene var enige i at etterlevelsen av rutiner ble godt nok gjennomført og hadde høy prioritet i avdelingene. Flere av informantene nevnte at det finnes en rutine for enhver handling, og påpekte derfor at så lenge disse er gode og ansatte følger dem vil informasjonssikkerheten være god. Lederen i avdeling 2 forklarte at rutinene som er satt på de forskjellige områdene fungerer som et verktøy, og skal sørge for at arbeidet gjennomføres på en sikker måte. Rutinene omfatter reglement som banken er pliktig til å følge som eksempelvis IKT-forskriften og personopplysningsloven.

Personvern og taushetsplikt

En grunnleggende del av informasjonssikkerhet er å inkludere all informasjonen i banken. Personvern og taushetsplikt var konsepter som både ledere og informantene snakket mye om. Analysen viser at ansatte og ledere forklarte ulike kontekster som handlet om brudd på informasjonssikkerheten, og hva som måtte gjøres for å følge personvernreglene. Det kunne eksempelvis være når ansatte lar papirer med konfidensielt innhold ligge åpent på pulten, og at banken hadde strenge retningslinjer for å unngå dette. Informasjonssikkerhet innebærer også og ikke sitte i kantinen å snakke om kunder, og unngå å nevne navn dersom saker diskuteres. Det ble også forklart at informasjon som sendes i åpne kanaler må krypteres for å holde sensitiv informasjon skjult. Lederen i avdeling 2 forklarte at etter at personvernloven kom har informasjonssikkerheten blitt mye strengere, som hevdes at kan ha ledet til en bedre informasjonssikkerhetskultur. Etter personopplysningsloven § 2 skal de ansatte verne om fysiske personer i forbindelse med behandling og om utveksling av personlige opplysninger. Dette gjelder både for "helt eller delvis automatisert behandling av personopplysninger og ved ikke automatisert behandling av personopplysninger", jf. Personopplysningsloven § 2. Det betyr at det gjelder for dokumenter som er lagret elektronisk, men også det som ikke er lagret elektronisk. I bank inkluderer dette fysiske dokumenter så vel som muntlig informasjon. Det er viktig å påpeke at den informasjonen som ikke oppbevares elektronisk heller ikke kan

beskyttes med tekniske systemer, det er derfor avgjørende at det gjøres for å sørge for en sikkerhetskultur blant alle ansatte. Disse elementene ble nevnt av at både ansatte og ledere i begge avdelingene og betyr at de er bevisst på håndtering av personopplysninger og taushetsplikt.

### *5.1.3. Anerkjente verdier og normer*

Anerkjente verdier og normer er uskrevne regler og prinsipper som er utviklet og fremmet av organisasjonens ledelse. Disse sier noe om hvilken atferd som anses som akseptabel og hva ansatte anser som viktig. Det handler ikke om dokumentene i seg selv, men den totale verdien som organisasjonen vil leve opp til (Schein, 2010). I banken har vi sett at disse anerkjente verdiene og normene i stor grad handler om å følge rutinene og behandle personopplysninger og sensitiv informasjon med den største forsiktighet. Dette er noe samtlige ansatte og lederne i begge avdelingene er opptatt av. En både uskreven og skreven regel er at rutiner skal følges og sensitiv informasjon og personopplysninger skal beskyttes.  Informasjonen i banken må beskyttes av hensyn til kundene og omdømmet i banken. Begge lederne og flere ansatte påpekte at dersom sensitive opplysninger lakk, ville dette være et stort omdømmeproblem for banken. Dette nivået handler som nevnt ikke om dokumentene i seg selv, og innebærer derfor ikke at ansatte og ledere vet hva disse inneholder. Det handler imidlertid om hvordan de ulike verdiene faller sammen i en større helhet, og dette nivået representeres av summen av disse verdiene. Summen av disse verdiene vil derfor være ansatte og lederes syn på viktigheten av å følge rutiner og regler for å opprettholde god informasjonssikkerhet. Verdiene reflekterer hvordan bedriften ønsker å fremstå, men det er ikke dermed sagt at ansatte handler i henhold til disse (Schein, 1999). Det betyr at selv om informantene sier de er opptatt av å følge rutiner og informasjonssikkerhetsregler og at dette representerer en norm i banken, betyr ikke det at deres atferd samsvarer med det. Dette må derfor ses i sammenheng med de to neste nivåene i kulturrammeverket (Niekerk & Solms, 2010; Schein, 1987).

### *5.1.4. Delte underliggende antakelser*

Delte underliggende antakelser består av ansattes tro og verdier som de deler og som blir tatt for gitt i banken (Schein, 2010). I analysen kom det frem at ansatte generelt i de to avdelingene stoler mye på systemene og rutinene de har. De føler seg trygge på at systemene sørger for at jobben de gjør i forbindelse med informasjonsbehandling er sikkert. Enkelte er

også trygge på at dersom det oppstår hendelser eller situasjoner vil det ikke være et problem fordi IT avdelingen vil ordne det. Én av de ansatte i avdeling 1 sier eksplisitt at IT avdelingen fikser alt, slik at det ikke er et stort behov for å bli god på informasjonssikkerhet. Det ble forklart at det er nok at ansatte klarer å gjøre jobben sin etter de reglene og rutinene som er satt. Disse underliggende antakelsene kan gi en indikasjon på at ansatte og ledere frasier seg ansvar, og i mindre grad bryr seg om informasjonssikkerhet fordi de stoler så mye på systemene og IT avdelingen. Hu et al. (2012) forklarer at det er vanlig at ansvar ofte knyttet til informasjonssikkerhet ofte delegeres til IT-ledere alene uten at ledelsen selv tar ansvar, i den tro at de har den beste IT-staben i selskapet til å ivareta det høyeste nivå av informasjonssikkerhet (Hu et al., 2012). Vårt inntrykk er at disse underliggende antakelsene er mer til stede i avdeling 1, enn i avdeling 2. Grunnen til dette var at det var flere som forklarte at det var viktig å fokusere på informasjonssikkerhet, og flere viste seg å være bevisst på dette i avdeling 2. Niekerk og Solms (2010) påpeker at det er viktig for de ansatte å vite hvorfor en spesifikk kontroll eller sikkerhetsfunksjon er viktig. Det betyr også at det viktig at ansatte vet om bakgrunnen for kursene de tar om informasjonssikkerhet. En ansatt i avdeling 1 påpekte spesifikt at det var mye de ikke skjønte konsekvensen eller rekkevidden av. Dersom ansatte og ledere får denne innsikten kan det medføre en forståelse for at det ikke er nok å stole på systemene og rutinene, men at også bevissthet rundt risiko er viktig. Det vil kunne spille en viktig rolle i å sikre etterlevelse av informasjonssikkerheten (Niekerk & Solms, 2010).

Delte underliggende antakelser finnes også i forbindelse med ansattes og lederes misjon. Misjon utgjør de ikke-eksplisitte tankene og følelsene som motiverer og driver individer eller organisasjoner fremover (Schein, 2010). I arbeidssammenheng er det slik at ansatte er grunnleggende opptatt av å skape organisatoriske resultater i tillegg til at man ofte har mye å gjøre. I bankvirksomhet er det viktig med god service overfor hver enkelt kunde. I mange tilfeller kan fokuset gli bort fra informasjonssikkerhet. Kundebehandlere skal for eksempel kryptere informasjon som skal sendes på epost, men dette er tungrodd og tar lang tid. Én ansatt i avdeling 1 forklarte at det var fristende å sende informasjon i åpen kanal fordi det var enklere. For at ansatte skal virke mest mulig serviceinnstilt overfor kunden kan det derfor tas raskere løsninger som å sende en epost på åpen kanal eller lignende som ikke vil ivareta kundens personopplysninger. Det er også press fra ledelsen at de skal prestere på sine arbeidsområder og at informasjonssikkerhet derfor ikke får noe fokus fordi det er viktigere å

skape gode resultater. Disse har derfor kunden i fokus, ikke informasjonssikkerhet. Ledere er også opptatt av kunden og at ansatte gjør arbeidet sitt på en god måte, og skape gode økonomiske resultater. IT avdelingen er mest opptatt av at systemene er velfungerende og sikre (Da Veiga & Eloff, 2010). Disse forskjellene i misjon var til stede i banken hvor flere ansatte i avdeling 1 forklarte at det ikke var informasjonssikkerhet de hadde mest fokus på. På flere av spørsmålene kom det også frem at enkelte ansatte ikke hadde reflektert så mye rundt informasjonssikkerhetskulturen i banken. Dette er forskjeller som potensielt kan skape brudd på informasjonssikkerheten. Bedre samordning må sannsynligvis til for å få en bedre informasjonssikkerhetskultur (Niekerk & Solms, 2010).

### *5.1.5. Kunnskap*

Kunnskap representerer den fjerde komponenten i informasjonssikkerhetskulturrammeverket (Niekerk & Solms ,2010 ; Schein, 1987). Flere ansatte og lederne i begge avdelingene forklarte at man ikke kan være helt sikker på at man har nok kunnskap om hva som er trygt og utrygt å gjøre fordi potensielle angripere er i forkant. Dette er i samsvar med de teoretiske perspektivene om at kunnskap må inkluderes som et viktig element i informasjonssikkerhetskultur sammenheng (Da Veiga & Eloff, 2010; Niekerk & Solms, 2010).

Analysen viste at ansatte og lederne hadde ulik kunnskap om risiko forbundet med informasjonssikkerhet. Vi presenterte de for to hendelser relatert til informasjonssikkerhet. Ansatte og ledere uttrykte i mindre grad bekymring om hendelsen som omhandlet phishing emails og krav om løsepenger. De var i større grad bekymret for hendelsen som omhandlet personopplysninger på avveie. En årsak til dette kan være at personopplysninger på avveie er noe ansatte i større grad kan relatere seg til og se konsekvensen av fremfor phishing emails. Én informant i avdeling 1 forklarte at dette med phishing emails var langt fra vedkommende sin "sfære". Det kan indikere at dette er noe som ikke blir tatt like alvorlig som personopplysninger på avveie. Det kan også indikere at ansatte ikke klarer å se risikoen på samme måte som de gjør med personopplysninger som de jobber med hver eneste dag. Mer kunnskap om risikoen forbundet med informasjonssikkerhet kan redusere en slik risiko ved at ansatte tar det mer alvorlig (Niekerk & Solms, 2010; Safa & Solms, 2016). Vi ser av analysen at ingen i avdeling 1 er bekymret, mens det tre ansatte i avdeling 2 ytrer bekymring for en slik hendelse. To ansatte i avdeling 2 forklarer at dette er noe de tenker over fordi "kjeltringene"

alltid er et hakk foran. Dette kan indikere at avdeling 2 har mer kunnskap om risiko forbundet med informasjonssikkerhet, og at de har mer fokus på dette. Leder i avdeling 2 forklarte imidlertid at en situasjon med phishing email hvor det kreves løsepenger er noe unge mennesker med et normalt forhold til teknologi har nok kunnskap til å oppdage. Det kan dermed tenkes at grunnen til at de fleste ikke er bekymret for en slik hendelse kan være at de opplever å ha nok kunnskap. Dette må derfor ses i sammenheng med spørsmålet vi stilte om ansatte og lederne hadde nok kunnskap til å vurdere hva som var trygt og utrygt, hvor de sa at de følte seg kompetente nok. Alle i avdeling 1 mener de er kompetente nok, mens tre informanter i avdeling 2 mener at de aldri blir utlært.

I analysen kommer det frem at de fleste ansatte og lederne vet om basen for uønskede hendelser. I avdeling 1 vet fire av seks ansatte hvor det skal rapporteres, men har ikke gjort det enda. Enkelte nevnte at de tror at mange hendelser forblir urapporterte. På denne måten kan det oppstå svikt. I avdeling 2 vet samtlige hvor og hvordan de skal rapportere. Det indikerer dermed at det er større bevissthet og fokus på dette i avdeling 2. Kunnskap og atferd påvirker hverandre på den måten at ansatte og ledere vil bruke informasjonen de har tilgjengelig om informasjonssikkerhet for å ta beslutninger og utføre spesifikke handlinger relatert til denne informasjonen (Niekerk & Solms, 2010).

Læring

Kunnskap om informasjonssikkerhet er nødvendig, og på grunn av rask teknologisk utvikling må det være fokus på dette. Den teoretiske antakelsen er at ikke alle har den nødvendige kunnskapen som behøves (Niekerk & Solms, 2010). I analysen ser vi at enkelte ansatte forklarer at selv om de opplever å den nødvendige kunnskapen til å håndtere informasjon på en sikker måte, er de som utøver kriminalitet "hakket foran". Jevnlig oppdatert informasjon som underbygger bevissthet og forståelse for informasjonssikkerhet er noe banken har i form av korte e-læringskurs som kommer med jevne mellomrom. I avdeling 2 er det større kultur for kunnskapsdeling, hvor analysen viste at ansatte og leder er mer opptatt av å prate om informasjonssikkerhet og lære av hverandres feil. Det er oftere oppe til diskusjon hvor leder i denne avdelingen i større grad tilrettelegger for en slik diskusjon. Kunnskapen ledere og ansatte tilegner seg gjennom opplæring vil påvirke deres bevissthet og atferd forbundet med informasjonssikkerhet (Nikerk & Solms, 2010; Safa & Solms, 2016). Flores & Ekstedt (2016) forklarer at ledere og ansatte kan være bevisst over trusler relatert til informasjonssikkerhet basert på tidligere erfaringer eller interesse, eller ved å gjennomgå spesifikk opplæring om

retningslinjer. Analysen viser at ansatte og ledere i begge avdelingene synes opplæring er viktig for at de skal være bevisste på informasjonssikkerhet. Begge lederne forklarte at jevnlig oppdatert informasjon kan underbygge bevissthet og forståelse for informasjonssikkerhet og er derfor svært nyttig. Dette samsvarer derfor i stor grad med de teoretiske perspektivene (Flores & Ekstedt, 2010; Nikerk & Solms, 2010; Safa & Solms, 2016).

Analysen viste at både ansatte og ledere i begge avdelingene mente det var en kultur for å lære av feil og uhell i banken. Rutinene blir endret dersom det dukker opp hendelser som gjør det nødvendig å justere dem. Det ble påpekt at hensikten med basen for uønskede hendelser er at det som meldes inn skal benyttes for å unngå at liknende hendelser skal skje igjen. På bakgrunn av denne hendelsesbasen blir det gjort endringer i rutiner, og at dette vurderes en gang i året. Det betyr at basen for uønskede hendelser skaper en læringssløyfe både for banken som helhet, men også på individuelt nivå. På denne måten vil ansatte og ledere bli mer bevisst på trusler relatert til informasjonssikkerhet basert på tidligere erfaring (Flores & Ekstedt, 2016). Da Veiga og Eloff (2010) påpeker imidlertid at det kan være krevende å få større mengder med informasjon om sikkerhetsretningslinjer. Enkelte ansatte kan oppleve informasjonen som vanskelig å forstå eller lite relevant for deres arbeid. Det er dermed viktig at lederne involverer seg for å sørge for at ansatte forstår retningslinjene, og forklarer hensikten med retningslinjene.

Atferd

Informasjonssikkerhetskomponentene som er omtalt under kapittel 5.1.2 om artefakter vil i stor grad ha en innvirkning på informasjonssikkerhetsatferden i organisasjonen (Da Veiga & Eloff, 2010). Rutinene og instruksene i banken legger i stor grad føringer for hvordan ansattes og lederes informasjonssikkerhetsatferd kan bidra til beskyttelse av informasjonen. En slik atferd kan eksempelvis være rapportering av sikkerhetshendelser og sikker avhending av fortrolige dokumenter (Da Veiga & Eloff, 2010; Robbins, 2001). Analysen viste at flere ansatte i avdeling 1 undersøkte linker, eposter og nettsider før de åpner eller bruker det, mens enkelte ikke gjorde det. Samtlige i avdeling 2 fortalte at de undersøkte, særlig linker og var bevisste på risiko forbundet med dette. Flere i denne avdelingen forklarte at de har opparbeidet seg en del forståelse og bevissthet omkring tegn ved både nettsider, linker og eposter som er mistenksomme, og velger å sjekke over en ekstra gang. Flere ansatte i begge avdelingene forklarte at de var bekymret for enkelte kollegaers informasjonssikkerhetsatferd, hvor det ble spåstått at enkelte gikk ubevisst inn på usikre nettsider og lignende.

Dersom ansatte synes innholdet i informasjonssikkerhetspolicyen og retningslinjene er vanskelig å forstå eller anser det for ikke å være relevant for deres arbeid, er det ikke sikkert at de overholder det. På denne måten vil informasjonssikkerhetskomponenten som er implementert være ineffektiv slik at ansatte selv kan utgjøre en potensiell trussel for informasjonssikkerheten (Da Veiga & Eloff, 2010; Robbins, 2001). Vi har tidligere nevnt i kapittel 5.1.2 at ansatte forholder seg til policyen gjennom rutiner og prosedyrer. Ansatte og ledere i banken påpeker at de synes rutinene og reglene er enkle å forstå og følge. Det betyr at det ikke kan være en årsak til at enkelte i avdeling 1 velger å ikke undersøke linker, eposter og nettsider. Ansatte og ledere påpeker også at de er flinke til å følge disse. Dette indikerer at informasjonssikkerhetskomponentene som er implementert fungerer på en god måte og således føre til en effektiv informasjonssikkerhetsatferd (Da Veiga & Eloff, 2010; Robbins, 2001). Likevel ser vi at når enkelte ansatte i avdeling 1 ikke undersøker at den informasjonen de får tilsendt kan dette føre til informasjonssikkerhetsbrudd.

### *5.1.6. Hjemmekontor*

På grunn av Covid-19 har en rekke ansatte i norsk og utenlandsk næringsliv måtte ta med seg arbeidet hjem. Ansatte forsøker å gjøre den samme jobben som før bare at det nå foregår hjemmefra. Dette betyr at behandling av informasjon ikke er beskyttet av de samme systemene og prosessene som eksisterer på arbeidsplassen. De fleste informantene i avdeling 2 forklarte at de har opparbeidet seg en del forståelse omkring tegn ved både nettsider, linker og eposter som gjør dem mistenksomme og velger å sjekke over en ekstra gang. Én informant svarte at det nok ikke var alltid det ble undersøkt, men at dette i større grad gjaldt utenfor jobben. Flere er flinkere til å undersøke og ikke gå inn på "skumle" nettsider på jobb. På et hjemmekontor kan dette være lettere å glemme bort, og enkelte bruker arbeidsdatamaskinen i privat sammenheng også. Det er fortere å glemme at man faktisk er på jobb. Det påpekes som en utfordring at grensen jobb/hjemme ikke eksisterer. Dette vil gjøre at informasjonssikkerhetskulturen blir mindre og vanskeligere å "dyrke", men desto viktigere. Norsis forklarer viktigheten av at virksomheter tar grep for å gjøre hjemmekontoret sikrere for å ivareta informasjonssikkerhet (NorSIS, 2020). Det er mange ansatte og ledere som ikke har hatt hjemmekontor tidligere og har manglende kunnskap som kan skape sikkerhetsrisiko. Den manglende kunnskapen øker risikoen for at virksomheten kan oppleve trusler eller sikkerhetsangrep. Det å sitte på et hjemmekontor vil være mer utrygt enn å sitte på kontoret

(NorSIS, 2020).

### *5.1.7. Informasjonssikkerhetskulturen i avdelingene*

Informasjonssikkerhetskulturen i banken vil som tidligere forklart avhenge av de fire nivåene i informasjonssikkerhetskulturrammeverket (Niekerk & Solms, 2010; Schein, 1987). Dokumentanalysen og samtalen med IT-avdelingen viste at banken hadde fokus på informasjonssikkerhet overordnet i banken. Det kom også frem at banker tradisjonelt sett har en god informasjonssikkerhetskultur. En virksomhet kan imidlertid ha forskjellig informasjonssikkerhetskultur i de ulike avdelingene (Niekerk & Solms, 2010; Schein, 1987). Det betyr at selv om informasjonssikkerhetskulturen fremstår som god overordnet i banken, kan det for eksempel være enkelte avdelinger som har svakheter. I det følgende vil vi oppsummere funnene som er presentert over og forklare hvordan informasjonssikkerhetskulturen er i avdelingene.

Artefaktene utgjør det første nivået, og skal påvirke informasjonssikkerhetsatferden direkte. Samtlige ansatte og ledere kjenner godt til og sørger for å følge personvernreglene, taushetsplikt og rutinene som er satt på området. Informasjonssikkerhetskomponentene som er implementert fungerer dermed på en god måte og fører således til en effektiv informasjonssikkerhetsatferd, og det er ingen forskjell mellom avdelingene på dette nivået (Da Veiga & Eloff, 2010; Niekerk & Solms, 2010; Schein, 1987). Anerkjente verdier og normer utgjør det neste nivået, og handler om hvordan de ulike verdiene faller sammen i en større helhet som sier noe om hvilken atferd som er akseptabel og ikke. I banken representerer dette ansatte og lederes oppfatning av viktigheten av å følge regler og rutiner. Vi har ikke identifisert noen forskjeller mellom avdelingene på dette nivået, og det virker som at dette er verdier som er anerkjent i banken som helhet. For å kunne si noe om informasjonssikkerhetskulturen må vi videre se hvilke delte underliggende antakelser som finnes i avdelingene (Niekerk & Solms, 2010; Schein, 1999).

For å virkelig forstå hva informasjonssikkerhetskulturen og kunne fastslå helheten av gruppens verdier og åpenbare atferd, er det avgjørende at man fordyper seg i de delte underliggende antakelsene (Schein, 2010). Delte underliggende antakelser utgjør det tredje nivået i kulturrammeverket, og består som forklart i punkt 5.1.3 av ansatte og lederes tro og verdier som blir tatt for gitt (Niekerk & Solms, 2010; Schlienger & Teufel, 2003; Schein,

2010). Ansatte og ledere i begge avdelingene føler seg trygge på systemene og stoler på IT avdelingen dersom det skulle oppstå hendelser. Denne underliggende antakelsen er mer til stede i avdeling 1. I avdeling 2 er det mer fokus på og fremstår som mer bevisste på informasjonssikkerhet. En annen underliggende antakelse vi identifiserte var i forbindelse med misjon (Schein, 2010). Ansatte, ledere og IT fagarbeidere er grunnleggende opptatt av sine primære arbeidsoppgaver. Dette betyr at det er grunnleggende forskjeller i deres syn på hva som er viktig å gjøre i banken. Særlig avdeling 1 er det flere som nevner at de har mye å gjøre i forbindelse med sine primære arbeidsoppgaver, slik at det ikke ligger et stort fokus på informasjonssikkerhet.

Kunnskap er det fjerde nivået i informasjonssikkerhetskulturrammeverket hvor også læring og informasjonssikkerhetsatferd omfattes (Niekerk & Solms, 2010). Ansatte i avdeling 1 var i mindre grad bekymret for risiko forbundet med phishing emails, hvor enkelte forklarte at dette var en situasjon som var vanskelig å relatere seg til. Det kan som forklart under punkt 5.1.4 indikere at de i mindre grad klarer å se risikoen forbundet med en slik hendelse. Det kom også frem av analysen at ansatte i avdeling 1 i mindre grad visste hvor og hvordan de skal rapportere uønskede hendelser, avdeling 2 hadde i større grad kunnskap om dette.

Avdeling 2 har også mer kunnskap om begrepene informasjonssikkerhet og informasjonssikkerhetskultur og klarte i større grad å redegjøre for disse. På generelt grunnlag kan vi derfor si at avdeling 2 har mer kunnskap og bevissthet om hvordan de skal sørge for informasjonssikkerhet. Det var mer kultur for å lære av hverandres feil i avdeling 2 hvor leder tilrettela for diskusjoner. Lederen skapte dermed muligheter for læring og kunnskapsdeling (Flores & Ekstedt, 2016; Nikerk & Solms, 2010; Safa & Solms, 2016).

Atferd påvirker alle nivåene som er omtalt. Kunnskap og atferd er interrelaterte menneskelige egenskaper som påvirker informasjonssikkerheten, hvor mangel på kunnskap vil ha en stor innvirkning på informasjonssikkerhetsatferden (Niekerk & Solms, 2010; Thomson et al., 2006). Ut fra definisjonen vi la til grunn i kapittel 2 er det klart at informasjonssikkerhetskultur er noe avdelingene har. Informasjonssikkerhetskulturen dannes på bakgrunn av holdningene, antakelsene, troen, verdien og kunnskapen ansatte har for å kunne samhandle med organisasjonens systemer og prosedyrer. Samspillet mellom informasjonssikkerhetskomponentene som omtalt i kapittel 2.2.5 og atferden til ansatte vil ha en innvirkning på den resulterende informasjonssikkerhetskulturen. Informasjonssikkerhetskultur skal sikre informasjonen fysisk og logisk, og omfatter også

lovkrav og forskrifter som omtalt i kapittel 2.1.1. Dette blir så en del av måten ting gjøres i banken for å beskytte informasjonsmidlene, og danner en informasjonssikkerhetskultur som kan endres over tid (Da Veiga & Eloff, 2010). Alle ansatte og ledere vet hva som er akseptabel og uakseptabel atferd i forbindelse med informasjonssikkerhet. Rutinene og instruksene i banken legger i stor grad føringer for hvordan ansatte og lederes informasjonssikkerhetsatferd kan bidra til beskyttelse av informasjonen. Flere i avdeling 2 så ut til å ha en bevisst atferd ved å undersøke linker, eposter og nettsider. Alle i avdelingene synes rutinene og instruksene var enkle og forså. Det betyr at det ikke kan være en årsak til at enkelte i avdeling 1 velger å ikke undersøke linker, eposter og nettsider (Da Veiga & Eloff, 2010; Niekerk & Solms, 2010; Thomson et al., 2006).

På bakgrunn av nivået delte underliggende antakelser og kunnskapsnivået kan vi anta at avdeling 2 har en bedre informasjonssikkerhetskultur enn avdeling 1. Leder i avdeling 2 er mer bevisst på informasjonssikkerhet og inkluderer sine ansatte for å jobbe mot det, og dette gjenspeiles i de ansattes kunnskapsnivå og bevissthet. På denne måten kan det argumenteres for at ledere må sørge for å ta initiativ, motivere og legge forholdene til rette for innføring og oppfølging av arbeidet med informasjonssikkerhet, og på denne måten skape en bedre informasjonssikkerhetskultur slik som leder for avdeling 2 har gjort. Nå i disse dager byr hjemmekontor på flere utfordringer tilknyttet informasjonssikkerhet, og leder har i mindre grad mulighet til å påvirke informasjonssikkerhet.

## *5.2. Lederstil*

I det følgende vil vi drøfte hvorvidt lederne har kvaliteter til transformasjonsleder eller transaksjonsleder i forhold til informasjonssikkerhet. Det er viktig å få frem at dette kapittelet omhandler tolkninger med bakgrunn i de innsamlede informasjonene fra analysen. Vi vil først ta for oss transformasjonsledelse og de fire i´ene og for deretter å se på transaksjonsledelse og de tre grunnleggende elementene (Bass,1990). Det er muligheter for at noen av under elementene vil forekomme som lite relevante for vår forskning.

### *5.2.1. Transformasjonsledelse*

Vi har valgt å sette opp drøftelsen av transformasjonsledelse på samme måte som analysekapittelet: idealisert innflytelse, inspirerende motivasjon, intellektuell stimuli og individualisert oppmerksomhet (Bass, 1990). Transformasjonsledelse handler om det som er best for gruppen og felleskapet. Det beste for felleskapet utgjøre det som er best for virksomheten ifølge teorien til Bass (Avolio et al., 2003; Bass 1985; Bass 1990). Vi vil drøfte forskjellene mellom lederne i avdelingene for å se hva slags lederstil de bruker for å praktisere informasjonssikkerhet før vi til slutt vil drøfte hvordan informasjonssikkerhetskulturen påvirkes.

Idealisert innflytelse

I analysen så vi at lederne har fokus på informasjonssikkerhet og hvordan de involverer ansatte i informasjonssikkerhetsarbeidet og ved endringer. Det viste seg at flere ansatte i avdeling 1 mente at leder hadde lite fokus på informasjonssikkerheten, men hadde kontroll på dette selv. Dette indikerer at lederen i avdeling 1 ikke aktivt er engasjert i informasjonssikkerhetsarbeidet. På bakgrunn av ansattes meninger om lederen finner vi ingen trekk for idealisert innflytelse som eksempelvis engasjerende eller fremstår som rollemodell for informasjonssikkerhetsarbeid (Avolio et al, 2003). I avdeling 2 forklarte ansatte at lederen har fokus på informasjonssikkerhet og kan komme med tips og råd. Lederen er også opptatt av å involvere alle ansatte ved nye endringer som er viktig for informasjonssikkerheten. Leder i avdeling 2 er engasjerende i informasjonssikkerhetsarbeidet og har tillitt til sine ansatte. I avdeling 2 fremstår lederen som en rollemodell for sine ansatte gjennom sitt engasjement og bevisstgjøring om informasjonssikkerheten (Avolio et al, 2003; Avolio & Bass, 1994; Bass, 1990; Hwang et al., 2019; Leidner og Kayworth, 2006). I avdeling 2 får de både individuell oppfølging og som en helhetlig gruppe. Lederen i avdeling 2 fortalte at de ikke har noen direkte mål for å ivareta informasjonssikkerheten, men at rutiner og regler er de faktorene de forholder seg til ved ivaretagelse av informasjonssikkerheten. Atferden som lederen utviser i forhold til rutiner og regler vil kunne ha en innvirkning på utviklingen av informasjonssikkerhetskulturen i banken. God tillitt mellom ansatte og leder kan være med på å skape en "riktig" type atferd (Da Veiga &Eloff 2010).

Individualisert oppmerksomhet

I analysen kommer det frem at begge avdelingene mener at lederne veileder de til å ta informasjonssikkerhet på alvor. Vi spurte lederne om de veileder ansatte når det kommer ny informasjon eller endring av sikkerhetsstandarder. Det kommer frem at lederen i avdeling 1 ikke direkte veileder ansatte til å ta det på alvor, men at det ligger en forventning om at rutinene og reglene som de er pålagt tas på alvor. Det kan antas gjennom de ansattes svar at rutiner og kursene tar for seg alvoret rundt informasjonssikkerheten, og at det forventes at ansatte ser alvoret selv. I avdeling 1 ser vi ingen direkte tilknytning til at leder har hovedtrekkene til individualisert oppmerksomhet der en leder skal se ansattes behov (Avolio et al., 2003; Bass, 1990). Det som legges til grunn er at ansatte i avdeling 1 skal forstå alvoret av ivaretagelse av sikkerheten ved kurs og rutiner.

I avdeling 2 mente alle ansatte at lederen tok informasjonssikkerheten på alvor og kunne diskuterer dette på avdelingsmøter. Lederen i avdeling 2 sier at nye retningslinjer følges opp, og prøver å gå foran som et godt eksempel for de ansatte. I avdeling 2 har leder mer fokus på at ansatte kan komme med spørsmål under avdelingsmøter. I informasjonssikkerhetslitteraturen påpekes viktigheten av å ha muligheten til å stille spørsmål siden det kan eksistere forskjellig synspunkt på informasjonssikkerhet gjennom regler og lover som skal følges (Da Veiga & Eloff, 2010). Individualisert oppmerksomhet handler om det at lederen ser de ansatte på individnivå og tilpasser seg den enkeltes behov. Det er slik at ansatte behandles likt i form at alle skal kunne få den samme behandlingen. Det er et støttende miljø i avdelingen der alle spørsmål er aksepterte og det ligger en forståelse av at ansatte kan ha forskjellige behov ved læring (Avolio et al., 2003; Bass, 1990). Leder i avdeling 2 har karakteristikker fra lederstilen individualisert oppmerksomhet. Lederen har skapt en kultur for å stille spørsmål angående informasjonssikkerhet og lederen bruker tid på sine ansatte for å få nødvendig kunnskap på plass. Leder har en støttende adferd til sine ansatte og ikke har noe problem med å ta opp endringer eller brudd på regler eller standarder i møter med de ansatte (Avolio et al., 2003; Bass, 1990; Da Veiga & Eloff, 2010).

Inspirerende motivasjon

I analysen kommer det frem at motivasjon er viktig for ansatte i begge avdelingene, slik at de har fokus på informasjonssikkerheten. I avdeling 1 er det mange av de ansatte som påpeker at en motiverende leder er viktig, men det kommer ikke frem at lederen deres er motiverende i

informasjonssikkerhetsarbeidet. Leder i avdeling 1 kunne ha hatt mer bevissthet om informasjonssikkerhet. Dette kan indikerer at lederen i avdeling 1 har lite fokus på å motivere ansatte når vedkommende ikke har noe bevissthet rundt det. Vi fikk forskjellige svar fra ansatte rundt spørsmålene tilknyttet motivasjon. Vi ser at en mulig årsak kan være lite refleksjon rundt dette spørsmålet. Det er derfor ikke mulig å si om lederen i avdeling 1 er motiverende eller ikke når det gjelder informasjonssikkerhet.

Leder avdeling 2 mener at det å motivere sine ansatte til å fokusere på informasjonssikkerhet er viktig for å skape tryggheten for ansatte. Ansatte i denne avdelingen syntes lederen motiverer dem til å fokusere på informasjonssikkerhet. Vi får ikke noe informasjon fra de ansatte på hva lederen gjør for å motivere de, som eksempelvis å se meningen bak informasjonssikkerhetarbeidet (Avolio et al., 2003; Bass 1985). Vi ser en mulig årsak til dette er at det ikke er satt noe fremtidig sikkerhetsmål som lederen kan motivere sine ansatte mot (Bass, 1990; Hetland, 2004). Fordi det ikke er satt noen sikkerhetsmål vil det være vanskelig å motivere ansatte til informasjonssikkerhet arbeid. En annen mulig årsak er at denne lederstilen ofte brukes ved implementering av nye sikkerhetssystemer eller ved endring av standarder der leder er optimistisk til å ta det i bruk (Hao og Padman, 2016). Lederen motiverer til å ta i bruk sikkerhetssystemene eller standardene. Vi har tatt for oss bankvirksomheten slik den fremstår i dag, og det er ingen implementeringer av nye sikkerhetssystemer eller standarder som leder kan motivere mot. Vi ser at en annen grunn til lite støtte for denne ledelsesstilen er at lederne stoler såpass på IT avdelingen. På denne måten fremstår det som at det er IT-avdelingen sitt arbeid å motivere ansatte, og ikke leder (Hu et al., 2012). Denne lederstilen har ikke gitt noe informasjon om hva leder gjør for å motivere sine ansatte mot informasjonssikkerhet og derfor vil ikke denne lederstilen være relevant for å se relasjonen mellom lederstil og informasjonssikkerhetskultur.

Intellektuell stimuli

Det er viktig at en leder er til stede for sine ansatte når det kommer nye regler eller standarder. Ansatte skal ha mulighet til å stille spørsmål ved reglene og instrukser slik at de oppfatter de slik de var ment (Avolio et al., 2003; Bass, 1990; Da Veiga & Eloff, 2010). I avdeling 2 har ansatte bekreftet at de har mulighet til å stille spørsmål om det skulle være behov. De fleste ansatte følte at lederen utfordret dem til å tilegne seg ny kunnskap og opprettholde sin kompetanse. Lederen fulgte de opp dersom det kom nye informasjonssikkerhetsendringer.

Gjennom e-læringskursene skal ansatte ha samme grunnlaget for å tilegne seg ny kunnskap. Det vil derfor være lederens ansvar at ansatte utfører e-lærings kursene som IT avdelingen utvikler. I avdeling 1 har ansatte samme e-lærings kurset som avdeling 2. Det som kommer i mindre grad frem ved avdeling 1 er om ansatte har mulighet til å stille spørsmål ved nye regler eller standarder. De ansatte antar at leder ville ha svart på spørsmål, men det kommer ikke frem om dette er noe som har skjedd på avdelingen. Det er kursene IT avdelingen sender ut som skaper muligheter for ansatte til å tilegne seg ny kunnskap og opprettholde sin kompetanse.

Det vi ser i forskningen rundt intellektuell stimuli er at lederadferd er av mindre betydning siden det ofte handler om at de ansatte skal kunne utvikle sin kreativitet og være nyskapende under sin leder (Avolio et al., 2003; Bass, 1990). Sistnevnte er svært vanskelig å oppnå når informasjonssikkerheten er bestemt gjennom ulike regler, standarder og rutiner. Det er vanskelig for leder å la sine ansatte være nyskapende når regler og standarder er fastsatte. Vi kunne muligens fått bedre svar dersom vi skulle besvart en problemstilling som omhandlet implementering av et nytt system. Det vi kan vektlegge ved intellektuell stimuli er at ansatte kan stille spørsmål ved nye rutiner eller regler (Avolio et al., 2003; Bass, 1990). Ansatte har ikke mulighet til å være nyskapende siden kursene lages av IT avdeling, og fordi de kun er pliktig til å gjennomføre kursene etter kursets formål. Denne lederstilen vil derfor være av mindre betydning for vår forskning som omhandler informasjonssikkerhet i en bank i nåtid. Dersom vi hadde fokusert på banken i en implementeringsprosess ville intellektuell stimuli vært mer relevant.

### *5.2.2. Transaksjonsledelse*

I det følgende vil vi drøfte de tre transaksjonsledelses elementene: ledelse ved unntak (aktivt), ledelse ved unntak (passivt) og laissez faire (Avolio et al., 2003; Bass, 1990). I analysen har vi ikke stilt direkte spørsmål tilknyttet transaksjonsledelse siden vi finner svar i transformasjonsledelse. Transaksjonsledelse handler om at leder ser ansattes behov og belønner ansatte for prestasjon (Avolio & Bass, 2004). Vi ser ikke så mye på dette med belønning, men har fokuset på om leder griper inn ved avvik eller sikkerhetsbrudd (Bass,1990).

Ledelse ved unntak (aktiv)

I analysekapittelet om transaksjonsleder finner vi at leder i avdeling 2 har et tett samarbeid med sine ansatte og at det er, som nevnt tidligere, muligheter for å stille spørsmål. Leder i avdeling 2 følger opp sine ansatte når det gjelder regler og rutiner, og kommer med tilbakemeldinger. Vi har gjennom informasjon fra de ansatte en forståelse for at leder av avdeling 2 har oversikt over sine ansatte, og griper inn før det oppstår avvik, rutinebrudd eller informasjonssikkerhetsbrudd. På denne måten vil denne lederen ha trekk fra ledelse ved unntak aktivt (Antonakis et al., 2003; Avolio et al., 1999; Guhr & Breitner, 2018). På denne måten kan vi se at leder i avdeling 2 har elementer i samsvar med både transformasjonsleder og transaksjonsleder. Denne lederen er interessert i å få alle ansatte til å følge rutiner og standarder for å redusere informasjonssikkerhetsavvik. Basert på ansattes meninger brukes det kort tid på å håndtere eventuelle sikkerhetproblemer som dukker opp (Avolio et al., 2003).

I avdeling 1 tar leder informasjonssikkerhet på alvor, men har ikke like stort fokus på det. De ansatte i avdeling 1 syntes det ikke er så stor bevissthet rundt dette med informasjonssikkerhet. Det kan bety at ansatte i avdeling 1 har mer ansvar for å følge rutiner som ivaretar informasjonssikkerheten. Vi har ikke fått forskjellige svar fra ansatte og lederen selv til å kunne et ta standpunkt til om leder i avdeling en omfattes av ledelse ved unntak (aktivt). Det er ingen klare trekk til ledelse ved unntak (passivt) som gjør at vi kan si at leder i avdeling 1 faller innunder denne lederstilen (Avolio et al., 2003).

Ledelse ved unntak (passiv)

I analysen av transaksjonsledelse kommer det frem at lederen i avdeling 1 ikke selv var med på å skape bevissthet rundt informasjonssikkerhet, men enkelte ansatte fortalte at det var en kultur for informasjonssikkerhet gjennom rutinene og instruksene. Det kom også frem i analysen at leder ikke har noe fokus på dette med informasjonssikkerhet, men at ansatte gjorde det de skulle. De funnene vi har gjort av leder av avdeling 2 indikerer at lederen følger opp sine ansatte og har god kontroll på å opplyse de om situasjoner av vesentlig betydning for informasjonssikkerheten. Ledelse ved unntak (passivt) sine hovedtrekk handler om at lederen griper inn i situasjoner når det har skjedd sikkerhetsbrudd eller brudd på regler og rutiner i virksomheten (Antonakis et al., 2003; Bass, 1990). Den informasjonen vi har fått innenhet fra de ansatte fra avdeling 2 vil si at denne lederen handler før situasjoner oppstår. Dette er derfor ikke en lederstil som praktiseres av leder i avdeling 2. Kjennetegnene ved ledelses ved unntak (passivt) er at ansatte har mye ansvar og bestemmer selv hvordan de skal håndtere

sikkerhetsregler eller standarder (Antonakis et al., 2003; Bass, 1990; Guhr & Breitner, 2018). Dette er noe vi ser mer av i avdeling 1, der ansatte snakker om det å følge regler og standarder er noe som sitter i "ryggmargen". I analysekapitlet om intellektuell stimuli kommer det frem at leder i avdeling 1 ikke arbeidet spesifikt for å opprettholde informantens kompetanse i forhold til sikkerhetstiltak og prosedyrer. Ansatte får kurs fra IT-avdelingen som skal ivareta deres kompetanse og læring. Ansatte har selv mye av ansvaret for å følge opp rutinene selv og bruke kompetansen fra kursene. Dersom det skulle dukke opp spørsmål angående rutiner og regler vil lederen av avdeling 1 komme med tilbakemeldinger for å oppklare uklarhetene. På bakgrunn av dette kan vi argumentere for at leder i avdeling 1 omfattes av denne lederstilen.

Laissez-faire-lederstil

Denne lederstilen handler om at lederen ikke tar ansvar eller beslutning (Bass, 1990). Vi finner ingen trekk ved leder i avdeling 2 for denne lederstilen, og vil derfor ikke omfattes av denne lederstilen. I avdeling 1 kan vi se noen trekk ved denne lederstil som blant annet at leder ikke har fokus på informasjonssikkerhet. Det er likevel slik at lederen er opptatt av at de ansatte skal ta kursene IT avdelingen sender ut for å øke kompetanse rundt informasjonssikkerhet noe som vil bety at lederen tar på seg ansvar. I analysen ser vi at leder i avdeling 1 bidrar når dersom det oppstår informasjonssikkerhetshendelser. Laissez-faire vil ikke være av betydning for vår oppgave siden ingen av lederen skyver fra seg ansvar eller beslutninger (Avolio et al., 2003; Bass, 1990).

## *5.3. Lederstil og informasjonssikkerhetskultur*

Vi vil i dette kapittelet drøfte hvilken betydning lederstilen til de to avdelingslederne har for informasjonssikkerhetskulturen, og med dette vil vi besvare vår problemstilling. Leder i avdeling 2 har trekk fra både transformasjonsleder (idealisert innflytelse og individualisert oppmerksomhet) og transaksjonsledelse (ledelse ved unntak aktivt) (Allen et al., 1995; Avolio et al., 2003; Bass, 1990). Lederen ved avdeling 1 har trekk hovedsakelig fra transaksjonsleder (ledelse ved unntak passivt) (Avolio et al.,1999; Bass,1990). Informasjonssikkerhetskulturen fremstår som god i begge avdelingene. Artefaktene og anerkjente verdier og normer representerer ingen forskjell mellom avdelingenes informasjonssikkerhetskultur. Delte underliggende antakelser og kunnskap viste imidlertid at det er en forskjell i avdelingenes

informasjonssikkerhetskultur. På bakgrunn disse kulturnivåene kan vi anta at avdeling 2 har en bedre informasjonssikkerhetskultur enn avdeling 1. I det følgende vil vi drøfte hvorvidt denne forskjellen kan ha noe med påvirkning fra leder å gjøre.

Idealisert innflytelse spiller en rolle for kunnskapsnivået

Avdeling 2 er i større grad flinkere på å rapportere uønskede hendelser, avvik eller skader, hvor leder har innarbeidet en kultur i avdelingen for å lære av hverandre feil og uhell. Vi ser at dette er positivt relatert til ansattes kunnskap om hvor og hvordan uønskede hendelser skal rapporteres. De har dermed en sikkerhetsatferd som bidrar til å beskytte informasjon (Da Veiga & Eloff, 2010; Niekerk & Solms, 2010; Robbins, 2001). Denne lederen bruker tid på å snakke om det i møter og skaper et engasjement blant ansatte i avdelingen som gjør at de har generelt mer fokus på dette. Vi ser at leder i avdeling 2 har skapt tillit til sine ansatte som former en åpenhet i avdelingen for å lære av hverandres feil (Avolio et al, 2003; Avolio & Bass, 1994; Bass, 1990; Hwang et al., 2019; Leidner & Kayworth, 2006). I avdeling 1 blir det også rapportert uønskede hendelser, og ansatte forklarer at de har god relasjon til sin leder. Det er imidlertid færre ansatte i denne avdelingen som vet hvor og hvordan disse hendelsene skal rapporteres. Denne lederen har ikke like stort fokus til å ta opp informasjonssikkerhet på møter i like stort omfang som leder i avdeling 2. Leder i avdeling 1 skaper ikke like stort engasjement rundt det, og kan derfor være en årsak til at hendelsene ikke rapporteres i like stor grad som i avdeling 2. På bakgrunn av dette kan det argumenteres for at idealisert innflytelse kan spille en positiv rolle for kunnskapsnivået i informasjonssikkerhetskulturrammeverket fordi idealisert innflytelse fører til større bevissthet, sikkerhetsatferd, tillit og læring i avdelingen (Avolio et al., 2003; Avolio & Bass, 1994; Bass, 1990; Da Veiga & Eloff, 2010; Hwang et al., 2019; Leidner & Kayworth, 2006; Robbins, 2001; Schein, 1987).

Rutiner og instrukser ligger til grunn i informasjonssikkerhetskulturen i banken, og er en beskrivelse av hvordan arbeidsoppgavene skal gjøres. På denne måten kan rutiner erstatte leders mulighet for bevisstgjøring og læring. Dette er noe vi ser som mulig utfall i avdeling 1 der lederen ikke ser behovet for å skape mer bevissthet rundt informasjonssikkerhet. Det kan være fordi de ansatte allerede skal ha fått denne kunnskapen gjennom e-læringskursene og rutinene. Mer fokus på det sees ikke på som nødvendig siden de ansatte skal kunne det fra før. Det at lederen ikke har mer bevissthet rundt informasjonssikkerhet kan være en årsak til at de ansatte er mer usikre på dette med å innrapportere uønskede hendelser og avvik i avdeling 1

(Avolio et al, 2003; Avolio & Bass, 1994; Bass, 1990; Hwang et al., 2019; Leidner & Kayworth, 2006). Det er enkelte i avdeling 1 som mener at det ikke er leders rolle å ha fokus på informasjonssikkerhet siden det er IT sitt ansvarsområde. En antagelse om grunnen til at leder i avdeling 1 viser lite engasjement til informasjonssikkerhet kan skyldes de delte underliggende antakelsene. Disse handler om at IT-avdelingen har ansvar for informasjonssikkerheten, og at leders rolle er av mindre betydning i den forbindelse.

Individualisert oppmerksomhet spiller en rolle for kunnskapsnivået

Sikkerhetsbevissthet rundt rutiner og instrukser er en viktig faktor for å redusere risikoen forbundet med brudd på informasjonssikkerhet. Mer kunnskap om dette kan redusere usikkerheten til ansatte slik at de eksempelvis ikke sender ukrypterte eposter i åpne kanaler eller lager lette passord (Niekerk & Solms, 2010; Safa & Solms, 2016; Norsis, 2016). Leder for avdeling 1 har en forventning om at ansatte følger og tar rutinene og reglene på alvor. Leder i avdeling 1 har eksempelvis ikke møter hvor dette tas opp som et eget tema eller diskuteres blant avdelingens ansatte. Ansatte får kunnskap om informasjonssikkerhet gjennom kursene som kommer fra IT avdelingen. Jevnlig oppdatert informasjon gjennom e-læringskurs fra IT avdelingen kan underbygge bevissthet og forståelse for informasjonssikkerhet. På denne måten stammer ikke kunnskapen og bevisstheten ansatte får om informasjonssikkerhet fra sin nærmeste leder. Når det kommer nye sikkerhetsregler eller rutiner kan det være vanskelig for ansatte å forstå disse, og relatere de til sitt eget arbeid. Det er derfor viktig med en leder som hjelper hver enkelt, ser og skaper et støttende miljø slik at det skapes læringsmuligheter (Avolio et al., 2003; Bass, 1990). En leder som behandler hvert enkelt individ ulikt avhengig av deres behov og ferdigheter vil være viktig for å skape bevissthet rundt de nye rutinene slik at de følges (Avolio et al., 2003; Da Veiga & Eloff, 2010). Problemet i avdeling 1 ser ikke ut til å ha noe med de ansattes tillit til sin leder å gjøre da samtlige forklarte at de går til sin leder for å få hjelp og støtte ved behov. Imidlertid ser vi at lederen ikke skaper et støttende miljø og kultur hvor informasjonssikkerhet er en naturlig del av avdelingens diskusjoner. Det er også en gjensidig forventning hos leder og ansatte at de pålagte instruksene og rutinene skal følges, noe som også kan sette en stopper for en slik utvikling.

Ansatte i denne avdelingen lærer også om informasjonssikkerhet fra de korte e-læringskursene. I avdeling 2 diskuterer lederen informasjonssikkerhet med de ansatte om nye situasjoner og rutiner. Denne lederen ser hvilke behov som gjør seg gjeldende blant de ansatte

og identifiserer om en ansatt trenger lederen en til en, eller om det det kan tas med hele avdelingen. Lederen hjelper hver enkelt og tar hensyn til individuelle behov og ferdigheter. Ansatte var fornøyde med at lederen forklarte dem nyttige tips i forbindelse med teknologi og informasjonssikkerhet og på denne måten fungerer lederen som en mentor for de ansatte. Leder har derfor en støttende adferd til sine ansatte og ikke har noe problem med å ta opp regler eller policyer i møter med de ansatte (Avolio et al., 2003; Bass, 1990). Vi ser at forskjellen mellom lederstilene i stor grad har en innvirkning på de ansatte, hvor bevisste de er og hvilken kunnskap de har rundt informasjonssikkerhet. Avdeling 2 har mer kunnskap og bevissthet rundt informasjonssikkerhet, og dette kommer særlig til syne ved begrepsavklaringen hvor ansatte i avdeling 2 reflekterte best rundt informasjonssikkerhet og informasjonssikkerhetskultur. På denne måten ser vi at leder gjennom individualisert innflytelse kan spille en positiv rolle ved bevisstgjøring og kunnskapen til ansatte, og på denne måten ha en positiv innvirkning på informasjonssikkerhetskulturen. Imidlertid er viktig å påpeke at det å skape bevissthet rundt informasjonssikkerhet ikke nødvendigvis vil føre til atferdsendringer (Jäger, 2018). Det betyr at selv om leder i avdeling 2 skaper bevissthet om informasjonssikkerhet, betyr ikke dette at ansattes atferd samsvarer med deres kunnskap.

Ledelse ved unntak spiller en rolle for artefakter

Leder i avdeling 1 hadde flere trekk som er karakteristisk for lederstilen ledelse ved unntak (passiv). Denne lederen griper inn i situasjoner når det har skjedd sikkerhetsbrudd eller rutinebrudd (Bass, 1990, (Antonakis et al., 2003). De ansatte har et eget ansvar for å følge rutinene, sikkerhetsregler og de standardene som er satt (Guhr & Breitner, 2018). Ansatte har i større grad muligheter til å prøve og feile, men lederen vil gripe inn dersom det skjer et regelbrudd (Guhr & Breitner, 2018). Det er slik at lederen forventer at de ansatte følger alle rutinene, sikkerhetsregler og de standardene som er satt i bankvirksomheten.

I kapittel 5.2.2 kom vi frem til at leder i avdeling 1 har ikke har karakteristikkene til ledelse ved unntak (aktiv). Leder i avdeling 2 følger opp ansatte gjennom tilbakemeldinger, og griper inn om det oppstår brudd på regler, instrukser, prosedyrer eller rutiner som er virksomhetens artefakter (Antonakis et al., 2003; Avolio et al.,1999; Guhr & Breitner, 2018). Dette er i stor grad karakteristikker som kjennetegner ledelse ved unntak (aktiv). Reglementet som IKT-forskriften og personopplysningsloven er banken pliktig til å følge, og ligger i bankens interne rutiner. Det vil være slik at en leder med karakteristikkene til ledelse ved unntak (aktiv) kan

komme med tilbakemeldinger dersom ansatte eksempelvis har papirer med sensitive opplysninger åpent på pulten. Denne lederstilen fremstår derfor som viktig for overholdelse av regler og rutiner, og vil fremme en sikkerhetsatferd (Avolio et al., 2003; Humaidi & Balakrishnan, 2015). Ved å fremme en informasjonssikkerhetsatferd vil virksomhetens artefakter styrkes og på denne måten ha en positiv innvirkning på informasjonssikkerhetskulturen (Da Veiga & Eloff 2010; Niekerk & Solms, 2010; Schein, 1987).

Anerkjente verdier og normer og delte underliggende antakelser setter en stopper for inspirerende motivasjon

Det finnes ikke konkrete målsetninger for informasjonssikkerhet på mellomledernivå i banken. De ansatte forholder seg til rutinene og opplæringen som kommer, og det faller leder i avdeling 1 naturlig å ikke blande seg inn i rutinene og prosessedyrene, med mindre det skjer brudd (Antonakis et al., 2003). Det virker derfor som at det ikke er meningen at det skal være fokus på informasjonssikkerhet på mellomledernivå. Vårt inntrykk er at mellomledere får beskjeder fra toppledelsen i banken, og følger opp det som er nødvendig i forhold til rutiner og kurs. Toppledelsen i banken gir beskjed om hvordan ting skal gjørs og når det skal gjøres endringer. IT avdelingen sørger for at dette gjøres på riktig måte i henhold til gjeldende systemer og sikkerhet. Problem med dette er at mellomledere og ansatte ikke har noe konkret sikkerhetsmål å arbeide mot. Det gjør det vanskelig å vite eksakt hva en skal forholde seg til utenfor det som er innbakt i rutinene. Dette betyr at mellomleder ikke får mulighet til å påvirke og motivere for arbeidet for informasjonssikkerhet. Vi antar at om banken hadde hatt konkrete målsetninger for informasjonssikkerheten på avdelingsnivå ville det ha vært enklere for ledere å motivere de ansatte til blant annet å rapportere uønskede hendelser og avvik.

Inspirerende motivasjon handler om at lederen motiverer ansatte ved å skape en mening bak arbeidet og kommer med utfordringer som skaper entusiasme og optimisme. Dette sørger for en individuell drivkraft og en lagånd i forbindelse med arbeidsoppgaver (Avolio et al., 2003; Bass 1985). Flores & Ekstedt (2016 ) legger frem at det er viktig å legge frem en sikkerhets visjon slik at alle ansatte forstår målene for informasjonssikkerhetsinnsatsen i virksomheten. På denne måten vil et mål gjøre det enklere for leder og ansatte å forstå hensikten med det som gjøres, og gjør det mer tilfredsstillende. Det er vanskelig for leder å uttrykke viktige formål og arbeidsoppgaver på en enkel måte slik at de ansatte kan strekke seg mot målene og visjoner for banken, når disse ikke eksisterer (Bass, 1990; Flores & Ekstedt 2016; Hetland,

2004). Dette hindrer fremveksten av anerkjente verdier og normer som omhandler de verdiene som banken vil leve opp til. I dag handler de anerkjente verdiene og normene om viktigheten av å etterleve rutiner og instrukser, fremfor at dette kunne vært basert på målsettinger som kunne skapt mer motivasjonsgrunnlag for ledere. Etterlevelsen av rutiner vil uansett oppnås gjennom artefaktene, hvor informasjonssikkerhetsatferd oppnås gjennom de ulike informasjonssikkerhetskomponentene som er implementert i banken (Da Veiga & Eloff, 2010; Niekerk & Solms, 2010).

## *5.4. Konklusjon*

Formålet med denne masteroppgaven har vært å besvare problemstillingen:

*"Hvilken rolle spiller lederstil for informasjonssikkerhetskulturen i bank?"*

Informasjonssikkerhetskulturen fremstår som god i begge avdelingene. Vi ser at avdeling 2 hvor lederen har flere karakteristikker fra transformasjonsledelse i større grad er bevisste på informasjonssikkerhet. Det kan indikere at transformasjonsledelse er en lederstil som er positiv for informasjonssikkerhetskulturen (Bass, 1990; Niekerk & Solms, 2010; Safa & Solms, 2016). Transaksjonsledelse fremstår likevel som en lederstil som er viktig for overholdelse av regler og rutiner som vil fremme en sikkerhetsatferd (Avolio et al., 2003; Humaidi & Balakrishnan, 2015).

Det er mer effektivt med en kultur som fremmer hensiktsmessig informasjonssikkerhetsatferd gjennom kunnskap, artefakter, verdier og antagelser enn å pålegge organisasjonsmedlemmene en viss type atferd gjennom regler (Thomson et al., 2006). Dette betyr at beskyttelse av informasjon må være en naturlig del av de ansattes og lederes atferd og deres daglige aktiviteter. Dette kan best gjøres ved at leder inspirerer og støtter sine ansatte (Avolio et al, 2003; Avolio & Bass, 1994; Bass, 1990; Da Veiga & Eloff, 2010). På denne måten anses transformasjonsledelse som en lederstil som kan ha en positiv innflytelse på informasjonssikkerhetskulturen (Da Veiga & Eloff, 2010; Niekerk & Solms, 2010; Thomson et al., 2006). Vi mener på bakgrunn av dette at sentrale trekk ved transformasjonsledelse er mer fordelaktig for en mer helhetlig tilnærming til arbeid for informasjonssikkerhetskultur i avdelingene. Det er ønskelig at ansatte er selvgående og proaktive, slik at de ikke bare følger regler og prosedyrer. De må også være aktive bidragsytere i sikkerhetsarbeidet på daglig basis (Guhr & Breitner, 2018).

## *5.5. Implikasjoner for teori og praksis*

Denne studien har et teoretisk bidra fordi koblingen mellom lederstil og informasjonssikkerhetskultur er lite studert tidligere. Studiet er utført i samarbeid med en norsk bank, hvor lederstil kan spille en viktig rolle for informasjonssikkerheten og informasjonssikkerhetskulturen. Det er slik at lederens arbeidsoppgaver er å få ansatte til å følge informasjonssikkerhetsreglementet.

Kunnskap om transaksjons- og transformasjonsledelse gjør at ledelsen kan bidra aktivt til medarbeidernes sikkerhetsarbeid. Dette gjøres ved å både ved å understreke viktigheten av å følge virksomhetens eksisterende regler og rutiner, men også ved å inspirere og støtte til overholdelse. Det er derfor viktig å overbevise ledelsen i banker om fordelene ved å fokusere på informasjonssikkerhetskultur. De konkrete ledelsesmessige implikasjonene om at transformasjons- og transaksjonsledelse i større grad kan påvirke ansatte til å fokusere på informasjonssikkerhet kan være interessant å ta med seg videre.

# 6. Kritikk av studien og studiens begrensninger

Vi har valgt embedded single case som forskningsdesign. I ettertid ser vi at det kunne også vært relevant å gjennomføre en komparativ casestudie som også kalles for multippel casestudie, hvor man sammenligner to eller flere caser. Det kan eksempelvis være tilfeller, enheter, og veldig ofte er det virksomheter. En multippel casestudie er ofte foretrukket fremfor enkeltcase fordi det åpner opp for større presisjon, sterkere argument, gir sammenligningsgrunnlag, og får frem ulikheter, mangfold og nyanseforskjeller (Yin, 2018). I vår avhandling kunne det vært interessant å sammenligne to avdelinger i en bank, med to avdelinger i en annen bank for å se etter forskjeller og likheter mellom disse. Ved å benytte en multippel casestudie vil det gi en forsikring om at funnene ikke bare gjelder ett case, men kan øke overførbarheten til andre kontekster (Yin, 2018). Vår studie ble imidlertid begrenset til en bank, hvor formålet vårt er å beskrive, forstå og forklare i dybden hvilken rolle lederstil kan spille for informasjonssikkerhetskulturen. Valget falt derfor på enkeltcase-design med flere analyseenheter.

En begrensning med avhandlingen er som nevnt innledningsvis at vi ikke har hatt mulighet til å gjennomføre observasjon. Observasjon er en hensiktsmessig metode for å kartlegge kultur i en virksomhet (Schein & Schein, 2017). Ved å benytte både observasjon og intervju som datainnsamlingsmetoder ville vi hatt mulighet til å kartlegge informasjonssikkerhetskulturen på en bedre måte. På grunn av begrenset tid til å gjennomføre studiet og Covid-19 situasjonen, var observasjon imidlertid vanskelig å gjennomføre.

En annen begrensning er tidsaspektet. Tiden vi har hatt til rådighet har gjort studiet krevende siden begge har lite erfaring med kvalitativ forskning. Det kan derfor tenkes at vi har oversett noe på grunn av tidsbegrensningen.

Vi tror også at vi kunne formulert og arbeidet mer med intervjuguiden, slik at spørsmålene kunne blitt enda bedre. Det kan ha vært svakhet ved spørsmålene som har gjort det vanskelig å måle intellektuell stimuli og inspirerende motivasjon på en god måte. En annen svakhet ved avhandlingen er hvorvidt våre tolkninger av informantenes meninger er korrekte og speiler virkeligheten.

# *7. Forslag til videre forskning*

Vi har som nevnt tidligere formulert at det er lite forskning på lederstil og informasjonssikkerhetskultur og mer forskning på dette område ville kunne bidra til at virksomheter kan arbeide mot en bedre informasjonssikkerhetskultur. Det å bruke både kvalitativ og kvantitativ forskningsmetode vil kunne kartlegge hvilke lederstil virksomheter benytter seg av i dag og se hvilke lederstiler som er best egnet for å skape en god informasjonssikkerhetskultur i fremtiden. Det å undersøke flere virksomheter i forskjellige sektorer vil derfor kunne bidra positivt til mer kunnskap på området.

Et inntrykk vi har fått i denne studien er at atferden til ansatte og ledere på avdelingsnivå kan ha noe å si for bankens totale informasjonssikkerhetskultur. Det kan derfor være interessant identifisere og måle den faktiske sikkerhetsatferden man ønsker å styrke, og ikke bare ansatte og lederes atferdsintensjoner.

Et forslag og ønske selv fra banken var å gjennomføre en longitudinell studie. Bankens ønske var å sammenligne to avdelinger før og etter ansatte og ledere hadde fått mer opplæring og kurs om informasjonssikkerhet.

# 8. Referanser

## Forskrift og Lover


Finansforetaksloven. (2015). Lov om finansforetak og finanskonsern (LOV-2015-04-10-17). Hentet fra https://lovdata.no/dokument/LTI/lov/2015-04-10-17/*

Forskrift om bruk av IKT-systemer. (2003). Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) (FOR-2003-05-21-630). Hentet fra https://lovdata.no/dokument/LTI/forskrift/2003-05-21-630

Personopplysningsloven. (2018) Lov om behandling av personopplysninger (LOV-2018-06-15-38). Hentet fra https://lovdata.no/dokument/LTI/lov/2018-06-15-38


## Bøker


Avolio, B. & Bass, B. M. (2004). *Mulitfactor Leadership Questionnaire* (utg 3). California: Mind Garden, Inc.

Avolio,B.J. & Bass, B.M.(1994). *Improving organizational effectiveness through Transformational leadership.* London: Sage Publications.

Bass, B. M. (1985). *Leadership and performance beyond expectation*. New York: Free Press.

Bass, B.M., & Stogdill,R.M. (1990).*Bass and Stogdill's Handbook of leadership. Theory, research, and managerial applications* (3.utg.). New York: Free Press.

Burns, J. M. (1978). *Leadership.* New York: Harper & Row.

Creswell, J.W. & Poth, C. N. (2018). *Qualitative inquiry & research design: choosing among five approaches* (4 utgave). Los Angeles: SAGE Publications.

Deal, T. & Kennedy, A. (1982). *Corporate cultures: the rites and rituals of organizational life*. Boston: Addison-Wesley.

Grønmo, S. (2004). *Samfunnsvitenskapelige metoder.* Fagbokforlaget, Bergen, Norge. Hall.

Jacobsen, D. I. (2000). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode.* Kristiansand: Høyskoleforlaget AS - Norwegian Academic Press.

Jacobsen, D.I. og Thorsvik, J. (2013). *Hvordan organisasjoner fungerer.* (4. utg). Bergen: Fagbokforlaget.

Johannessen, A., Christoffersen, L. og Tufte, P.A.(2011). *Forskningsmetode for økonomisk-akademisk-administrative fag* (3 utg.). Oslo: Abstrakt forlag AS.

Kvale, S., Brinkmann, S., Anderssen, T. M., & Rygge, J. f. (2009). *Det kvalitative forskningsintervju*. Gyldendal akademisk, Oslo, Norge.

Miles, M.B, Hubermann, A.M. & Saldana, J. (2014). *Qualitative Data analysis*. SAGE Publications.

Mjølsnes, S. F. (2012). *A multidisciplinary introduction to information security.* Florida; CRC Press.

Myers, M.D. & Avison, D.E. (2002). *An Introduction to Qualitative Research in Information Systems In: Qualitative Research in Information Systems*. London: SAGE Publications. Doi: 10.4135/9781849209687.

Myers, M.D. & Avison, D.E. (2002). A*n Introduction to Qualitative Research in Information Systems In: Qualitative Research in Information Systems.* SAGE Publications: London. Doi: 10.4135/9781849209687.

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

Robbins S. (2001). Organizational behaviour. 9th ed. New Jersey: Prentice

Savin-Baden, M. & Major, C.H. (2013). *Qualitative research : the essential guide to theory and practice.* London: Routledge.

Schein E. H. (1999). *The corporate culture survival guide: sense and nonsense about culture change.* San Fransisco: Jossey-BassInc.

Schein, E. H. (1987). *Organisasjonskultur og ledelse: Er kulturendring mulig?* Oslo: Mercuri Media Forlag.

Schein, E. H. (2010). *Organizational Culture and leadership* (4.utg.). San Francisco: A wiley Imprint.

Schein, E.H & Schein, P.A. (2017). *Organizational culture and leadership (5.utg.). New* Jersey: John Wiley & Sons, Incorporated.

Thagaard, T. (2013). *Systematisk og innlevelse en innføring i kvalitativ metode* (4 utg). Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Yin, R.K. (2018). *Case study reserach and applications* (6 utg). London: SAGE publications. Ltd.

### *Artikler*


AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior,* 49, 567-575. https://doi.org/10.1016/j.chb.2015.03.054.

Antonakis, J., Avolio, B.J. & Sivasumbramaniam, N. (2003). Context and leadership: an examination of the nine-factor full-range leadership theory using the Multifactor Leadership Questionnaire. *The Leadership Quarterly*, 14, 261–295.https://doi.org/10.1016/S1048-9843(03)00030-4.

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

Avolio, B.J., Bass, B.M., Berson, Y. & Jung, D.I. (2003). Predicting unit performance by assessing transformational and transactional leadership. *Journal of Applied Psychology,* 88 (2), 207-218. https://doi.org/10.1037/0021-9010.88.2.207.

Avolio, B.J., Bass, B.M. & Jung, D.I. (1999). Re-examining the components of transformational and transactional leadership using the Multifactor Leadership Questionnaire. *Journal of Occupational and Organizational Psychology,* 72, 441-462. Hentet fra https://ezproxy2.usn.no:3759/docview/57862169?rfr_id=info%3Axri%2Fsid%3Aprimo.

Bang, H. (2013). Organisasjonskultur: En Begrepsavklaring. *Tidsskrift for Norsk Psykologforening.* 50(4), 326-336. Hentet fra http://www.psykologtidsskriftet.no/pdf/2013/326-336.pdf

Bass, B.M. (1990). From transactional to transformational leadership: Learning to share the vision. *Organizational Dynamics,* 18(3), 19-31. https://doi.org/10.1016/0090-2616(90)90061-S.

Bongiovanni, I. (2019) The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security,* 86, 350–357. Doi: 10.1016/j.cose.2019.07.003.

Bycio, P., Hackett, R. D., & Allen, J. S. (1995). Further assessments of Bass's (1985) conceptualization of transactional and transformational leadership. *Journal of Applied Psychology*, 80(4), 468-478. https://doi.org/10.1037/0021-9010.80.4.468.

Choi, M. (2016). Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing. *Sustainability,* 8 (7), 638. https://doi.org/10.3390/su8070638.

Crossler, R. E., Johnston, A. C., Lowry, P.B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security,* 32, 90-101. Doi: 10.1016/j.cose.2012.09.010.

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.

Davenport, H.T., De Long, W.D. & Beers, C.M. (1998). Successful knowledge management projects. *Sloan Management Review,* 39 (2), 43-57. Hentet fra https://www.researchgate.net/profile/Thomas_Davenport2/publication/200045855_Building_Successful_Knowledge_Management_Projects/links/53db93a40cf216e4210bf847.pdf.

Du Bois, J. (1991). Transcription design principles for spoken discourse research. *Pragmatics,* 1, 71-106. DOI: 10.1075/prag.1.1.04boi.

Dubois, A. & Gadde, L.E. (2002).Systematic combining: an abductive approach to case research. *Journal of business*, 55(7), 553-560. Doi.org/10.1016/S0148-2963(00)00195-8

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review,*14(4), 532-550. DOI: 10.2307/258557

Eriksen, F. J. (2018). Mørketallsundersøkelsen 2018: informasjonssikkerhet, personvern og datakriminalitet*. Gjennomført av Opinion AS for Næringslivets Sikkerhetsråd.* (Rapport 2016-2018). Hentet fra https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/Mørketallsundersøkelsen/Mørketallsundersøkelsen%202018%20low.pdf.

Flores, W.R. & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security,* 59, 26-44. DOI: 10.1016/j.cose.2016.01.004.

Guhr, N., Lebek, B. & Breitner, M.H.(2018). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information system journal*, 29 (2), 340- 362. https://doi.org/10.1111/isj.12202.

Guldenmund, F.W. (2000). The nature of safety culture: a review of theory and research. *Safety Science,* 34, 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. *Risk Analysis ,*30 (10), 1466-1480. https://doi.org/10.1111/j.1539-6924.2010.01452.x.

Hao, H. & Padman, R.(2016). An empirical study of opinion leader effects on mobile technology implementation by physicians in an American community health system. *Journal indexing & metrics*, 24 (3), 323-333.https://doi.org/10.1177/1460458216675499.

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, 29(24), 249–257.

Hetland, H. (2004). Transformajonsledelse i en norsk kontekst. *Magma Econas tidsskrift for økonomi og ledelse,*1/2004,1. Hentet fra https://www.magma.no/transformasjonsledelse-i-en-norsk-kontekst.

Hu, Q., Dinev, T., Hart, P. & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision sciences journal ,*40(4), 615-659. Doi: 10.1111/j.1540-5915.2012.00361.x.

Humaidi, N. & Balakrishnan, V. (2015). Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness. *International Journal of Information and Education Technology*, 5 (4), 311- 318. DOI: 10.7763/IJIET. 2015.V5.522

Hwang, I., Wakefield,R., Kim, S. & Kim, T. (2019). Security awareness: The first step in information security compliance behaviour. *Journal of computer information system*. https://doi.org/10.1080/08874417.2019.1650676

Jäger, L. (2018). Information security awareness: Literature review and integrative framework. *Proceedings of the 51st Hawaii International Conference on System Sciences,* 4703- 4712. Doi: 10.24251/HICSS.2018.593.

Kankanhalli, A. Teo, H-H., Tan, B.C.Y. & Wei, K-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23, 139–154. Doi:10.1016/S0268-4012(02)00105-6.

Leidner, D.E. & Kayworth, T. (2006). Review: a review of culture in information systems research: toward a theory of information technology culture conflict. *MIS Quarterly,* 30 (2), 357-399. Hentet fra https://dl.acm.org/doi/10.5555/2017307.2017316

Moon, Y.J., Choi, M. & Armstrong, D. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. *International Journal of Information Management,* 40, 54-66. DOI: 10.1016/j.ijinfomgt.2018.01.001.

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

Orlikowski, W. J. & Scott, S.V. (2008). Sociomateriality: Challenging the separation of Technology, work and organization. *Academy of Management Annals,* 2 (1), 433-474. Doi: 10.1080/19416520802211644.

Reason, J. (1998). Achieving a safe culture: theory and practice. *Work & Stress,* 12(3), 293-306. Doi:10.1080/02678379808256868.

Safa, N.S. & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior,* 57, 442-451. Doi:10.1016/j.chb.2015.12.037.

Schlienger, T. & Teufel, S. (2003). Analyzing security culture: increased trust by an appropriate information security culture. *Database and Expert Systems Applications, Proceedings. 14th International Workshop,* 1, 1-6. DOI: 10.1109/DEXA.2003.1232055.

Soomro, Z.A., Shah, M.H. & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36, 215–225. Doi: 10.1016/j.ijinfomgt.2015.11.009.

Stogdill, R. M. (1950). Leadership, membership and organization. *Psychological bullet,* 47 (1), 1-14.https://doi.org/10.1037/h0053857.

Straub, D.W. & Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22 (4), 441-469. DOI: 10.2307/249551

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

Thite, M. (2000). Leadership styles in information technology projects. *International Journal of Project Management,* 18(4), 235-24. Doi: 10.1016/S0263-7863(99)00021-6.

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

Weich, K. E. (1989). Theory Construction as Disiplined Imagination. *The Academy of Management Review,* 14(4), 516-531. DOI: 10.2307/258556

### *Nettsider*

Datatilsynet. (2018, 23 august). Iverksette styringssystem for informasjonssikkerhet. Hentet fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

Datatilsynet. (2018, 30 oktober). Etablere internkontroll. Hentet fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

Datatilsynet. (2019, 17 juli). Hva er personopplysning? Hentet fra https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/

Experis. (2019). Experis Security Workforce Study; Alvorlig mangel på komeptanse innen IT-sikkerhet. Hentet 14. April 2020 fra https://www.experis.no/kunder/om-experis2/nyheter/pressreleases/experis-security-workforce-study-alvorlig-mangel-paa-kompetanse-innen-it-sikkerhet-1391046

Knapskog, S.J. & Eilertsen, Ø. (2019, 30. november). Kryptografi. Hentet fra https://snl.no/kryptografi

Nasjonal sikkerhetsmyndighet. (2014, 12. mai). Sikkerhetskultur. Hentet 20. Mars 2020 fra https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/

NorSIS. (2020, 18.mars). Økt cyberfare med koronaviruset: Slik får du et trygt hjemmekontor. Hentet 25. Mai 2020 fra https://norsis.no/okt-cyberfare-med-koronaviruset-slik-far-du-et-trygt-hjemmekontor/

# *Vedlegg*

## *Vedlegg 1: Informert samtykke*

**Vil du delta i forskningsprosjektet**

«*Hvilken rolle spiller lederstil for informasjonssikkerhetskultur?*»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke hvilken rolle lederstil har for informasjonssikkerhetskulturen i deres virksomhet. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

**Formål**

Informasjonssikkerhet handler ikke bare om programvarer, brannmurer og lignende, det har også en menneskelig side. Det er menneskene i organisasjonen som forholder seg til systemene, og det er dette vi ønsker å se nærmere på. Med denne forskningen kan vi bringe innsikt i hvordan menneskelige faktorer kan påvirke hvordan informasjonssikkerheten er i virksomheten. Dette er en masterstudie.

**Hvem er ansvarlig for forskningsprosjektet?**

Universitetet i Sørøst-Norge er ansvarlig institusjon for dette prosjektet.

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

Utvalget er trukket på bakgrunn av avdelinger i virksomheten hvor vi skal intervjue totalt 16 personer.

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

Dersom du velger å delta innebærer det at vi intervjuer deg i ca. 1 time. Intervjuet inneholder spørsmål om lederstil og informasjonssikkerhetskultur. Dine svar fra intervjuet vil bli registrert med lydopptak og notater.

**Det er frivillig å delta**

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil da bli anonymisert.

Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

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

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

- Det er kun oss og vår veileder Glenn Kristiansen som vil ha tilgang ved behandlingsansvarlig institusjon.
- Kontaktopplysningene dine vil vi erstatte med en kode som lagres på egen navneliste adskilt fra øvrige data, lagre datamaterialet på forskningsserver ved behandlingsansvarlig institusjon.

Du som deltaker vil ikke kunne gjenkjennes i publikasjon, da det er kun oppfatninger tilknyttet informasjonssikkerhet som vil publiseres.

**Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?**

Prosjektet skal etter planen avsluttes 15.05.20. Datamaterialet anonymiseres og lydopptakene blir slettet ved prosjektslutt.

**Dine rettigheter**

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

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

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

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Sørøst-Norge har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

**Hvor kan jeg finne ut mer?**

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

- Universitetet i Sørøst-Norge eller Glenn Kristiansen, Spesialiseringsansvarlig for bedriftsøkonomisk analyse.
  Vårt personvernombud: Paal Are Solberg, på epost (personvernombud@usn.no)
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no)
  eller telefon: +47 55 58 21 17

Med vennlig hilsen

| Prosjektansvarlig | Studenter |
|---|---|
| (Glenn Kristiansen) | Tonje Langelid og Viktoria Røtterud |

---

**Samtykkeerklæring**

Jeg har mottatt og forstått informasjon om prosjektet «Hvilken rolle spiller lederstil for informasjonssikkerhetskultur?», og har fått anledning til å stille spørsmål. Jeg samtykker til:

☐ å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. 15.05.20

---

(Signert av prosjektdeltaker, dato)

### *Vedlegg 2: Intervjuguide ansatte*

Vi skriver jo som nevnt en masteroppgave nå innen fagfeltet strategi og kompetanseledelse. Temaet for oppgaven vår er knyttet til lederstil og informasjonssikkerhetskultur, og vårt ønske gjennom denne samtalen er at du skal kunne bidra til at vi får svar på vår problemstilling. All informasjon du kommer med vil bli behandlet anonymt, og det vil ikke komme frem på noen som helst måte hvem du er eller hvor du jobber da alt dette vil bli sensurert.

Vi ønsker å benytte oss av båndopptaker under hele intervjuet, da dette vil kunne sikre viktig informasjon og unngå misforståelser. Dette vil resultere i en mer korrekt og troverdig oppgave. Det vil også gjøre at selve intervjuet vil kunne foretas raskere, da vi ikke behøver å notere oss det som blir sagt underveis. Ingen andre vil ha tilgang til båndopptakere, og alle svarene blir anonymisert og analysert. Vi lurte derfor på om det greit at vi tar opp samtalen? Vi vil selvfølgelig slette opptakene når alt er transkribert i løpet av to uker.

**Generelt**

1. Hva er din stilling og hva innebærer det?
2. Hvor lenge har du arbeidet i denne bedriften?
3. Trives du på denne arbeidsplassen?

**Informasjonssikkerhetskultur**

4. Hvordan forstår du begrepet informasjonssikkerhet?
5. Er du kjent med begrepet informasjonssikkerhetskultur? Hvordan vil du forklare begrepet?
    - For at vi skal ha samme forståelse av begrepet forteller vi deg hvordan vi har valgt å definere informasjonssikkerhetskultur som *"holdningene, antagelsene, troen, verdiene og kunnskapen som ansatte bruker for å samhandle med organisasjonens systemer og prosedyrer. Samspillet resulterer i akseptabel eller uakseptabel atferd (dvs. hendelser) som er tydelig i det som er skapt, og blir en del av måten ting gjøres i organisasjonen for å beskytte informasjonsmidlene. Denne informasjonssikkerhetskulturen endres over tid".*
6. Hvordan synes du informasjonssikkerhetskulturen er hos dere?

7. Hvilke verdier jobber dere ut ifra i banken, og på hvilken måte kan du koble disse verdiene til sikkerhetsarbeidet?
8. Kjenner du til en sikkerhets-policy eller om dere har noen sikkerhetsmål? Finnes det sikkerhetsmål i din avdeling? Hva går disse ut på?
9. Vet du om det finnes regler eller instrukser for informasjonssikkerhet? Hva vet du om disse?
10. Følger du regler eller instrukser i banken? Hvordan?
11. Hvordan synes du reglene og instruksene er å forstå? Hvordan er de å forholde seg til?
12. Er du med å utvikle eller komme med innspill til informasjonssikkerhetsregler?
13. Har du selv opplevd tilfeller av trusler eller sårbare situasjoner relatert til informasjonssikkerhet?
    - Kan du beskrive dette?
    - Har du observert tilfeller av trusler relatert til informasjonssikkerhet i banken som gjelder andre ledere eller ansatte?
14. Føler du at du har nok kunnskap til å vurdere hva som er trygt eller utrygt å gjøre på nett?
    - Har du opplevd usikkerhet i enkelte situasjoner? Hvorfor?
    - Hvilke situasjoner opplevde du usikkerhet?
15. Er du bekymret for at følgende skal hende deg:
    - At du for eksempel får en e-post som tilsynelatende er fra din sjef, men viser seg å være en phishing-email hvor du blir utsatt for et hackerangrep hvor bedriften og din leder blir tvunget til å betale løsepenger for å få tilbake kontrollen på systemet.
    - Hvor bekymret er du for at kundenes personopplysninger skal lekke?
    - Hvor stor risiko forbinder du med at følgende hendelser kan skje?
    - Er det andre hendelser du er bekymret for at skal hende deg?
16. Hva er det sannsynlig at du vil gjøre dersom følgende skjer deg:
    - Blir utsatt for svindel eller blir hacket på e-post eller lignende?
17. Vet du hvordan du skal melde avvik om uønskede hendelser eller sikkerhetsbrudd?
    - Rapporterer du avvik eller sikkerhetsbrudd?
18. Undersøker du om en nettside, link eller epost er trygg før du bruker eller åpner den?
    - Har dere et system som sorterer utrygge eposter før dere mottar dem?
19. Hva er ditt forhold til bruk av passord?
    - Bruker du samme passord over alt?

- Har du passordverktøy for å hjelpe deg å håndtere ulike passord?
- Bruker du forskjellige passord for de ulike tjenestene?
- Bruker du tid på å lage sikre passord?

20. Hva veit du om sikkerhetskopiering på din pc?
    - Skjer det automatisk eller må du gjøre det manuelt?
    - Hvor ofte sikkerhetskopierer du data som er viktige for deg?
21. Har dere rutiner for å oppdatere programvare på din arbeidsdatamaskin?
    - Hvordan er disse rutinene? Hvordan gjennomføres dette?
    - Skjer det automatisk?
22. Er du interessert i å lære om teknologi og IT?
23. Hvem lærer deg å behandle informasjon på en sikker måte?
    - Er det deg selv, leder, IT-avdelingen eller andre?
24. Har du fått opplæring i informasjonssikkerhet i løpet av det siste året?
    - Hva slags opplæring har du fått, og i hvilken forbindelse?
25. Synes du du har fått bedre kunnskap og ferdigheter etter opplæringen om informasjonssikkerhet? På hvilken måte?
26. Kunne du tenke deg mer opplæring om informasjonssikkerhet?
    - Hva slags opplæring kunne du tenke deg?
27. Tar dere lærdom av feil og uhell for å forhindre at skader inntreffer på nytt? På hvilken måte?

**Lederstil og leders rolle**

28. Opplever du at din leder tar informasjonssikkerhet på alvor? På hvilken måte?
29. Følges regler og rutiner opp av din leder? Hvordan?
30. Hvordan ville din leder håndtert et mulig sikkerhetsproblem?
31. Hvordan synes du din leder jobber med å skape bevissthet omkring risiko forbundet med informasjonssikkerhet?
32. Opplever du at din leder jobber for å involvere deg i sikkerhetsarbeid? På hvilken måte?
33. Dersom du ikke forstår et sikkerhetsmål, vil da din leder forklare deg det på en god måte?
    - Om ikke leder gjør det, hvordan går du frem for å forstå sikkerhetsmålene?
34. Synes du det er viktig at leder motivere deg til å fokusere på informasjonssikkerhet?

- Hvorfor synes du dette?

35. Er din leder engasjert for at du skal gjennomføre kurs og opplæring om informasjonssikkerhet?
    - Hvor ofte får du påminnelse om å gjennomføre?
36. Hvordan arbeider din leder for å opprettholde din kompetanse og forståelse i forhold til sikkerhetstiltak og prosedyrer?
37. Hvordan utfordrer din leder deg med tanke på tilegning av ny kunnskap om informasjonssikkerhet?
38. Opplever du at din leder veileder deg til å ta informasjonssikkerhet på alvor? På hvilken måte?
39. Hvordan er tilliten mellom deg og din leder om det skulle dukke opp ett informasjonssikkerhets problem?
    - Ville du gått til din leder med problemet?
    - Får du tilbakemelding av din leder om problemet blir løst?
    - Blir du oppfordret av leder til å innrapportere uønskede hendelser, avvik eller skader?

**Avsluttende**

40. Hva mener du er nødvendig for å få en optimal informasjonssikkerhet i din bank?
41. Er det noe annet du vil legge til?

### *Vedlegg 3: Intervjueguide ledere*

Vi skriver jo som nevnt en masteroppgave nå innen fagfeltet strategi og kompetanseledelse. Temaet oppgaven vår er knyttet til er lederstil og informasjonssikkerhetskultur, og vårt ønske gjennom denne samtalen er at du skal kunne bidra til at vi får svar på vår problemstilling. All informasjons du kommer med vil bli behandlet anonymt, og det vil ikke komme frem på noen som helst måte hvem du er eller hvor du jobber da alt dette vil bli sensurert.

Vi ønsker å benytte oss av lydopptaker under hele intervjuet, da dette vil kunne sikre viktig informasjon og unngå misforståelser. Dette vil resultere i en mer korrekt og troverdig oppgave. Det vil også gjøre at selve intervjuet vil kunne foretas raskere, da vi ikke behøver å notere oss det som blir sagt underveis. Ingen andre vil ha tilgang til lydopptakene, og alle svarene blir anonymisert og analysert. Vi lurte derfor
på om det er greit at vi tar opp samtalen? Vi vil selvfølgelig slette opptakene når alt er transkribert i løpet av to uker.

**Generelt**

1. Hva er din stilling og hva innebærer det?
2. Hvor lenge har du arbeidet i denne bedriften?
3. Trives du?

**Informasjonssikkerhetskultur**

1. Hvordan forstår du begrepet informasjonssikkerhet?
2. Er du kjent med begrepet informasjonssikkerhetskultur? Hvordan vil du forklare begrepet?
    - For at vi skal ha samme forståelse av begrepet forteller vi deg hvordan vi har valgt å definere informasjonssikkerhetskultur som *"holdningene, antagelsene, troen, verdiene og kunnskapen som ansatte bruker for å samhandle med organisasjonens systemer og prosedyrer. Samspillet resulterer i akseptabel eller uakseptabel atferd (dvs. hendelser) som er tydelig i det som er skapt, og blir en del av måten ting gjøres i organisasjonen for å beskytte informasjonsmidlene. Denne informasjonssikkerhetskulturen endres over tid"*.
3. Hvordan synes du informasjonssikkerhetskulturen er hos dere?

4. Hvilke verdier jobber dere ut ifra i banken, og på hvilken måte kan du koble disse verdiene til sikkerhetsarbeidet?
5. Kjenner du til om dere har en sikkerhets-policy eller om dere har noen sikkerhetsmål? Hva går disse ut på?
6. Vet du om det finnes regler eller instrukser for informasjonssikkerhet? Hva vet du om disse?
7. Hvordan synes du reglene og instruksene er å forstå? Hvordan er de å forholde seg til?
8. Deltar du i utvikling av eller har mulighet til å komme med innspill for informasjonssikkerhetsregler?
9. Har du selv opplevd tilfeller av trusler eller sårbare situasjoner relatert til informasjonssikkerhet? Kan du beskrive dette?
    - Har du observert tilfeller av trusler relatert til informasjonssikkerhet i banken som gjelder andre ledere eller ansatte?
10. Rapporterer du om avvik og sikkerhetsbrudd? Hvordan er dette organisert?
11. Føler du at du har nok kunnskap til å vurdere hva som er trygt eller utrygt å gjøre på nett?
    - Har du opplevd usikkerhet i enkelte situasjoner? Hvorfor?
    - Hvilke situasjoner opplevde du usikkerhet?
12. Er du bekymret for at følgende skal hende deg?
    - At du for eksempel får en e-post som tilsynelatende er fra en kollega, men viser seg å være en phishing-email hvor du blir utsatt for et hackerangrep hvor bedriften din blir tvunget til å betale løsepenger for å få tilbake kontrollen på systemet.
    - Hvor bekymret er du for at kundenes personopplysninger skal lekke?
    - Hvor stor risiko forbinder du med at følgende hendelser kan skje?
    - Er det andre hendelser du er bekymret for at skal hende deg?
13. Hva er det sannsynlig at du vil gjøre dersom det følgende skjer deg?
    - Blir utsatt for svindel eller blir hacket på e-post eller lignende?
14. Undersøker du om en nettside, link eller epost er trygg før du bruker eller åpner den?
    - Har dere et system som sorterer utrygge eposter før dere mottar dem?
15. Hva er ditt forhold til bruk av passord?
    - Bruker du samme passord over alt?
    - Har du passordverktøy for å hjelpe deg å håndtere ulike passord?
    - Bruker du forskjellige passord for de ulike tjenestene?

- Bruker du tid på å lage sikre passord?

16. Hva vet du om sikkerhetskopiering på din pc?
    - Skjer det automatisk eller må du gjøre det manuelt?
    - Hvor ofte sikkerhetskopierer du data som er viktige for deg?
17. Har dere rutiner for å oppdatere programvare på din arbeidsdatamaskin?
    - Hvordan er disse rutinene? Hvordan gjennomføres dette?
    - Skjer det automatisk?
18. Er du interessert i å lære om teknologi og IT?
19. Hvem lærer deg å behandle informasjon på en sikker måte?
20. Har du fått opplæring i informasjonssikkerhet i løpet av de siste to årene?
    - Hva slags opplæring har du fått, og i hvilken forbindelse?
21. Synes du at du har fått bedre kunnskap og ferdigheter etter opplæringen om informasjonssikkerhet?
22. Kunne du tenke deg mer opplæring om informasjonssikkerhet?
    - Hva slags opplæring kunne du tenke deg?
23. Tar dere lærdom av feil og uhell for å forhindre at skader inntreffer på nytt? Hvordan?

**Lederstil og leders rolle**

24. Hva er dine viktigste lederoppgaver innenfor informasjonssikkerhet?
25. Følger du opp dine ansatte i forhold til regler og rutiner? Hvordan?
26. Hvilke mål har du om å ivareta informasjonssikkerheten i bedriften?
27. Hvordan kan du være en rollemodell for de ansatte i forhold til informasjonssikkerhet?
28. Hvor viktig synes du det er å motivere ansatte til å opprettholde en god informasjonssikkerhet? Hvorfor?
29. Hvordan engasjerer du de ansatte til å utføre kurs om informasjonssikkerhet?
30. Hvordan gir du tilbakemeldinger på sikkerhetsarbeidet til dine ansatte?
31. Hvordan arbeider du for å opprettholde ansattes kompetanse og forståelse i forhold til sikkerhetstiltak og prosedyrer?
32. Hvordan utfordrere du dine ansatte med tanke på tilegning av ny kunnskap om informasjonssikkerhet? (For eksempel ved kurs, organisering).
33. Hvordan forsøker du å veilede de ansatte til å ta informasjonssikkerhet på alvor?

34. Hvordan er tilliten mellom deg om de ansatte om det skulle dukke opp ett informasjonssikkerhets problem?
    - Ville den ansatte kommet til deg med problemet?
35. Hvordan veileder du de ansatte til å håndtere ett mulig sikkerhetsproblem?
    - Gir du tilbakemelding til dine ansatte om problemet blir løst?

**Avsluttende**

36. Hva mener du er nødvendig for å få en optimal informasjonssikkerhet i din bank?
37. Er det noe annet du vil legge til?

## *Vedlegg 4: Intervjueguide IT-avdelingen*

**Generelt**

1. Hva er din stilling og hva innebærer det?
2. Hvor lenge har du arbeidet der?
3. Hvordan trives du?

**Informasjonssikkerhet**

4. Hvordan vil du definere informasjonssikkerhet?
5. Hva legger du i begrepet informasjonssikkerhetskultur?

**Kulturbygging og elementer ved sikkerhetskultur**

6. Hvilke trusler anser dere som relevante for deres bank?
    - Hvordan imøtekommer din bank disse truslene?
7. Hvordan jobber dere med kulturbygging i forbindelse med sikkerhetsarbeidet?
    - Kan du gi noen eksempler (opplæringsprogram, atferdsendringskampanjer, kulturprogram og lignende)
8. Hvordan jobber dere med å skape bevissthet om sikkerhetsrisiko?
    - Hvordan kan ansatte og ledere bidra til å redusere denne risikoen?
    - Hvordan arbeider dere for å opprettholde ansattes og lederes kompetanse og forståelse i forhold til sikkerhetstiltak og prosedyrer?
9. Hvordan jobber dere med å involvere de ansatte og ledere i sikkerhetsarbeidet?
10. Hvilke regler er dere forpliktet å forholde dere til?
11. På hvilken måte arbeider dere for å skape ansvarsfølelse hos ledere og ansatte i forbindelse med sikkerhet?
12. Har dere formulert en security policy?
    - På hvilket nivå i virksomheten er denne formulert? (ledelsesnivå, toppledelsesnivå etc).
13. Har dere utarbeidet sikkerhetsmål og en strategi for dette?
14. Har dere et opplæringsprogram for alle ansatte i forhold til sikkerhet?
15. Hvordan oppfordres ansatte til å rapportere sikkerhetsrelaterte-hendelser/ eventuelt mistenksomheter?
16. Hvordan sørger dere for kontinuerlig læring for å forhindre uønskede hendelser?

17. Hvordan jobber dere for å informere ansatte og ledere om risikoen som er forbundet med informasjonssikkerhet?

**Avsluttende spørsmål:**

18. Hva forventer du at leder bør kunne om informasjonssikkerhet?
19. Hva forventer du at ansatte bør kunne om informasjonssikkerhet?
20. Hva mener du er nødvendig for å få en optimal informasjonssikkerhet i din bank?
21. Hva mener du ledere kan gjøre for informasjonssikkerhet på et generelt nivå?
    - Hva kan lederne gjøre bedre i dag?