Informasjonssikkerhet i banknæringen

Masteroppgave i Samfunnssikkerhet

Det teknisk-natur vitenskapelig fakultet

Universitetet i Stavanger

Julia M. Slettemoen

Stine Ertenstein

Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Samfunnssikkerhet	Vårsemesteret, 2018 Åpen
Forfatter: Julia M. Slettemoen & Stine Ertenstein	Julia M. Slettemoen Stine Ertenstein
Fagansvarlig: Ole Andreas H. Engen Veileder(e): Kristiane M. Lindland	
Tittel på masteroppgaven: Informasjonssikkerhet i banknæringen *En studie om hvordan banknæringen forstår og jobber for å sikre informasjon mot uønskede hendelser* Engelsk tittel: Information security in the banking sector *A study on how the banking sector understands and work to secure information against unwanted events*	
Studiepoeng: 30	
Emneord: Informasjonssikkerhet, risiko og sårbarhet, risikostyring, risikopersepsjon og organisatoriske faktorer	Sidetall: 77 + vedlegg/annet: 82 Stavanger, 14.06.2018

Sammendrag

I nyere tid har samfunnet vært gjennom et radikalt teknologisk skifte, noe som også har påvirket banknæringen. Tidligere har banknæringen hatt arbeidsoppgaver som har krevd direkte kontakt med kundene, og med dette vært utsatt for trusler i form av fysiske ran. I forbindelse med digitaliseringen er dagens kundebehandling endret ved at man i stor grad anvender applikasjoner, nettbank og andre systemer til å utføre betalinger. Dette medfører at bankene oppbevarer store mengder elektroniske opplysninger om kundene. På bakgrunn av dette har trusselbildet endret seg, ved at potensielle angrep kan utføres når som helst og hvor som helst av datakyndige personer. Med dette har banknæringen vært nødt til å endre sine arbeidsmetoder i takt med digitaliseringen, for å kunne ivareta informasjon mot uønskede hendelser. Hensikten med studiet er å belyse hvordan banknæringen forstår og jobber for å sikre informasjon mot uønskede hendelser, hvilket la grunnlaget for følgende problemstilling:

Hvordan forstår og jobber banknæringen for å møte risikoen for uønskede hendelser i forbindelse med informasjonssikkerhet?

For å svare på problemstillingen, er det valgt å gjennomføre en casestudie med abduktiv tilnærming. Det er gjennomført 13 dybdeintervjuer med bankansatte i fire ulike banker, hvor fire av dem er informasjonssikkerhetsledere, fire mellomledere og fem rådgivere. Funnene viser at bankene har et høyt fokus på sikring av informasjon. Likevel ser man at det er noen tiltak som bankene kan innføre for å øke sikkerheten enda mer. Det viser seg blant annet at inkludering og kommunikasjon ut til de ansatte kunne vært bedre, og det anbefales å benytte refleksjonsgrupper for å øke forståelsen og bevisstheten til de som jobber nedover i virksomhetene. I tillegg ser man at innføringen av nye lovkrav medfører at bankene må endre måten de jobber på, noe som kan medføre økt risiko og sårbarhet.

Abstract

In recent times, society has been through a radical technological shift, which has also affected the banking industry. The banking industry previously had tasks that required direct contact with customers, and as a result of this they have been exposed to robberies. In connection with digitization, today's customer management is changing, largely by using applications, online banking and other payment systems. This means that banks store large amounts of electronic information about the customers. Therefore, the threat has changed, because potential attacks against information systems can be carried out at anytime and anywhere. With this, the banking industry has been forced to change how they do their tasks at work because of the digitization, in order to be able to secure information against unwanted events. The purpose of this study has been to gain an understanding of how the banking industry understands and handles unwanted events aimed at their information systems, which laid the foundation for the following issue:

How does the banking industry understand and work to address the risk of unwanted events against the information security systems?

In order to answer the issue, it is chosen to conduct a case study with an abductive approach. 13 depth interviews has been conducted with bank employees in four different banks, four of which are information security managers, four office leaders and five advisors. The findings show that banks have a high focus on securing information. Nevertheless, there are some measures that banks can implement to increase safety even more. Among other things, it appears that inclusion and communication to employees could be better, and it is recommended to use reflection groups to increase the understanding and awareness of those working in the banking sector. In addition, it is seen that the introduction of new statutory requirements entails that banks have to change the way they work, which can lead to increased risk and vulnerability.

Forord

Denne masteravhandlingen er skrevet som en endelig del av masterstudiet i samfunnssikkerhet ved Universitetet i Stavanger (UiS). Disse to årene har vært lærerike, spennende, og ikke minst utfordrende. Gjennom studiet har vi hatt en bratt faglig utvikling, etablert nye bekjentskap, samt tilegnet oss en enorm kunnskap fra dyktige forelesere. Valget av tematikken for masteravhandlingen har vært vanskelig, da studiet gir rom for mange spennende vinklinger. Til slutt endte vi opp med å fokusere på informasjonssikkerhet, da dette er et svært spennende og dagsaktuelt tema.

Masteravhandlingen er gjennomført i tett samarbeid mellom to studenter med ulik bakgrunn, der en av oss tilhører det samfunnsvitenskapelige fakultet. Den andre tilhører teknisk-naturvitenskapelig fakultet. Det er samarbeidet om alle kapitlene i oppgaven, og det har vært fokus på lik fordeling av arbeidsmengde.

Vi vil rette en takk til vår veileder Kristiane M. Lindland som hele tiden har ledet oss inn på rett spor, på en positiv og motiverende måte. Vi vil også takke våre informanter som har tatt seg tid til å bli intervjuet, tross en hektisk hverdag. Uten deres faglige kunnskap som de har delt med oss, ville ikke oppgaven latt seg gjennomføre. Til slutt, og ikke minst vil vi takke våre familier for god støtte og forståelse for sene kvelder, samt helger dedikert til oppgaven.

Hjertelig takk!

Innholdsfortegnelse

Tabelloversikt

1. Innledning

Nyhetsbildet er ofte preget av saker som omhandler hendelser som har rammet informasjonssikkerheten i ulike virksomheter. Således er informasjonssikkerhet blitt et viktig system som man må sikre mot profesjonelle hackere som ønsker å benytte informasjon til egen vinning. Informasjonssikkerheten er utfordret av både intenderte og ikke intenderte handlinger, som medfører store konsekvenser for brukerne, virksomhetene og samfunnet. Hele samfunnet er avhengig av at betalingsformidlingen fungerer, dermed er det grunnleggende med effektive, robuste og stabile betalingssystemer (NSM, 2015). Med dette er det valgt å fokusere på banknæringen da dette er en kritisk samfunnsfunksjon, som er sårbare for blant annet profesjonelle hackere. Dette kan belyses med en hendelse i 2016 der det ble gjennomført et cyberangrep der angriperne benyttet stjålet legitimasjon for å stjele 81 millioner dollar fra kontoen som sentralbanken i Bangladesh har i den amerikanske sentralbanken (Norges Bank, 2017).

Digitaliseringen medfører økt risiko for uønskede hendelser på informasjonssystemene. Størsteparten av angrepene har som formål å stjele informasjon fra datasystemene til store eller viktige norske virksomheter. I 2014 ble det varslet 88 alvorlige dataangrep, sammenlignet med 51 i 2013 (NSM, 2015). Dette viser til en omfattende økning i antall dataangrep på ett år. Finansiell stabilitet er av betydning for hele det norske samfunnet, og er en verdi som forvaltes på virksomhetsnivå. Utfordringer som er knyttet til informasjonssikkerhet belyses blant annet av NOU (2015:13) der det vises til at ved manuelle papirbaserte prosesser har mennesker en viss forståelse for hvordan de skal sikre informasjon. Digitaliseringen derimot medfører at man i stor grad er fremmedgjort, og sårbarhetsbildet blir uoversiktlig.

Det er betydelige konsekvenser knyttet til angrep på informasjons- og kommunikasjonsteknologi (IKT), der mange mål kan rammes samtidig, og store mengder informasjon kan stjeles. Et vellykket datainnbrudd kan medføre tap av personopplysninger, og annen informasjon (NSM, 2015). Dette belyser hvorfor man må ha fokus på sikring av personopplysninger på nett. Noe som også vil være viktig for banknæringen, både i dag og i fremtiden. Dette er fordi at banknæringen øker bruken av applikasjoner og andre digitale

tjenester. I følgende delkapittel, vil det redegjøres for valg av problemstilling og tilhørende forskningsspørsmål.

1.1 Problembeskrivelse

Samfunnet er i større grad avhengig av IKT-baserte informasjonssystemer sammenlignet med tidligere, noe som fører med seg sårbarheter i det digitale rom. Økt avhengighet av internett kan medføre at nettverksbaserte angrep får omfattende skadevirkninger og kan potensielt nå hele spekteret av norske interesser. Trusselaktører i det digitale rom kan være hvem som helst, og metodene som benyttes blir stadig mer avanserte og målrettede (NOU 2016:19). Informasjonssystemer har blitt kjernen i moderne banker, og informasjon er blitt det mest verdifulle å beskytte mot innside og utside trusler og konkurrenter. De mest vanlige risikoene eller truslene mot banknæringen er phishing angrep (Ula, bt Ismail & Sidek, 2011). På bakgrunn av dette er det sett på viktigheten med å sikre god kunnskap om hva som forårsaker truslene og hvordan disse kan håndteres, noe som kan bidra til å sikre at informasjonen som bankene behandler ikke kommer på avveie. Med dette tar problemstillingen for seg nettopp denne problematikken.

Formålet med studien er å belyse hvordan banknæringen jobber med å sikre informasjon, og hvordan de ansatte forstår informasjonssikkerhet. Dette er på bakgrunn av digitaliseringen av banktjenestene, og stadig voksende kompleksitet i deres tjenester. I sammenheng med dette søkes det å belyse hvordan eksperter, her informasjonssikkerhetsledere, og bankansatte forstår risikoen for uønskede hendelser på bankens IKT-systemer. I tillegg søkes det å belys hvordan forståelsen for risikoen for uønskede hendelser avviker mellom ekspertene, mellomledere og rådgivere i banknæringen. Med dette er følgende problemstilling lagt til grunn:

"Hvordan forstår og jobber banknæringen for å møte risikoen for uønskede hendelser i forbindelse med informasjonssikkerhet?"

Det er utarbeidet følgende forskningsspørsmål som skal bidra til å besvare problemstillingen:

i) Hvilke faktorer påvirker risikostyring i banknæringen, og hva påvirker de ansattes forståelse av risiko og sårbarheter?

ii) Hvilke faktorer er nødvendige for å opprettholde god informasjonssikkerhet, og klarer banknæringen å oppfylle disse faktorene?

For å svare på problemstillingen er det valgt å se på hvordan de ansatte i banknæringen forstår risikoene og sårbarhetene som er knyttet til informasjonen de besitter om kundene. Med dette vil det fokuseres på uønskede hendelser som skyldes organisatoriske forhold, samt cyberangrep rettet mot informasjonssystemene. Med tanke på at banknæringen omfatter flere segmenter er det valgt å fokusere på sparebankene, og kontorene som har en direkte rådgivende funksjon rettet mot privatkunder. Ansatte innen banknæringen forstås i denne sammenheng som dem som arbeider direkte med informasjonssikkerhet, mellomledere, samt kunderådgivere i banknæringen. Det er intervjuet én informant i hver stillingsfunksjon fra hver bank.

Det er lagt vekt på hvorvidt cyberangrep, organisatoriske normer, tillit og sikkerhetskultur har en innvirkning på hvordan bankene sikrer seg mot uønskede hendelser. I tillegg er det fokusert på hvordan de ansatte i banknæringen arbeider med å forebygge uønskede hendelser i forbindelse med deres informasjonssikkerhetssystemer, samt hvordan deres forståelse påvirker dette arbeidet. Dermed er det lagt vekt på teorier om risiko og sårbarheter, risikostyring, risikopersepsjon, samt organisatoriske normer. I forbindelse med risikostyring innebærer dette alle vurderinger, og organisatoriske faktorer som er med på å bygge den forståelsen internt innen banknæringen. Gjennom aktuelle og nødvendige vurderinger bør bedrifter tydeliggjøre ønskelig sikkerhetsnivå, og hvilke trusler og sårbarheter som de må skjerme seg mot (NOU 2015:13; NOU 2016:19). Det er påpekt at fraværende rapportering innen banknæringen er et dagsaktuelt problem (Sviggum, 2017), dermed er det et tema som vil belyses i studien. Forskningsspørsmålene skal bidra til en forståelse for hvordan bankene arbeider for å sikre informasjon, samt hvilke faktorer som påvirker de ansatte og hvordan de sikrer informasjon i det daglige arbeidet.

1.2 Omfang og begrensninger

Informasjonssikkerhet er en tverrfaglig disiplin, som sprer seg over landets grenser. Dette studiet vil dog avgrenses. Dermed vil ikke den tekniske delen av informasjonssikkerhet vektlegges. Det velges heller å fokusere på de organisatoriske forholdene som er av betydning for sikring av informasjon. Samtidig vil det fokuseres på norske banker og forhold som de selv har mulighet til å påvirke, ved gjennomføring av ulike sikkerhetstiltak. Med dette søkes det å vurdere informasjonssikkerheten opp imot de organisatoriske og menneskelige faktorene innad

i bankene som er intervjuet. Med begrepet *informasjonssikkerhet innenfor bank* vil det i denne oppgaven bli analysert hvordan bankansatte forholder seg til dette fenomenet, og søker ved bruk av dette begrepet å forstå hvordan de håndterer opplysninger, og hvordan virksomhetene sikrer dette.

1.3 Oppgavens disposisjon

Første kapittel viser til utgangspunkt for studiet, problemstilling og forskningsspørsmålene, samt avgrensning av oppgaven.

Kapittel to redegjør for fenomenet informasjonssikkerhet og digitaliseringen av banknæringen, samt hvilke trusler bankene er utsatt for, etterfulgt av lovverk og krav som er relevante for banknæringen i lys av studiens innhold.

Kapittel tre innebærer gjennomgang av den teoretiske rammen for studiet. Her er det valgt å fokusere på teorier om risikostyring, risikopersepsjon, samt organisatoriske normer, og sentrale elementer som inngår i disse teoriene.

Kapittel fire presenterer studiens forskningsdesign og metodiske tilnærming, og inkluderer en refleksjon over de valg og vurderinger som tas underveis. Avslutningsvis diskuteres etiske betraktninger, samt studiens styrker og svakheter.

Kapittel fem vil beskrive studiens resultater i en empirisk presentasjon, strukturert etter forskningsspørsmålene som ble tydeliggjort i første kapittel.

Kapittel seks består av en diskusjon av resultatene, sett sammen med studiens teoretiske forankring, for å vurdere hvordan forskningsspørsmålene sammen kan besvare problemstillingen.

I kapittel vil det presenteres en konklusjon som skal besvare studiens problemstillingen.

2. Informasjonssikkerhet i norske banker

Følgende kapittel fremstiller rammene til studien. Det vil først gis en kort innføring i hva informasjonssikkerhet er, og betyr for denne oppgaven. Videre vil digitaliseringen av banknæringen beskrives, og hvordan denne har en innvirkning på banknæringen. Deretter vil rammeverket for IKT-sikkerhet i finanssektoren presenteres. Avslutningsvis vil ulike former for cyberangrep beskrives, etterfulgt av en kort innføring av relevante lover som gjelder for banknæringen.

Informasjonssikkerhet

For å kunne besvare problemstillingen er det nødvendig å undersøke hva informasjonssikkerhet innebærer, og hvilke aspekter som er viktig i forbindelse med sikring av opplysninger i banknæringen. Det er ikke én enkelt teori om informasjonssikkerhet, men flere teorier som tar for seg ulike elementer (Hong, Chi, Chao & Tang, 2003).

Begrepet informasjonssikkerhet omhandler blant annet tre elementer, *konfidensialitet, integritet* og *tilgjengelighet*. Konfidensialitet omhandler sikring av informasjon mot uvedkommende, og påse at kun autoriserte personer som har tilgang til denne informasjonen. I praksis er det ikke mulig å gjenopprette et brudd på konfidensialitet i det digitale rommet (NOU 2015:13), dermed er det viktig at personopplysninger om kunder i banknæringen ikke kommer på avveie. Integritet på sin side handler om å sikre fullstendig, nøyaktig og gyldig informasjon, samt behandling av den, og innebærer at informasjonen skal være til å stole på (NOU 2015:13). Tilgjengelighet skal på sin side sikre at tjenestene oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov (NOU 2012:10).

Det er som nevnt ikke en klar og entydig definisjon av begrepet informasjonssikkerhet og flere har utvidet begrepet til å også omhandle nøyaktighet, autentisk, nytte og besittelse. Tidligere var informasjonssikkerhet teknisk, men den digitale utviklingen har ført til en utvidelse av begrepet (von Solms & van Niekerk, 2013). Informasjonssikkerhet handler dermed også om tiltakene som anvendes for å sikre at informasjonen blir ivaretatt, også i forhold til IT-funksjonene som benyttes i finansnæringen for å overføre og behandle informasjon (DSB, 2014). Hvordan de tre kriteriene integritet, konfidensialitet og tilgjengelighet vektlegges, vil avhenge av hvilken type informasjon den enkelte virksomhet besitter og skal sikre. Informasjonssikkerhet består av både fysisk- og logisk sikring. Fysisk sikring innebærer sikring

av all informasjon både i IT-systemer, og i papirformat mot fysisk tilgang fra utenforstående personer, eller mot naturkatastrofer. Fysisk sikring kan for eksempel være adgangskort og koder som kun rettshaverne besitter, eller ved at man har en back-up, eller informasjonen lagret i en sky. Logisk sikring er bevaring av konfidensialitet, integritet og tilgjengelighet av IT-systemer, der man sikrer seg mot uønskede hendelser som blant annet hacking, virus og sabotasje (Skuterud, 2003).

2.1 Digitaliseringen av banknæringen

For å få en forståelse for de store endringene som banknæringen har gjennomgått og stadig gjennomgår, vil det først gis en presentasjon av den mer generelle digitaliseringen. Deretter vil de nye trendene som er mer spesifikke for banknæringen og måten de leverer sine tjenester på trekkes frem. Utviklingen av digitale medier kan historisk sett deles inn i tre faser (Hannemyr, 2015). De tre fasene har hatt store ringvirkninger for handels- og næringsindustrien. Apple sin utvikling av mer funksjonelle og brukervennlige datamaskiner bidro til et større antall personer som tok maskinen i anvendelse til hverdagsbruk. Internett har i fase 2 gjort det stadig enklere å utveksle informasjon på kryss og tvers av landegrensene. Veksten i antallet internettbrukere var voldsom, og spredte seg mange ganger raskere enn både avislesing, radio og fjernsyn (Hylland-Eriksen, 2005). I tillegg åpnet internett mulighetene for elektronisk handel som ikke var begrenset av åpningstider og fysiske møter, og var med på å endre kundebehovet (Giovannetti, Kagami & Tsuji, 2003).

Den siste fasen karakteriseres av mobiltelefoner som har blitt stadig mer elementære bindeledd mellom forbrukeren og omverdenen. Alle disse utviklingene har vært med på å danne et essensielt skifte i måten bankene leverer sine tjenester på, der selvbetjeningsløsningene får et større fokus (Pikkarainen, Pikkarainen, Karjaluoto & Pahnila, 2004). Den teknologiske utviklingen innen banknæringen, samt andre sektorer kjennetegnes av disruptiv teknologi. Dette er teknologi som består av nyskapninger som forstyrrer den eksisterende markedsflyten og kundebehovet. Utfordringen ved disruptiv teknologi er at infrastrukturen i store organisasjoner har vanskeligheter med å håndtere slike store omveltninger. Banknæringen er ansett som spesielt utsatt (Christensen, 1997). Med dette er forfatteren kritisk til bankens fremtidige rolle, og mener at bankens rolle i stor grad vil bli overtatt av eksterne IT-selskaper. Samtidig ser man at finansnæringen gjør store grep for å forsøke å svare på utfordringene

knyttet til disruptiv innovasjon, for eksempel gjennom store investeringer i IT og teknologi (Denning, 2014; Lorentzen, 2016).

I 2015 utga World Economics Forum (WEF) en rapport der det ble undersøkt hvilke innovasjoner som ville ha størst påvirkning på bank- og finansnæringen, og i hvilken grad disse innovasjonene ville påvirke fremtiden. Her ble det fremstilt stadig større overgangen til et kontantløst samfunn, som skaper et kontinuerlig press på bankene, der det kreves at de leverer stadig bedre tjenester (WEF, 2015). Dette er en utvikling man i stadig større grad observerer i Norge og i banktjenestene. Norge er et av de mest ledende landene når det kommer til å ta i bruk ny teknologi og vokse sammen med digitaliseringen, og en antar at Norge skal være et av de første landene til å bli helt kontantløst (Lorch-Falch, 2014).

2.2 Risiko og sårbarheter i banknæringen grunnet digitaliseringen

Risiko omhandler fremtiden, og har således en grad av usikkerhet knyttet til seg (Engen et al., 2016). Risiko for cyberangrep er et voksende problem innen finansnæringen, og kostnadene som oppstår ved cyberangrep mot finansnæringen ble ansett som de største kostnadene for å reparere skadene dette medfølger. Et worst-case scenario som er tenkelig innen finansnæringen er eksempelvis organisert cyberkriminalitet som forårsaker at finanstjenestene opplever et bortfall som strekker seg utover flere dager, og som fører til tap på over flere billioner dollar (Camillo, 2016). I tillegg kan ikke-intenderte hendelser være en utfordring for banknæringen i forbindelse med sikring av informasjon. Dette belyser eksempelvis NOU (2015:13), da de viser til menneskelige feilhandlinger som en årsak til uønskede hendelser i banknæringen.

2.2.1 Intenderte hendelser

På tross av at digitalisering har forenklet hverdagen til enkeltindividet, og er en driver for innovasjon, økonomisk vekst og produktivitet, skaper teknologien også nye sårbarheter og utfordringer i banknæringen. Den gir blant annet en utvidet **angrepsflate** for kriminelle. Grunnet rask vekst innen digitaliseringen, kan en vente at man i stor grad vil mangle kompetanse på disse områdene. Dette kan føre til at bankene er dårligere rustet til å bekjempe kjente og ukjente trusler. En bred analyse viser til at digitaliseringen i stor grad er fremmedgjort, og ingen har en total oversikt over sårbarhetsbildet. I dag er harddisker smarte og lagrer data fortløpende. Dette innebærer at lagringsenheten har full tilgang til systemets internminne, og kan misbrukes ved at det leses inn til andre steder enn ment (NOU 2015:13). Samtidig viser

Financial Times til en undersøkelse, der det fremkommer at 1/3 av alle cyberangrep mot bankene lykkes (Mehta, 2017).

Cyberangrep er en intendert handling, og utføres av ulike grupper av trusselaktører som har varierende motivasjon og tilgang på ressurser, samt grad av kunnskap og organisering. Motivene for cyberangrep kan blant annet være økonomisk vinning, stjele informasjon eller å forstyrre tjenesten. Aktørene som står bak angrepene kan være organiserte kriminelle, hackeraktivister eller utro tjenere. I enkelte tilfeller kan kriminelle også være støttet av andre lands myndigheter. Angrep kan være målrettet mot et spesifikt offer, eller ramme tilfeldige (NOU 2015:13; Norges Bank, 2017). Et vellykket cyberangrep kan gjøre stor skade på den globale finansielle infrastrukturen. Betalingssystemene er gjennomgående sentraliserte, noe som gjør dem sårbare for cyberangrep. Et vellykket cyberangrep på den finansielle infrastrukturen kan medføre tap av store verdier og føre til at kunder ikke får gjennomført sine betalinger. Et vellykket angrep kan også innebære at sensitiv informasjon kommer på avveie (NOU 2015:13).

Aktørene som utfører cyberangrep benytter seg av ulike *metoder og verktøy* som, anonymiseringstjenester, kryptering og virtuell valuta. Fremgangsmåtene er med på å skjule hvem som kommuniserer, og hva som blir formidlet. Dette vanskeliggjør sporing av økonomiske transaksjoner (NOU 2015:13). *Sosial hacking* er en metode som går direkte på de ansatte i en organisasjon, som i en bank. Denne metoden innebærer at angriperen sender ansatte persontilpassede e-postmeldinger med infiserte vedlegg eller lenker. En annen metode som benyttes er oppringing for å lure den ansatte til å oppgi informasjon om virksomhetens sikkerhetssystemer. Ut i fra erfaring er det bestandig noen som lar seg lure av slike angrep, og det rapporteres om en økning i antall phisingangrep. Denne metoden kan også foregå via SMS, eller sosiale medier (NOU 2015:13).

2.2.2 Ikke-intenderte hendelser

Ikke-intenderte hendelser forekommer av eksempelvis teknisk svikt, menneskelige feilhandlinger og organisatoriske faktorer, og er hendelser som oppstår uten at det foreligger en intensjon om å medføre skade (Aven, Boyesen, Njå, Olsen & Sandve, 2004). Den raske utviklingen av digitale tjenester kan medføre svikt i systemene, noe som kan karakteriseres som en ikke-intendert hendelse. I tillegg kan slike hendelser forekomme av naturlige årsaker, som lynnedslag. Det kan også være menneskelige feilhandlinger som utføres ubevisst. Dette

kan eksempelvis være en ansatt som programmerer feil ved et uhell, noe som kan føre til at systemene krasjer, som kan medføre utfordringer for brukerne og virksomheten i sin helhet. Det er viktig å ha fokus på både intenderte og ikke-intenderte hendelser når man vurdere risiko og sårbarheter i forbindelse med IKT-sikkerhet (Kraemer & Carayon, 2006).

2.3 Standarder og beste praksis i norske banker

Standarder gir en beskrivelse av mål i tillegg til å klargjøre hvordan de kan oppnås. Det er mer enn et dusin standarder i 27000-familien, dermed er det opp til næringen selv å lage styringsdokumenter som skal oppfylle kravene. Dette kan medføre ulik håndtering av informasjonssikkerhet i de ulike organisasjonene. Banknæringen er underlagt en rekke internasjonale standarder (ISO-standarder) som skal sikre informasjon, blant annet ISO 27000, ISO 27001 (ISACA, 2018). I det følgende vil en beskrivelse av ISO-27000 og ISO 27001 presenteres.

ISO-standarder presenterer modeller som skal sikre at styringssystemene for informasjonssikkerhet oppfyller kravene om konfidensialitet, integritet og tilgjengelighet. Hovedkravet til standarden er at virksomheten skal etablere, implementere, vedlikeholde og forbedre et styringssystem for informasjonssikkerhet. ISO-27001 omfatter alt fra tilgangskontroll, sikkerhetspolicy, personellsikkerhet og vedlikehold. Håndtering av hendelser er også en vesentlig del av å sikre åpenhet om hendelser og sårbarheter, samt etablere en lærende kultur i virksomheten. *Compliance* nevnes også i denne standarden, og går ut på å sikre at lover og regler blir overholdt (Difi, 2013).

2.4 Lovkrav som berører den norske banknæringen

Det finnes flere lover som direkte og indirekte legger føringer for informasjonssikkerheten i banknæringen. Det er blant annet forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften), lov om behandling av personopplysninger (personopplysningsloven), *General Data Protection Regulation* (GDPR) *og Revised Payment Service Directive* (PSD2) som har en direkte innvirkning på sikring av informasjon i bankene. Med dette er oppgaven avgrenset til disse følgende lovkravene.

IKT-forskriften

Banknæringen er underlagt IKT-forskriftene, og hensikten er å sikre at banknæringen fastsetter overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten. Det skal også foreligge en beskrivelse av de enkelte prosessene, samt hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en sikker måte. Dersom virksomheten har eksterne brukere av IKT-systemene, skal det foreligge avtaler som skal sikre at forskriftenes krav til sikkerhet og dokumentasjon ivaretas. Forskriftene omfatter blant annet krav til at virksomheten skal gjennomføre risiko- og sårbarhetsanalyser (ROS-analyser) en gang i året. Risikoanalyseprosessen skal dokumenteres med definerte ansvarsforhold og tiltak som iverksettes som et resultat av den gjennomførte risikoanalysen (IKT-systemer, 2003).

Personopplysningsloven

Personopplysningsloven skal beskytte enkeltindivider mot krenkelser ved behandling av personopplysninger. Den skal også bidra til at personopplysninger blir behandlet i overensstemmelse med grunnleggende personvernhensyn. Loven omfatter behov for personlig integritet, privatlivets fred, og tilstrekkelig kvalitet på personopplysninger (Personopplysningsloven, 2001).

GDPR

I løpet av 2018 skal EU/ EØS´s forordning for personvern bli norsk lov, og stiller krav til at virksomhetene skal ha etablerte rutiner for å sikre etterlevelse etter personopplysningsloven. Forordningen innebærer nye krav, som igjen vil føre til at virksomhetene må endre de etablerte rutinene slik at de er i samsvar med det nye regelverket (Datatilsynet, 2016). Forenklet kan man si at GDPR handler om samtykke, sikker lagring og sletting av data. Brudd på loven kan medføre store økonomiske konsekvenser for virksomhetene, da bøtene for brudd kan utgjøre 20 millioner euro, eller 4% av bedriftens globale omsetning (Moe, 2018).

PSD2

PSD2 er en endring som fører til at bankenes monopol på kundenes kontoinformasjon og betalingstjenester forsvinner. Med andre ord gjør PSD2 det mulig for bankkunder å benytte tredjepartsleverandører, i stedet for sin opprinnelige bank. Framtidig vil dette gi muligheter til å eksempelvis benytte Facebook og Google til å utføre betalinger, overføringer, samt drifte eget

forbruk. Samtidig vil bankene i Norge være pålagt å gi tredjepartsleverandørene tilgang til kundenes informasjon. Det nye EU-direktivet åpner opp for alle selskaper som er interessert i å benytte seg av bankenes informasjon (Evry, u.å).

Digitaliseringen av banknæringen har som nevnt gjennomgått store endringer. Den vil fortsette å ha en rask utvikling, noe som vil kreve stadig bedre kunnskap om hvordan digitaliseringen vil kunne påvirke sikkerheten i banknæringen. Digitaliseringen medfører nye lovkrav og retningslinjer som må etterleves, for å påse at sikkerheten blir ivaretatt. På bakgrunn av dette, er det interessant å studere hvordan bankansatte forstår risikoen for uønskede hendelser i forbindelse med IKT-systemene, og hvilke organisatoriske forhold som er av betydning for hvordan de arbeider med å forebygge uønskede hendelser.

3. Teoretisk forankring

I dette kapittelet vil studiens teoretiske forankring beskrives, for å kunne svare på studiens problemstilling. Hvordan bankansatte erkjenner risikoer og sårbarheter i informasjonssystemene vil ha en betydning for hvordan de arbeider. Dermed er det valgt å anvende teorier som adresserer disse aspektene. Oppgavens problemstilling er todelt. På den ene siden søkes det en forståelse for hvordan de ansatte i banknæringen arbeider for å unngå uønskede hendelser, mens det på den andre siden søkes innsikt i hvordan de ansatte forstår risiko knyttet til uønskede hendelser i forbindelse med informasjonssystemene.

For å belyse den første delen av problemstillingen, er det benyttet teorier som tar for seg de organisatoriske faktorene som er av betydning for risikostyringsprosessen. Dette er fordi at en god risikostyringsprosess oppnås ikke ved å bare gjennomføre risikoanalyser, etablere rutiner og håndbøker, men er et samspill mellom alle disse elementene. Det er også benyttet teorier om risiko og sårbarhet for å få en forståelse for hva disse begrepene innebærer i forbindelse med informasjonssikkerhet. I tillegg er det benyttet teorier om risikopersepsjon som er med på å belyse faktorer som kan bidra til å forklare hva som påvirker bankansatte når det kommer til beslutninger som tas i forbindelse med sikring av informasjon. Teoriene er viktige for å få en forståelse for hvordan de ansatte arbeider for å unngå uønskede hendelser, og hvorfor bestemte beslutninger blir foretatt i forbindelse med dette.

For å besvare den andre delen av problemstillingen, hvordan banknæringen forstår risikoen for intenderte og ikke-intenderte hendelser, er det nødvendig å se på faktorer som påvirker de ansattes forståelse. Dermed er det benyttet teorier om sikkerhetskultur og organisatoriske normer, siden dette er faktorer som anses å påvirke de ansattes forståelse for sikkerhetsarbeidet.

For å besvare problemstillingen er det utarbeidet to forskningsspørsmål. For å besvare forskningsspørsmål *i) Hvilke faktorer påvirker risikostyring i banknæringen, og hva påvirker de ansattes forståelse av risiko og sårbarheter?* Er det blitt valgt å benytte teorier om risiko og sårbarhet, samt ROS-analyser. Dette for å skape en forståelse for hva risiko og sårbarhet er, og hvordan den vurderes. Dette skal bidra til å gi leseren en forståelse for hvorfor ulike uønskede hendelser kan oppstå. Begrepet kan brukes som en pekepinn for hvilke tiltak som kan være aktuelle å iverksette for å styrke banknæringen i forhold til trusler som kan påvirke informasjonssikkerheten. I forbindelse med risikostyring i banknæringen er det lagt vekt på

organisatoriske faktorer som kommunikasjon og inkludering, integrering samt refleksjon. Dette er faktorer som er av betydning for en god risikostyringsprosess. Avslutningsvis er det benyttet teorier som forklarer risikopersepsjon og hvordan de ansattes risikoforståelse er av betydning for å unngå uønskede hendelser. Teorier om risikopersepsjon kan bidra til å gi en forståelse for hvordan de ulike bankene jobber for å sikre seg mot uønskede hendelser i forbindelse med sikring av informasjon.

For å besvare forskningsspørsmål *ii) Hvilke faktorer er nødvendige for å opprettholde god informasjonssikkerhet, og klarer banknæringen å oppfylle disse faktorene?* Er det benyttet teorier om sikkerhetskultur og informasjonssikkerhetskultur for å belyse de organisatoriske faktorene som er av betydning for informasjonssikkerheten i banknæringen. Det er valgt å belyse disse begrepene siden de tar for seg flere elementer som påvirker alle ansatte på tvers av nivåer. Det er fokusert på organisatoriske normer, innflytelse fra ledelsen, samt sikkerhetsbevissthetsprogrammer. I de kommende delkapitlene vil de ulike teoriene som er anvendt for å besvare forskningsspørsmålene presenteres.

3.1 Risiko og sårbarhet

Risiko omhandler kommende hendelser, som kan resultere i positive og negative utfall for noe en organisasjon verdsetter (Njå, Solberg & Braut, 2017). I forbindelse med informasjonssikkerhet i banknæringen kan dette omhandle risiko knyttet til blant annet tekniske, organisatoriske, finansielle og juridiske forhold (von Solms & van Niekerk, 2013). I denne forbindelse søkes det å se på hvordan eksperter, her informasjonssikkerhetsledere, og bankansatte forstår risikoen for uønskede hendelser på bankens IKT-systemer. Når det kommer til IKT-systemer og risikoer forbundet med informasjonssikkerhet, kan dette være krevende å gjenkjenne. Årsaken til dette henger sammen med at det er stor usikkerhet knyttet til mulige konsekvenser tilknyttet dette feltet. Risikoanalyser og verdivurderinger kan bidra til å gi nødvendig innsikt, for å håndtere denne utfordringen (Aven et al., 2004).

Når det gjelder cyberangrep i finansnæringen kan også sårbarhet være et problem, som kan tillate trusselagenter å utnytte svakheter eller feil i systemene. Dette kan gi trusselagenten uautorisert tilgang til virksomhetens informasjon. Med dette kan sårbarhet defineres som et systems forutsetninger for, eller manglende evne til å fungere under/etter at det har blitt utsatt for en uønsket hendelse (Engen et al., 2016; Aven et al., 2011). Sårbarhet kan her forstås som forutsetningene for at driftsforstyrrelser med negative følger eller alvorlige hendelser kan

inntreffe, og utfordringene med å gjenopprette funksjonaliteten i etterkant. Bortfall av finansielle tjenester, eller en betydelig endring i en slik kritisk infrastruktur kan medføre store konsekvenser for verdi, liv og helse. Det påpekes utover dette at teknologiske systemer ofte inneholder sårbarheter (Engen et al., 2016). Dette kan utnyttes av grupper eller individer, som ved en tilsiktet handling ønsker å oppnå personlig gevinst, eller skade en bruker av systemet (Rausand & Utne, 2009). Noe som kan være bekymringsverdig for de som blir utsatt. Det er derfor viktig å sikre robuste systemer, slik at systemet har evne til å unngå skader og/eller tap. Robusthet er proaktivt, og er noe man planlegger og bygger inn i et system som skal sikre informasjon. Robusthet kan defineres som fleksibilitet og tilpasning. En robust organisasjon har evnen til å tilpasse seg forventede, samt uforventede forstyrrelser, og til å gjenopprette funksjonaliteten etter en alvorlig hendelse (Engen et al., 2016). Leveson (2011) påpeker utfordringer relatert til tiden det tar for produsenter å utvikle nye produkter. Tiden er betydelig redusert, og i mange tilfeller har man ikke mulighet til å teste produktene i like stor grad som tidligere, grunnet tidspress. Når man skal vurdere risikoer forbundet med informasjonssystemene er det viktig å ha mest mulig fakta om situasjonen i dag. En bør ha evnen til å se hva som vil endre seg over tid, og den raske utviklingen innen teknologien innebærer sårbarheter knyttet til risiko (Berg, 2012). Dette kan også relateres til IKT-systemer, siden dette er systemer som er i rask utvikling.

3.2 Risikostyring

Alle virksomheter er pålagt å kartlegge trusler og vurdere risiko, samt utarbeide tilhørende risikoreduserende tiltak (Internkontrollforskriften, 1996). Risikostyring dreier seg om handlinger og mål, som bestemmes på bakgrunn av et relevant risikobilde. I risikostyringsprosessen tar man for seg styring, aktører, regler og prosesser. Sammen skaper dette et helhetlig situasjonsbilde, og bistår bedriften i å avdekke, samt vurdere risiko (Aven & Renn, 2010; Aven, 2015). I en rapport utarbeidet av Committee of Sponsoring Organizations of the treadway Commission (COSO, 2004) vises det til denne definisjonen av risikostyring, som vil bli lagt til grunn i denne oppgaven:

> *Helhetlig risikostyring er en prosess, gjennomført av virksomhetens styre, ledelse og ansatte, anvendt i fastsettelse av strategi og på tvers av virksomheten, utformet for å identifisere potensielle hendelser som kan påvirke virksomheten, og håndtere risiko slik at den er i samsvar med virksomhetens risikoappetitt, for å gi rimelig grad av sikkerhet for virksomhetens måloppnåelse.*

Risikostyring er metodene som anvendes for å overvåke risiko innenfor en organisasjon. De fleste banker krever eierstyring og selskapsledelse (*corporate governance*) som en del av deres organisatoriske strategi for å dempe risiko (Rahima, Mahatb, Nassirb & Yahyab, 2015). Risikostyring vil være ulike tiltak og aktiviteter som kan gjøre risiko mer håndterbart, der formålet med risikostyring er å sikre den riktige balansen mellom det å skape verdier, samt å unngå ulykker, skader og tap (Aven et al., 2004). Risikostyring er ikke en ensidig prosess, og er heller ikke én enkel modell som enkelt kan overføres til en organisasjon.

Hvilke metoder man benytter for å kartlegge risikobildet er opp til de individuelle virksomhetene. Risikostyring er en krevende prosess, der vanskeligheter ofte kommer av avvikende forståelse og innsikt i elementære aspekter. Dette angår en forståelse for hva risiko er, samt hvordan man gjengir og kommuniserer risiko (Aven, 2007). Hvordan organisasjoner utfører risikostyring i forbindelse med informasjonssikkerhet, kan ha direkte innvirkning på IKT-sikkerheten. Således utgjør dette rammen for studien, og spesielt ettersom virksomheters risikostyring legger føringer for ekspertenes vurderinger av risiko.

Det er tre prinsipper som bør vurderes for å oppnå god risikostyring, særlig i forbindelse med usikre og komplekse/tvetydige risikoer. De tre prinsippene er som følgende:

- kommunikasjon og inkludering
- integrering
- refleksjon

Disse tre prinsippene vil bli nærmere omtalt i de følgende avsnittene, og bør vurderes i hvert trinn eller stadium av risikostyringsprosessen, fremfor som separate steg eller stadier (Asselt & Renn, 2011).

3.2.1 Kommunikasjon og inkludering

Kommunikasjon gjenspeiler et meningsfullt samspill der kunnskap, erfaringer, tolkninger, bekymringer og perspektiver utveksles (Löfstedt, 2003). I sammenheng med risikostyring er toveiskommunikasjon en viktig faktor for å oppnå god risikostyring (Pidgeon et al., 2005). Årsaken til dette henger sammen med at gjensidig kommunikasjon er en av de største utfordringene innen risikostyring. Det er ikke et eget trinn, i motsetning til hvordan det ofte behandles, men sentralt gjennom hele arbeidet (Asselt & Renn, 2011). Kommunikasjon er kjernen i enhver vellykket risikostyringsaktivitet (Pidgeon et al., 2005).

Kommunikasjon i forbindelse med risikostyring refererer til utveksling av informasjon mellom beslutningstakere, eksperter, interessenter, allmennheten og hverandre. Effektiv risikokommunikasjon bør være en integrert del av risikostyringen (Frewer, 2004). Formålet med kommunikasjon er å gi et bedre grunnlag for styring av usikre og komplekse/tvetydige risikoer. Kommunikasjon i sammenheng med risikostyring er imidlertid ikke enkel. Det er ikke tilstrekkelig med organisert kommunikasjon. Hovedutfordringen er å legge til rette for at ulike aktører fra forskjellige bakgrunner lykkes i å samhandle meningsfylt i møte med usikkerhet, kompleksitet/tvetydighet. Sosial læring er nødvendig for å finne ut hvilken type kommunikasjonsform som er nødvendig å opprettholde med ulike aktører i de ulike fasene av risikostyringen (Asselt & Renn, 2011).

For at risikostyring skal fungere, er man også avhengig av inkludering. Inkludering betyr at ulike aktører er inkludert, samt at de spiller en nøkkelrolle i utforming eller forhåndsevaluering av risikoen (Renn, 2008). Inkludering bør være åpen og adaptiv på samme tid (Stirling, 2007). Vesentlige problemer for å oppnå dette er å kunne definere hvem som er inkludert, hva som er inkludert, samt omfanget og mandatet til risikostyringsprosessen. Inkludering kan ta forskjellige former, blant annet rundbord, åpne fora, forhandlet regelverk, øvelser, mekling eller blandede rådgivende komiteer, inkludert forskere og interessenter (Asselt & Renn, 2011; Renn, 2008).

Det er flere grunner til at man argumenterer for inkludering. For det første hevdes det at i lys av usikkerhet, kompleksitet og tvetydighet, er det nødvendig å utforske ulike kilder til informasjon og å identifisere ulike perspektiver. Det er viktig å vite hva de ulike aktørene opplever som risikoproblemer, da dette vil kunne føre til integrering av all relevant kunnskap og inkludering som beror seg internt i en organisasjon. For det andre hevdes det at aktører som er berørt av risikoen og/eller hvordan risikoen styres, har en rett til å delta i å avgjøre om disse risikoene. Med denne oppfatningen er inkludering også en måte å koordinere risiko på, samt evaluering og utforming av risikostyring (Asselt & Renn, 2011). Inkludering har vist seg å ha en positiv effekt, da det gir bedre kvalitet på beslutningstakingen (Bierle, 2000). Dette er fordi man oppnår et bredere perspektiv av det som blir vurdert (Charley & Engelbert, 2005).

3.2.2 Integrasjon

Integrasjon refererer til behovet for å samle all relevant kunnskap og erfaring fra ulike disipliner og ulike kilder, inkludert usikkerhet og informasjon av risikooppfattelser samt verdier. Ekspertkunnskap spiller en rolle innen risikostyring, men bør likevel ikke anses som tilstrekkelig for å unngå risikoproblemer (Renn, 2008). Dette fordi risiko som består av usikkerhet, kompleksitet og/eller tvetydighet kan ikke identifiseres ved den tradisjonelle forståelsen av risiko (Aven, 2015). Dessuten handler ikke risikostyring kun om risiko, og særlig ikke om en enkelt risiko. Derfor krever risikostyring risikovurdering(er) og evaluering(er). For å forstå risikoer og sårbarheter på best mulig grunnlag, er det nødvendig å innhente kunnskap og erfaringer fra lekfolk (Aven, 2015), som for eksempel bankkundene. Kulturelle og sosiale verdier, samt preferansesyn og verdenssyn vil også kunne bidra til en utvidet oppfattelse av risikoen som den enkelte organisasjon kan oppleve (Asselt & Renn, 2011).

3.2.3 Refleksjon

Det er viktig at aktørene innen banknæringen reflekterer over det de gjør, og tydeliggjør omfanget av risikoen som blir vurdert, da den kan være svært usikker, kompleks og/eller tvetydig (Beck, Giddens & Lash, 1994). Dette for å unngå at man strekker seg mot enkle og kjente rutiner for å behandle denne typen risiko. Refleksjon viser til behovet for er en kollektiv diskusjon, for å kunne overveie de ulempene og fordelene som kan oppstå ved ulike tiltak. Det klassiske spørsmålet innen risikostyring er: "Hvor trygt er trygt nok? " Refleksjonsbegrepet erstatter dette spørsmålet med: "Hvor mye usikkerhet er vi villige å akseptere i bytte mot noen fordeler?". Med dette flyttes fokuset fra sikkerhet til usikkerhet (Asselt & Renn, 2011).

3.2.4 Risiko- og sårbarhetsanalyser (ROS-analyser)

Risiko- og sårbarhetsanalyse er en viktig del av risikostyringen, dermed er det valgt å beskrive det videre i dette teorikapittelet. ROS-analysene er en proaktiv tilnærming, ved at den forholder seg til potensielle trusler og farer. ROS-analyser består av systematisk bruk av tilgjengelig informasjon, for å identifisere farer og risikoer, og for å estimere risikoen for menneskene, virksomheten og miljøet. ROS-analyser vil kunne gi støtte ved beslutninger som angår sikkerhet, da de kan avdekke og utbedre svakheter som truer virksomheten. Svakheter som blir avdekket og utbedret på en riktig og kostnadseffektiv måte, kan gi økt pålitelighet og større driftssikkerhet, samt styrke virksomheten totalt sett (Aven et al., 2004; Johnsen, 2009).

3.3 Risikopersepsjon

Hva som anses som en risiko er avhengig av hvem, hvordan og hva som vurderes (Aven et al., 2004; Engen et. al., 2016). Mennesker konstruerer deres egen realitet og evaluerer risiko i samsvar med deres subjektive persepsjon. Denne type intuitiv risikopersepsjon er basert på hvordan informasjon om risikokilden er kommunisert, de psykologiske mekanismene for å prosessere usikkerhet, og tidligere erfaringer. I den moderne verden er risiko forstått og reagert på med utgangspunkt i to fundamentale måter. Risiko som følelser refererer til vår instinktive og intuitive reaksjon til farer. Risiko som analyse medfører logikk, årsak, og vitenskapelige diskusjoner om risikostyring (Slovic & Peters, 2006). I den første måten å forstå og reagere på risiko viser til risikopersepsjon.

Risikopersepsjon betegner hvordan man erkjenner signaler eller informasjon om potensielle uønskede hendelser, og hvordan man skaper egen forståelse av hvor alvorlig en uønsket hendelse er. Menneskets atferd er hovedsakelig drevet av persepsjon, ikke fakta, og at man benytter sin egen forståelse for å vurdere ulike risikoer. Mennesker linker forventninger, håp, frykt og følelser sammen med aktiviteter eller hendelser som har usikre utfall, og følger ofte kognitive mønster for å skape forventninger til risiko og for å evaluere den (Aven & Renn, 2011; Renn, 2008). Beslutningstakere vil som ifølge dette vurdere fordeler mot ulemper for å ta et valg om man skal utøve en handling eller ei. Dette er en generelt tidkrevende analyseprosess, og mennesket vil ved manglende kunnskap og informasjon bruke intuisjon og heuristikker for å forenkle oppgaven (Renn, 2008).

Heuristikker er en form for intuitiv forenklingsstrategi, og er uavhengige av risikoen som studeres, personlig tro, følelser, samt andre persepsjonsmønster. Heuristikkene bidrar til å velge samt vurdere alvorligheten av risiko. Strategien anvendes av både lekmenn og eksperter, og man bruker "sunn fornuft" for å behandle informasjon. Når man vurderer risikoer, vil man som regel anvende tommelfingerregler, fremfor rasjonelle beslutningsmetoder. Faren ved denne måten å vurdere risiko på, er at man ikke alltid ser sammenhenger som faktisk eksisterer, som igjen kan føre til at man tar feil beslutning (Renn, 2008).

Man kan også se forskjeller i hvordan lekfolk og eksperter vurderer risiko (Sjøberg & Sjøberg, 2001). Tillit kan betraktes som en sosial og relasjonell tilstand der man er sårbar overfor andres beslutninger, som baseres på en antakelse om like verdigrunnlag (Earle & Siegrist, 2008).

Begrepet kan bidra til å forstå hvordan mennesker vil reagere på endringer som kan påvirke informasjonssikkerheten (Fukuyama, 1996). Tillit opprettes vanligvis sakte, men kan bli ødelagt på et øyeblikk ved et enkelt uhell eller feil. Når tillit er tapt, kan det derfor ta lang tid å gjenoppbygge den til sin tidligere tilstand. I noen tilfeller kan mistet tillit aldri bli gjenvunnet (Slovic, 1999).

Forskning viser til at *tillit* avhenger av informasjonen som mennesker mottar av ekspertene, som man igjen har tillit til. Tiltroen som lekfolk har til eksperter vil også være avhengig av hvorvidt ekspertene deler likt verdisyn med lekfolket. Dersom tilliten eksisterer, vil dette kunne bidra til et mindre kritisk syn på risiko som teknologien kan inneha (Siegriest, 2000; Siegrist, Cvetkovich & Roth, 2000). Årsaken til at individer uttrykker tillit til mottakeren er fordi de har manglende kunnskap om hva som kan forårsake en uønsket situasjon, og de tar ofte for seg få eller ingen forhåndsregler for å unngå dette. Bakgrunnen for dette, kan være basert på at tillitsgiveren ikke vet at det eksisterer forhåndsregler, eller ikke vet at det er mulig å forebygge det. Dette er med på å gjøre individet sårbart i et komplekst og digitalt samfunn. Videre vil mennesker ha tillit til de ulike systemene de anvender, dersom de har en positiv erfaring til dem. Ut i fra dette vil tillitsgiveren ha en forventning om at mottakeren har tilstrekkelig kompetanse for å sikre at de ikke blir utsatt for uønskede hendelser, uten at de har noen garanti for at dette er tilfellet (Grimen, 2009).

3.4 Organisatoriske forhold som er av betydning for sikring av informasjon

Hvordan informasjonssikkerheten blir ivaretatt i banknæringen, vil avhenge av den interne organisasjonskulturen, og hvordan den enkelte organisasjon forholder seg til dette fenomenet (Chen, Ramamurthy & Wen, 2014; Dhillon, Syed & Pedron, 2016; Soomro, Shah & Ahmed, 2016). Dermed har forskning beveget seg stadig lengre bort fra å forstå sikkerhetssystemene, til å heller fokusere på forståelsen til de ansatte, samt hvordan de forstår informasjonssikkerhet. Det er flere aspekter på arbeidsplassen som påvirker hvordan ansatte forholder seg til informasjonssikkerhet.

3.4.1 Organisatoriske normer

Det er flere teorier som viser til sikkerhetskultur som en viktig faktor for å hindre at ulykker inntreffer. Organisatoriske ulykker påpeker at sikkerhetskulturen er en avgjørende faktor for et

proaktivt sikkerhetsarbeid i en næring som opererer med sikkerhetskritiske oppgaver (Reason, 1997), som banknæringen. For å forstå sikkerhetskulturens funksjon i lys av informasjonssikkerhet, er både sikkerhetskultur og informasjonssikkerhetskultur benyttet, da begge konseptene er aktuelle for oppgaven. Sikkerhetskultur og informasjonssikkerhetskultur er tidvis overlappende, og bidrar til økt sikkerhetsutførelse og forståelse av fenomenet som studeres.

Organisatoriske ulykker oppstår blant annet ved at organisasjonskulturen ikke har en felles oppfatning av viktigheten med sikkerhet, og en felles tro på effekten av forebyggende tiltak. Dersom dette er tilfellet, vil denne mangelen kunne føre til organisasjonsulykker. Slike ulykker oppstår i samspill mellom latente forhold i organisasjonen som berører blant annet ledelse, planlegging, og forholdet mellom menneskene og det tekniske, samt aktive feil som begås av mennesket. Derfor søker man etter å forhindre ulykker ved å utvikle barrierer, slik at latente forhold ikke utløser katastrofer, eller blir svekket, herunder en god sikkerhetskultur (Reason, 1997). I tillegg viser tidligere forskning at ledelsen spiller en stor rolle i hvordan ansattes persepsjon på informasjonssikkerhet blir formet. Reddick (2009) viser til sentrale faktorer for hvordan bedrifter opererer med informasjonssikkerhet. En av disse faktorene omhandler ledelsens innflytelse, herunder påpeker forskeren at ledelsens rolle er av betydning for hvordan ansatte forstår og arbeider med informasjonssikkerhet. Arbeidsnormer kan også påvirke hvordan ansatte i finansnæringen forholder seg til informasjonssikkerhet. Blant annet ved hvordan kolleger følger rutiner og regler, samt organisasjonens kulturelle forventning til fenomenet (Guo, Yuan, Archer & Connelly, 2011; Da Veiga & Martins 2015). Dersom organisasjoner skal forstå viktigheten med sikkerhetskultur, og påse at den ikke svikter, er de ansatte avhengig av å bli bevisstgjort på dens relevans og viktighet. Dette kan gjøres gjennom kommunikasjon, og det er ulike måter å gjøre dette på:

- Bevisstgjørelse - gir forståelse for hva som må beskyttes.
- Trening – Tilfører kunnskap om hvordan sikkerheten kan oppnås.
- Undervisning – Tilfører en dypere forståelse om hvorfor sikkerhet er påkrevd.

Det er lite sannsynlig at alle ansatte vil ha behov for den samme kunnskapen. Trening benyttes for å oppnå samme kunnskap, men krav til utdannelse vil likevel være begrenset til personalet som arbeider spesifikt med sikkerhet (Furnell & Clarke, 2005). Med dette ser man at krav til utdannelse innen sikkerhet vil være begrenset til de som jobber med informasjonssikkerhet i

banknæringen. Dermed vil informasjonssikkerhetslederne ha en annen forståelse enn de andre ansatte i virksomheten. Likevel kan trening benyttes for å øke forståelsen og kunnskapen hos de andre ansatte. En viktig faktor for sikkerheten er menneskene som jobber i virksomheten, da det er de som behandler informasjon. Dermed er det valgt å fokusere på menneskelige feilhandlinger, og hvorfor de oppstår. Dette henger sammen med de organisatoriske normene.

Menneskelig svikt

Det er flere teoretikere som trekker frem menneskelig svikt som årsaksforklaring for hvorfor uønskede hendelser finner sted i avanserte teknologiske systemer (Engen et al., 2016). Dekker (2006) forklarer hvordan teorien med fokus på menneskelig svikt består av "*the old view"* og *"the new view"*. I *"the old view"* har man fokus på at mennesket er det svakeste leddet, og at ellers fungerende teknologiske systemer hadde fungert utmerket, dersom enkeltpersoner ikke begikk feil. Dette er en svært mye anvendt teori da den er enkel å benytte for å finne årsaken til hvorfor en hendelse fant sted, og med dette tilfredsstille interessenter. "*The new view"* ser derimot på de bakenforliggende årsakene til at uønskede hendelser finner sted, og mener at de henger sammen med organisasjonen som er berørt og dens organisasjon. Med dette kan man si at det nye synet viser til menneskelig feil som symptomer av problemer dypere i systemet. Slike problemer kommer av at en organisasjon ikke kun fokuserer på sikkerhet, og derfor forsøker å nå flere mål samtidig, som fortjeneste, service og tillit (Dekker, 2006). Med andre ord viser teorien til at hendelsene og feilene som begås, kommer av kompleksiteten på arbeidsplassen til den enkelte organisasjon. Menneskene i slike organisasjoner arbeider under press for å nå satte mål, samtidig som de utvikler strategier for at feil ikke skal oppstå. I tillegg kan mennesker fokusere på feil risiko. Fokus på feil område kan henge sammen med hva de blir fortalt om av ledelsen, om hvor hovedfokuset skal være, for eksempel effektivitet og inntjening (Dekker, 2006).

3.4.2 Sikkerhetskultur

Det finnes ikke en entydig definisjon av sikkerhetskultur i litteraturen. Reason (1997) definerer sikkerhetskulturen som et produktet av individuelle verdier og gruppeverdier, kompetanse, holdninger og handlingsmønster. En god sikkerhetskultur består av flere elementer som, rapporterende-, rettferdig- og lærende kultur. Disse tre elementene trenger kontinuerlig fokus for å sørge for at sikkerhetssystemene i finansnæringen ikke skal oppleve svikt. De nevnte elementene utgjør en informativ kultur, som sett i et organisatorisk perspektiv er en

sikkerhetskultur (Reason, 1997). For å oppnå en god risikostyringsprosess er rapporteringskulturen av betydning. En effektiv rapporteringskultur vil avhenge av hvordan en organisasjon håndterer uønskede hendelser. Dersom organisasjonen innehar en rettferdig kultur, vil det skape en atmosfære der de ansatte oppfordres og belønnes, for å gi essensiell sikkerhetsrelatert informasjon. Videre er tillit et viktig fenomen innen organisasjonskulturen, for å hindre selektiv rapportering. Det er også viktig å ha et tydelig skille mellom akseptabel og ikke-akseptabel oppførsel for å opprettholde troverdighet hos de ansatte (Reason, 1997).

Et viktig aspekt i sikkerhetskulturen er læring (Reason, 1997). En lærende kultur er villig og kompetent til å trekke rette konklusjoner fra dens sikkerhetsinformasjonssystemer. Det vil si at man samler inn, analyserer og formidler informasjon fra hendelser. Elementer som er relevante for å oppnå god læring er observering, reflektering og handling. Det vil også være viktig å kunne implementere store reformer ved behov for å forbedre sikkerheten. Dette er en prosess basert på kollektiv læring, som igjen er vesentlig for å oppnå en god sikkerhetskultur (Reason, 1997).

Informasjonssikkerhetskultur

Begrepet informasjonssikkerhetskultur kommer av den menneskelige faktoren i studier relatert til informasjonssikkerhetsstyring (Soomro, Shah & Ahmed, 2016; Tsohou, Karyda & Kokolakis & Kiountouzis, 2015; Yildirim, Akalp, Aytac & Bayram, 2011). Klassifiseringen *informasjonssikkerhetskultur*, er valgt å benyttes da det er dette fenomenet som adresseres innen banknæringen. Informasjonssikkerhetskultur er et system med felles mønstre eller tro, når det gjelder informasjonssikkerhet, som holdes av medlemmer i en organisasjon (Snyman & Kruger, 2017).

Tidligere forskning på informasjonssikkerhet viser at mennesker er det svakeste leddet i den skjøre informasjonssikkerhetskjeden. Innflytelsen av informasjonssikkerhetskulturen fortsetter å ha en vidtgående innvirkning på datasystemets sikkerhet og integritet, på grunn av de iboende mangler som mennesker utviser når de sammenlignes med tekniske barrierer. Folk kan lett påvirkes av omstendigheter, og de kan avsløre informasjon grunnet uvitenhet eller som utro tjenere. Dette kan ha en negativ innvirkning på sikkerheten og integriteten til systemene de kommuniserer med innen finansnæringen (Snyman & Kruger, 2017).

Sikkerhetsbevissthetsprogrammer

En måte å håndtere manglene på, er å sikre at sikkerhetsbevissthetsprogrammer blir implementert i organisasjonene. Sikkerhetsbevissthetsprogrammer er ulike tiltak som virksomheten kan iverksette for å bevisstgjøre de ansatte om ønsket atferd. Med dette kan slike programmer blant annet være e-læring, øvelser og opplæring. Formålet med slike programmer er å utdanne og instruere medlemmene i en organisasjon. Dette gjøres ved å stille dem spørsmål angående informasjonssikkerhet i lys av det som er undervist. Deretter søker man å påvirke deres oppførsel og informasjonssikkerhetskulturen på en positiv måte (Tsohou et al., 2015). Sikkerhetsbevissthetsprogrammer kan være et godt verktøy som fremmer god adferd når det gjelder informasjonssikkerhet. Programmene bør tilpasses den enkelte organisasjon, for å sikre at programmene lykkes (Snyman & Kruger, 2017). Dette gjøres ved å analysere oppførselen i den enkelte organisasjon. Ved å anvende ulike atferdsmodeller, som bidrar med å bestemme årsaken til at det enkelte individet, og gruppen i sin helhet oppfører seg på en bestemt måte (Tsohou et al., 2015).

Sikkerhetsbevissthetsprogrammer spiller en viktig rolle i styringen av informasjonssikkerhetskulturen i en organisasjon (Tsohou et al., 2015). Disse programmene formidler informasjon om sikkerhetspolitikk og mulige sikkerhetstrusler i en organisasjon, og tjener som en mekanisme for å utdanne personalet innen banknæringen. I tillegg skaper de bevissthet om relevante sikkerhetsproblemer som organisasjonen står overfor. Det antas vanligvis at brukerne i en organisasjon utøver risikabel oppførsel når det gjelder sikkerhet fordi de ikke er klar over at deres oppførsel er risikabel. Selv om de er informert om det motsatte, er de ikke klar over de potensielle konsekvensene av deres handlinger.

Derfor bør sikkerhetsbevissthetsprogrammer fokusere på de relevante emnene, for å påvirke menneskelig atferd på en positiv måte. For vidt fokus på sikkerhet, utover det som er relevant for organisasjonen, kan føre til at de ansatte blir overbelastet med sikkerhetsinformasjon. Dette kan igjen føre til sikkerhetsutmattelse (Furnell & Thomson, 2009). For å forhindre dette bør virksomheten skreddersy innholdet i sikkerhetsbevissthetsprogrammer, noe som i tillegg vil kunne fremme effektiviteten av sikkerhetsbevissthetsprogrammene som er benyttet.

Det er retningslinjene og standardene som styrer utviklingen av sikkerhetsbevissthetsprogrammer. Likevel mislykkes de ofte fordi de ikke klarer å påvirke hvordan personalet danner ideer og meninger på et kognitivt nivå. Ved å ikke ta dette i

betraktning, blir personalet bare bombardert med informasjon gjennom sikkerhetsbevissthetsprogrammene, som medfører at de ikke påvirker deres adferd som ønsket (Tsohou et al., 2015).

3.5 Oppsummering

Teoriene belyser faktorer som kan påvirke hvordan man jobber mot å sikre informasjonssystemene, samt faktorer som påvirker de ansattes forståelse for informasjonssikkerhet og uønskede hendelser. Det er her valgt å fokusere på organisatoriske forhold som: kommunikasjon og inkludering, integrasjon og refleksjon, da dette faktorer som påvirker risikostyringsprosessen. Teorier om risikopersepsjon viser på sin side til ulike faktorer som påvirker menneskets forståelse av risiko, og dermed handlinger. Organisatoriske normer og sikkerhetskultur utgjør rammene for hvordan sikkerhetsarbeidet foregår i virksomhetene. Sammen utgjør disse teoriene og faktorene grunnlaget for den empiriske analysen som skal belyse hvordan de ansatte i banknæringen forstår og jobber for å sikre informasjon mot uønskede hendelser. Videre har forskningsspørsmålene lagt rammene for hvordan empirien er strukturert.

4. Forskningsdesign og metode

I dette kapittelet vil det redegjøres for valgt forskningsstrategi, metodisk tilnærming, samt en begrunnelse for valg og vurderinger som er tatt underveis. Problemstillingen og forskningsspørsmålene har lagt føringer for fremgangsmåten.

4.1 Forskningsdesign

I følge Thagaard (2013) handler forskningsdesign om retningslinjene for hvordan forskningen skal foregå. Med dette ble det laget en prosjektskisse med tilhørende plan for delmål i forkant av prosjektet. Målet med studien var å oppnå en forståelse for hvordan banknæringen forstår trusler mot deres informasjonssystemer, og hvilke faktorer som påvirker deres arbeid med å beskytte informasjon. Det er flere måter å tilnærme seg problemstillingen på, der det i denne sammenheng valgt å fokusere på teorier som blant annet belyser aspekter som risiko og sårbarhet, risikostyring, risikopersepsjon og organisatoriske normer.

Forskningsstrategier angir en logikk for hvordan forskningen bør legges opp, og danner et grunnlag for hvilke konklusjoner man kan trekke (Blaikie, 2010). På bakgrunn av problemstillingens hensikt er det valgt å benytte en abduktiv tilnærming. Dette er fordi det er tatt utgangspunkt i teorier som la grunnlaget for en foreløpig intervjuguide, men senere i studieforløpet er disse teoriene endret på bakgrunn av interessante funn. Problemstillingen er også blitt endret underveis, og oppgaven er formet etterhvert som studien har utviklet seg.

4.2 Metodisk tilnærming

Casestudier egner seg godt når man skal undersøke samspillet mellom en spesifikk kontekst og individets forståelse av et fenomen (Jacobsen, 2010), som er tilfellet i denne oppgaven. En slik studie er også nyttig i kombinasjon med abduktiv forskningsstrategi, der resultatene blir vurdert som en helhet for å undersøke årsaksforklaringer (Yin, 2014).

Formålet med studien er å belyse hvordan banknæringen jobber med å sikre informasjon, og hvordan de ansatte forstår informasjonssikkerhet. I vårt tilfelle er caset de ansattes "risikoforståelse i banknæringen". Det er valgt å benytte en abduktiv tilnærming siden forskningen vår er av iterativ karakter. Dette innebærer at vi startet med en idé om hva som skulle forskes på, samt hvilke teorier som skulle benyttes, og startet deretter arbeidet med en tentativ problemstilling. I løpet av forskningsprosessen har det vært behov for å endre

problemstillingen, noe som også har ført til endringer av innholdet i teorikapittelet. Ved å benytte denne metoden fremfor en spørreundersøkelse har det vært mulig å få en dypere forståelse av fenomenene som undersøkes. Dette er fordi man i en intervjusituasjon har muligheten til å stille oppfølgingsspørsmål.

4.2.1 Dokumenter

For å kartlegge aktuelle dokumenter ble internett hovedsakelig benyttet. Det ble benyttet ulike søkeord som *"Risk management", "Sårbarheter og risikoer i banknæringen"*, og *"Informasjonssikkerhet i banknæringen".* Dokumentene som er benyttet, er referert til som *"faglig ekspertkunnskap"*. Det er blitt søkt etter relevant informasjon om hvilke risikoer banknæringen er utsatt for, utfordringer med nye regulatoriske krav, samt hvilke faktorer faglige ekspertene anser som nødvendige for å håndtere disse. Det er i denne sammenheng valgt å benytte følgende dokumenter:

Utgiver	***Årstall***	***Dokumentnavn***
Norges Bank	*2017*	*Finansiell infrastruktur*
NOU	*2015*	*Digital sårbarhet - sikkert samfunn*
NSM	*2015*	*Helhetlig IKT-Risikobilde*
NSM	*2017*	*Risiko og sårbarheter i ny tid*

Tabell 1: Oversikt over dokumenter

Dokumentene i tabell 1, har blitt valgt ut fordi de tar for seg flere av de temaene som berører denne studien, som er banknæringen og de risikoene den er utsatt for, IKT-sikkerhet og sårbarhet tilknyttet bankens infrastruktur og digitalisering. Sammen utgjør dokumentene et helhetlig risikobilde av informasjonssikkerhet i banknæringen.

4.2.2 Valg av informanter

Prosessen med å innhente informanter startet tidlig, da vi var forberedt på at dette kunne være en tidkrevende prosess. Prosessen startet med innhentingen av informanter ved å sende ut e-

post med forespørsel om informanter til flere ulike banker, samt bekjente som satte oss i kontakt med aktuelle kandidater. Etter å ha fått kontakt med noen få informanter, ble snøballmetoden benyttet, som har satt oss i kontakt med flere informanter, ved å ha latt «ballen rulle» til neste kontakt. Dette har vært en tidkrevende prosess, da man legger beslag på arbeidstiden til informantene, som ikke var aktuelt for alle som ble kontaktet. I utgangspunktet var ønsket å innhente en jevn alders- og kjønnsfordeling, siden dette er faktorer som kan påvirke resultatet, men oppdaget raskt at det i større grad var mannlige informanter blant dem som er ansatt i en høyere stilling. Til slutt ble 13 informanter intervjuet fra fire ulike bankfilialer, som er presentert i *tabell 2*, som gir en oversikt over informantene og deres rolle i banken. Utover dette var det et ønske om å styrke forståelsen av hvordan banknæringen forstår risikoen for cyberangrep på deres informasjonssystemer og hvordan de arbeider med dette ved å intervjue representanter fra FinansCert, Datatilsynet og Finanstilsynet. Dessverre var det en manglende respons fra disse organisasjonene, og grunnet begrenset med tid så vi oss nødt til å se bort ifra informanter på dette nivået.

Det er flere faktorer som har lagt føringer for et strategisk utvalg av informanter. Formålet og avgrensing av oppgaven er medvirkende i utvelgelsen (Johannessen, Christoffersen & Tufte 2011). På bakgrunn av dette har informanter som arbeider direkte med informasjonssikkerhet i banknæringen, mellomledere og kunderådgivere blitt inkludert. Dette utvalget kan bistå oss i å undersøke likheter og forskjeller blant de ulike nivåene, i forbindelse med hvordan de vurderer informasjonssikkerhet og hvilke risikoer de adresserer som mest vesentlige. Det har også bidratt til å kunne vurdere hvordan de ulike gruppene forholder seg til endringer i lovverket som påvirker banknæringen.

Informant	***Rolle***	***Bank***
Informant A	*Informasjonssikkerhetsleder*	*Bank A*
Informant B	*Informasjonssikkerhetsleder*	*Bank B*
Informant C	*Informasjonssikkerhetsleder*	*Bank C*
Informant D	*Informasjonssikkerhetsleder*	*Bank D*

Informant A1	*Mellomleder*	*Bank A*
Informant B1	*Mellomleder*	*Bank B*
Informant C1	*Mellomleder*	*Bank C*
Informant D1	*Mellomleder*	*Bank D*
Informant A2	*Rådgiver*	*Bank A*
Informant A3	*Rådgiver*	*Bank A*
Informant B2	*Rådgiver*	*Bank B*
Informant C2	*Rådgiver*	*Bank D*
Informant D2	*Rådgiver*	*Bank D*

Tabell 2: Oversikt over informanter

4.2.3 Intervju

I utgangspunktet var det ønskelig å gjennomføre intervjuene ansikt til ansikt, men siden flere av informantene ikke var bosatt i Rogaland, ville dette bli en tids- og kostnadskrevende prosess. I tillegg ønsket flere av informantene i Rogaland å gjennomføre intervjuet per telefon, da det ofte krever mindre tid å gjennomføre. Med dette ble 8 av de 13 intervjuene gjennomført per telefon. Alle intervjuene ble tatt opp med diktafon, med informantenes godkjenning.

I forkant av intervjuene fikk informantene en beskrivelse av prosjektet i muntlig eller skriftlig form. I tillegg fikk informantene tilbudet om å få tilsendt intervjuguiden på forhånd. Årsaken til dette henger sammen med at banknæringen forvalter store mengder opplysninger. Ved å dele intervjuguiden med informantene på forhånd sikret man dem at dette ikke er informasjon man ønsket å innhente. Samtidig fikk de muligheten til å reservere seg mot å besvare spørsmål av sensitiv karakter. Å dele intervjuguiden på forhånd kan skape både fordeler og ulemper. På den ene siden kan man oppnå mer reflekterte svar, noe som opplevdes som tilfellet av dem som hadde gjort seg kjent med intervjuguiden på forhånd. Ulempen er derimot er at man ikke får

tak i de første reaksjonene og svarene. Intervjuguiden er tematisk bygd opp, men informantene fikk prate fritt uten å følge intervjuguiden slavisk. Med dette fungerte intervjuguiden som et godt hjelpemiddel eller "sjekkliste" for å sikre at alle de ulike temaene som var satt i forkant ble besvart. Under intervjuene hadde flere av informantene innspill for temaer som ikke hadde blitt reflektert over i forkant av intervjuet. En del av disse innspillene ble videreført til neste informant, da de ble ansett dem som aktuelle for å besvare problemstillingen.

4.3 Analyse

I denne studien er dokumentene i tabell 1, og informasjon innhentet fra informantene analysert hver for seg. Deretter er rådataene satt opp mot hverandre for sammenligning, for å søke en helhetlig forståelse og tolkning. Det ble først foretatt en analyse av dokumentene, der relevant informasjon ble hentet ut, og sortert etter fargekoding knyttet til temaene for oppgaven. Dette er fordi noen av dokumentene er omfattende, og tar for seg flere aspekter som ikke er relevante for problemstillingen. Dokumentene har blitt analysert i flere omganger etterhvert som studiet begynte og ta form. På denne måten er det søkt å unngå tunnelsyn, samtidig som det har bidratt til et mer reflektert syn.

Intervjuguiden var tematisk inndelt etter tema, noe som gjorde det mulig å samle all informasjon fra intervjuene i et dokument som var inndelt etter de samme temaene, etter at intervjuene var transkribert. I likhet med dokumentanalysen, ble det benyttet ulike fargekoder for å skille de ulike informantene. På denne måten fikk man en oversikt over hva de ulike informantene hadde sagt, og kunne sammenligne utsagnene opp mot hverandre. Deretter ble et tema tatt for seg om gangen, og det ble benyttet sitater som belyste våre funn. I tillegg ble dokumentene benyttet for å få en utdypende forståelse for hvordan informantene opplever ulike fenomener sammenlignet med de faglige ekspertene.

4.4 Studiens transparens og troverdighet

Når det kommer til kvalitative studier, handler det om å ivareta troverdigheten og pålideligheten av forskningen, og det er med dette foreslått at man benytter seg at kriteriene troverdighet, overførbarhet, pålitelighet og bekreftbarhet (Lincoln & Guba, 1985). Ved at vi er to studenter som skriver sammen har det vært mulig å undersøke fortolkningene opp mot hverandre, noe som anses som en styrke for oppgavens kvalitet.

Troverdighet

Troverdighet omhandler hvorvidt man har klart å presentere funnene på en riktig måte. For å sikre troverdighet har det gjennom hele prosessen vært åpnet for ulike tolkningsmuligheter. På denne måten kan nye og interessante fenomener vise seg (Lincoln & Guba, 1985). Refleksjonene og tankene i forbindelse med denne studien startet idet masteroppgaven ble påbegynt, og gjennom analysen har de hele tiden utviklet seg. Utenom informanter på ulike nivå innad i bankene, er det også benyttet ulike kilder siden analysen både omfatter informanter og dokumenter som belyser temaet. I teorien har det blitt sett etter ulike kilder til informasjon om de samme fenomenene, og dette har bidratt til ny forståelse av de ulike fenomenene som er omtalt i denne studien. Gjennom hele studieprosessen har det vært tett dialog med veileder, og andre medstudenter som er i samme situasjon som har bidratt til økt refleksjon hos oss som forskere. Besvarelsene, anvendte teorier og dokumenter er blitt sett tilbake på, som har bidratt til stadig bedre forståelse med hva informasjonssikkerhet i banknæringen innebærer. Gjennom åpne intervjuer var det mulig å stille oppfølgingsspørsmål, oppklare eventuelle uklarheter underveis, samt kontrollere fortolkninger hos informantene.

Overførbarhet

For å sikre transparens har funnene blitt tydeliggjort ved å vise til hva informantene forteller, og hvordan deres utsagn tolkes. Det er også benyttet tykke beskrivelser av ulike fenomener slik at leseren skal få økt forståelse (Lincoln & Guba, 1985). Gjennom metodekapittelet ble det søkt å gi leseren et innblikk i utviklingen av masteravhandlingen, hvordan fokus for oppgaven med tilhørende temaer og forskningsproblemer har utviklet seg gjennom prosjektet. Dette er for å gi leseren muligheten til å selv vurdere studien, og om konklusjonen kan forstås som troverdig og interessant, med hensyn til studien som er gjennomført og teoriene som er benyttet.

Pålitelighet

Pålitelighet omhandler hvorvidt funnene i forskningen er avhengig av våre interesser, teoretisk synspunkt og tidligere erfaring. I henhold til Lincoln og Guba (1985) er det viktig å se på forskningsprosessen i lys av avhengighetskriteriet. Således kan man som forskere være påvirket av våre jobber, der en av oss jobber mot informasjonssikkerhet og informasjon i en annen sektor. Dette er naturligvis noe som påvirker vårt syn på informasjonssikkerhet. Likevel er det gjennom intervjuene lagt vekt på hvordan informantene forstår og jobber mot informasjonssikkerhet, og det er blitt forsøkt å ikke la vår forståelse påvirke informantenes forståelse av fenomenet. Igjen er det fokusert på å ha et åpent syn i forhold til informantene, og latt de fortelle uten innblanding

fra oss. Forskningsområdet og problemstilling har naturligvis en sammenheng med våre interesser, og utgangspunktet for oppgaven var preget av dette.

Bekreftbarhet

Bekreftbarhet innebærer at man søker å basere funnene på reelle data, og ikke på forskerens personlige tolkning eller konstruksjon (Lincoln & Guba, 1985). I denne forskningen består store deler av empirien av transkriberte intervjuer som i seg selv vil være mulig å overføre, men med hensyn til konfidensialitet vil dette likevel ikke kunne gjøres. Samtidig har sitater blitt benyttet i empirien slik at andre får innsyn i den dataen som anses som viktigst for forskningen, og det vises til vår tolkning av disse utsagnene. Dermed vises det til det datagrunnlaget som er ansett som viktigst, og dermed opprettholder prinsippet om bekreftbarhet.

4.5 Etiske betraktninger

Under forskning ligger det et etisk ansvar hos oss som forskere der man søker å unngå at studiet gir negative konsekvenser for informantene ved å beskytte deres integritet (Thagaard, 2013), samt opprettholde konfidensialitet. Før intervjuprosessen startet, ble meldeplikttesten som NSD har gjort tilgjengelig på deres nettside utført for å vurdere om prosjektet er meldepliktig. Resultatet viser at prosjektet ikke er meldepliktig da det ikke inneholder personopplysninger som kan knyttes til informantene. Deretter er konfidensialitet blitt etterstrebet ved å anonymisere bedriftene informantene arbeider for, slik at det ikke skal være mulig å knytte stilling eller person til en bestemt bedrift. Under intervjuene ble det benyttet båndopptaker. Intervjuene ble transkribert så tidlig som mulig, slik at alle lydfiler kunne slettes fortløpende. Under transkribering av intervjuene har lojalitet overfor informanter blitt etterstrebet, ved å gjenspeile deres erfaringer og forståelse. Personlig informasjon ble utelatt for å bevare informantenes integritet og konfidensialitet, og ble ansett som unødvendig i lys av studiens formål.

I forkant av en intervjuundersøkelse er det hensiktsmessig å benytte seg av noen etiske spørsmål, da etiske utfordringer vil forekomme gjennom hele intervjuet som man må ta hensyn til helt frem til den endelige rapporten er ferdig (Brinkmann & Kvale, 2009). Som forskere har det blitt reflektert over vår rolle og innvirkning på informantene slik at dette ikke påfører dem negative konsekvenser, og med dette har informasjonen blitt gjengitt så korrekt som mulig. Samtlige

informanter fikk tilbud om lese oppgaven både før og etter innlevering, der flere var interessert i å lese den endelige oppgaven.

4.6 Styrker og svakheter

Fordelen med en kvalitativ studie er at man kan gjennomføre dybdeintervjuer, og stille oppfølgingsspørsmål slik at man får en dypere forståelse for hvordan banknæringen jobber mot og forstår informasjonssikkerhet. Ulempen er at man ikke får samme bredde i besvarelsen som man ville gjort ved en kvantitativ tilnærming siden man ikke får besvarelser fra like mange informanter. Det kan både være en svakhet og styrke for oppgaven at det er valgt ut fire ulike bankfilialer til å delta i vår studie. På den ene siden får man innsikt i hvordan informasjonssikkerhet håndteres i de ulike bankene, og man får reflektert over eventuelle likheter/ulikheter. Samtidig kan mange informanter og en sammenligning av virksomhetene bidra til at analysearbeidet blir mer omfattende, og med det redusere kvaliteten på empirien. Likevel anses kontakt med flere banker som en styrke for oppgaven, særlig med tanke på at det er blitt intervjuet tre eller fire informanter i hver bank.

5. Empiri

I denne delen vil funnene fra intervjuene i forbindelse med informasjonssikkerhet i banknæringen presenteres. Det vil gjøres rede for hvilke utfordringer banknæringen anser som reelle i forhold til informasjonssikkerhet, hvordan de jobber for å unngå uønskede hendelser, samt hvordan sikkerhetskultur og risikoforståelse spiller inn på dette arbeidet. Dette relateres direkte til problemstillingen:

Hvordan forstår og jobber banknæringen for å møte risikoen for uønskede hendelser i forbindelse med informasjonssikkerhet?

For å besvare problemstillingen er det benyttet informasjon innhentet fra de ulike informantene, som representerer ulike roller fra banknæringen, herunder informasjonssikkerhetsleder, mellomleder og kunderådgiver. Det er i tillegg supplert med informasjon innhentet fra dokumentene som er presentert i (tabell 1). Kapittelet er strukturert etter forskningsspørsmålene, men vil likevel gli litt inn i hverandre, da det ikke er et tydelig skille mellom funnene.

5.1 Hvilke faktorer påvirker risikostyring i banknæringen, og hva påvirker de ansattes forståelse av risiko og sårbarheter?

For å besvare forskningsspørsmål *(i)* er det fokusert på hvordan de ulike informantene forholder seg til risiko og sårbarheter, risikostyring, og hvordan de ulike informantene forstår informasjonssikkerhet. I forbindelse med risikostyringen er det særlig tre områder som er vektlagt, herunder kommunikasjon, inkludering og integrering, da dette er organisatoriske faktorer som kan ha en innvirkning på hvordan banknæringen sikrer informasjonssystemene sine.

I forbindelse med IKT-sikkerhet er det flere utfordringer som kan oppstå. NSM (2015) fremhever blant annet at digitale tjenester må være pålitelige, troverdige og tilgjengelige, samtidig som de må være robuste overfor uønskede hendelser. Det er også en utfordring at automatisert saksbehandling og vedtak krever en høy grad av innebygd sikkerhet med sporbarhet og pålitelige digitale krav. Digitaliseringen medfører høye krav til risikostyring og sikkerhetskompetanse. Samtidig som økt teknologiavhengighet krever en robust digital infrastruktur, og en felles risikoforståelse på tvers av hele leveransekjeden (NSM, 2015).

5.1.1 Risikostyring i banknæringen

Risikostyring går ut på å identifisere, vurdere og håndtere risikoene som en virksomhet er utsatt for, samt følge opp risikoene og påse at de er under et akseptert nivå. Risikostyring er knyttet til ressursbruk, der målet er å finne en balanse mellom mål, risiko og tiltak. I tillegg til hvilke kostnader og tap en eventuell uønsket hendelse vil kunne påføre organisasjonen samt samfunnet (DSB, 2012). Banknæringen er pålagt å gjennomføre risikoanalyser, og en god operasjonell risikostyring er nødvendig for å forstå hvilke risikoer virksomheten er utsatt for (NOU 2015:13). I en rapport fra NSM (2015) konkluderer de med at det er stor risiko knyttet til bruk av IKT, og at alle er et mål for IKT-angrep. Dette viser til viktigheten av å jobbe systematisk med det digitale risikobildet. En utfordring for sikkerhetsarbeidet er mangelfull planlegging og styring av sikkerhetsarbeidet, noe som er grunnleggende for å gjennomføre sikringstiltak. Det er også indikasjoner på at sårbarhetsreduserende tiltak ikke samsvarer med utviklingen i trusselbildet (NSM, 2017).

Samtlige informasjonssikkerhetslederne forteller at banken forholder seg til ISO-standarden 27000 når det gjelder risiko- og sårbarhetsanalyser. Informant A påpeker at standardene i seg selv ikke er tilstrekkelige og må tilpasses den enkelte organisasjon: "*Så det er jo klart, du kan jo ikke bare ta det som er publisert og bruke det blindt, det er jo noe som må være tilpasset organisasjonen."* Informant D sier at de utover ISO 27000 bruker interne krav etablert i banken som rutiner og regler, som skal påse at det ikke forekommer brudd i forhold til risikostyringen i banken. En annen informant forteller at de benytter ISO-standarden, men at de også benytter etiske retningslinjer som er med på å underbygge dette arbeidet. Med dette ser man at de fleste informantene viser til ISO 27000 som utgangspunkt for deres sikkerhetsarbeid, men at denne tilpasses den enkelte virksomhet.

Informantene forteller også at risikostyring er et kontinuerlig prosess, og at de gjennomfører risiko- og sårbarhetsanalyser flere ganger i løpet av året for å se om det er endringer som de ikke er bevisste over. I tillegg er det en av informantene som sier at de har en årlig gjennomgang av systemene som er klassifisert som kritiske. Videre forteller informanten at dette utgjør en lang liste, der de analyserer de ulike risikoene tilført systemene, og at de arbeider systematisk med risikoer og sårbarheter ved å benytte en kvantitativ tilnærming. I tillegg sier informantene at de benytter en tredjepart som gjennomfører ROS-analyser av applikasjoner som bankene benytter seg av.

Inkludering og kommunikasjon

Når kommer til hvem som inkluderes i selve risikostyringen, og utarbeidelsen av ROS-analyser forteller informantene at dette er avhengig av hendelsens omfang. *"For små hendelser er det leder/eier av berørt område som tar ansvar. Er hendelsen stor er det hele beredskapsgruppen som er med. For de største hendelsene er det bankens kriseledelse som deltar i risikostyringen"* (Informant D). I likhet med informant D forteller også de andre informasjonssikkerhetslederne at det er hendelsens størrelse som avgjør hvem som inkluderes i ROS-analysene dersom uønskede hendelser inntreffer. Med dette ser man at informasjonssikkerhetslederne henviser til inkludering ved håndtering av hendelse, men det er ingen som sier noe om at mellomledere og rådgivere er inkludert i det forebyggende arbeidet. Dette kan man forstå slik at informasjonssikkerhetslederne har en noe reaktiv forståelse av inkludering.

Informasjonssikkerhetslederne opplyser at de forventer og pålegger samtlige ansatte i bankene å gjennomføre ulike e-moduler. Med dette forstås disse modulene som et ledd i risikostyringen, da de skal bidra til at ansatte i banknæringen oppnår en felles forståelse av blant annet regler, rutiner og endringer. Dette kan hjelpe informasjonssikkerhetslederne til å påse at alle ansatte i banken blir inkludert i risikostyringen. Ut ifra hva informasjonssikkerhetslederne forteller, forstås det slik at andre avdelinger under dem, som mellomledere og rådgivere blir informert i etterkant av en hendelse, og ikke når den pågår, slik at alle skal få den samme forståelsen av hvilke tiltak som ble innført for å håndtere den aktuelle risikoen. For å formidle dette brukes det flere hjelpemidler: *"Vi har jo interne systemer, intranett som vi legger ut hendelser på som alle ansatte skal lese [...] Det er forskjellige måter å formidle budskapet på, og ofte så bruker vi lederne i banken som jevnlig har møter med de ansatte der vi ber lederen ta opp dette på neste møte"* (informant B).

De fleste informasjonssikkerhetslederne forteller at de likevel opplever avvik fra det som er ønskelig situasjon. Her forteller blant annet informant B at grunnet fokus på kundetilfredshet har de til tider for lite fokus på å opplyse sine egne ansatte om hva som har skjedd. Dette henger sammen med at de ønsker å opprettholde tilliten fra kundene i slike situasjoner. Samtidig opplyser informant C at grunnet fokus på deres hovedområde som er bank og finans, er informanten usikker på om alle avdelinger får samme forståelse av hva de søker å formidle via intranett, e-moduler og andre verktøy. Ut i fra opplysningene gitt av

informasjonssikkerhetslederne oppfattes det som at det er stort fokus på å spre budskapet om hva som har skjedd i bankene i etterkant av en hendelse, fremfor når den faktisk pågår.

Mellomlederne sin respons på hvorvidt de blir inkludert og hvordan risikostyringsprosessen blir kommunisert er ulik i de forskjellige bankene, dette på tross av at flere av de intervjuede bankene har samme avdeling som håndterer risikostyring. Informant D1 forteller at de ikke blir inkludert i risikostyringsprosessen, og påpeker at de er mer informert i etterkant av en hendelse. Informant A1 på sin side forteller at de blir inkludert i risikostyringen ved å besvare en spørreundersøkelse et par ganger i året som omhandler temaer som berører risikostyring, i tillegg til at de får en aktiv rolle dersom en uønsket hendelse finner sted. Ut ifra det informant A1 forteller, kan man tolke det som at i bank A blir mellomlederne inkludert ved at de er med på å skape et risikobilde av hvilke trusler som er aktuelle. I henhold til informant B1 blir mellomlederne i bank B inkludert i ROS-analysene gjennom kommunikasjon med bankens avdeling, men utdyper ikke dette ytterligere. I likhet med mellomlederne forteller rådgiverne at de i liten grad inkludert i risikostyringen, utover de nevnte e-læringsmodulene og informasjon formidlet via intranett. Når man vurderer de fire bankene sammen i forhold til inkludering innen risikostyring på et mellomleder- og rådgivernivå, kan man her forstå det slik at halvparten av bankene inkluderer mellomlederne i denne prosessen. Det er likevel noe vagt i hvilken grad dette foregår, mens de to andre bankene ikke har noen tilknytning til risikostyringsprosessen, da dette er forbeholdt et høyere nivå. Et viktig aspekt ved risikostyringen er hvordan de ulike informantene forstår informasjonssikkerhet, og hva de legger i begrepet, da forståelsen av informasjonssikkerhet har innvirkning på hvordan man jobber for å sikre informasjon.

Det er store forskjeller i hvilke risikoer og sårbarheter de ulike informantene trekker frem. I de neste avsnittene vil de risikoene og sårbarhetene som fremstår som mest bekymringsverdig blant informantene og faglige ekspertene bli presentert. Dette er fordi det er faktorer som har en innvirkning på hvordan de ansatte jobber mot å sikre informasjon, og det søkes å belyse hvordan bankene arbeider mot informasjonssikkerhet i banknæringen.

5.1.2 Nye krav kan medføre økt risiko for banknæringen

I løpet av 2018 er det to nye regelverk som skal innføres, og som vil berøre banknæringen. PSD2 er et av de nye regelverkene som skal innføres innen banknæringen i Norge, og som vil medføre en del endringer for hvordan bankene opererer. GDPR er en ny forordning som skal styrke personvernet i EU/EØS og implementeres også i Norge. Formålet med det nye lovkravet

GDPR er å sikre at alle kan være trygge på at personopplysningene behandles på en sikker og riktig måte, og at enkeltpersoner kjenner til hvilke rettigheter de har (Datatilsynet, 2016).

Sikkerheten til banktjenestene kan bli påvirket av nye aktører og ny teknologi. På den ene siden skal ny teknologi gjøre det enklere og mer forutsigbart for sikrere betalinger, blant annet gjennom sikker autentisering. PSD2 stiller strenge krav til aktører som skal tilby betalingstjenester. Dette gjør de ved å stille krav til rutiner for betalingsautentisering, samt at aktørene må stille sikkerhet for å dekke eventuelle tap. Likevel kan nye aktører føre til enkelte utfordringer når det kommer til sikkerheten i betalingssystemet, ved at det blir flere aktører som det må føres tilsyn på. Samtidig kan sikkerheten bli utfordret hvis betalingstjenester tilbys til aktører utenfor Norge. Hvis denne aktøren da opplever teknisk svikt, kan konsekvensene få et større omfang for de norske bankene. Cyberkriminalitet er et av områdene som blir vurdert som utfordrende ved innføring av nye aktører og teknologi på det norske markedet. Dette henger sammen med at de nye kravene innebærer en omstrukturering av hvordan banknæring gjør bank på, og strengere bruk av personopplysninger som kan medføre både utfordringer og nye risikoer (Norges Bank, 2017).

To av våre informanter som arbeider direkte med informasjonssikkerhet, bekrefter at de uroer seg i forhold til de nye kravene, herunder PSD2 og GDPR, én av informantene stiller seg positiv til dem, og én har ikke noen formening om de nye kravene. Det som viser seg som mest fremtredende i dialog med informantene er at de uroer seg for at de må endre arbeidsrutinene sine, mot et ukjent område, som igjen kan utnyttes av organisert kriminalitet. Informantene frykter at trusselagenter vil vente på feil som åpner et vindu for å kunne bryte seg inn på deres systemer. Dette kan medføre enorme konsekvenser for deres kunder, samt banken sitt renommé. To av informantene påpeker at kravene ikke er fullstendige. For å være i stand til å sikre at kravene oppnår sin hensikt, og oppleves som fullstendige forteller informant B at det er nødvendig at banknæringen samarbeider om dette. Informant A mener at de nye kravene er noen av de største risikoene som banknæringen står overfor for øyeblikket: "*Sånn umiddelbart så er det jo det regulatoriske noe av det største som jeg ser i form av risiko for banknæringen."* Informant B som deler denne bekymringen sier at de nye kravene skaper nye utfordringer i forbindelse med sikkerheten.

Siden kravene innebærer mer deling av informasjon, samt strengere bruk av personopplysning opplever banknæringen utfordringer med motstridende krav. På den ene siden skal bankene i

lys av den nye personvernloven GDPR ikke lagre personopplysninger, mens på en annen siden er det pålagt å lagre opplysninger som kommer frem i bokføringsloven, for å kunne spore opp eventuelle lovbrudd og kriminelle handlinger. Dette er noe som byr på utfordringer i forhold til hvordan de kan tilfredsstille begge kravene, siden de er så motstridende. *"Portabilitet og retten til å bli glemt, og da er det jo for eksempel retten til å bli glemt så har vi jo andre regulatoriske krav som gjør at de ikke kan bli glemt, vi har bokføringsloven og flere andre lover som gjør at vi må ta vare på data"* (informant B). Andre utfordringer som utheves, knyttet til GDPR, er at det ikke er helt klare retningslinjer for hvordan det skal gjennomføres. Dette er også noe informant B tar opp som en utfordring, *"Spesielt dette med hvem har ansvar når noe går galt, samt at vi må åpne opp løsninger for nye tredjeparter som våre kunder ønsker å benytte seg av så er ikke ansvaret plassert tydelig enda, så det mangler jo litt i dette regelverket då."*

Blant mellomlederne oppleves ikke de nye regelverkene som en like stor risiko, sammenlignet med informasjonssikkerhetslederne. Likevel er det en av informantene som uttrykker en bekymring knyttet til PSD2: "*Så det er jo mer det, hvordan blir det med PSD2 og dette med å dele alt av informasjon når alt er åpnere."* Ut i fra dette ser man at informanten er bekymret for faktumet at banken skal dele informasjon om kundene med andre aktører. I tillegg nevner informanten at systemene vil være åpnere. Med dette kan man tolke at informanten er bekymret for at systemene kan få flere svakheter ved at det blir enklere for kriminelle å stjele informasjon.

Rådgiverne på sin side har ikke like mye kunnskap om de nye regelverkene som er og skal innføres, PSD2 og GDPR, sammenlignet med informasjonssikkerhetslederne og mellomlederne. Likevel er de fleste av informantene kjent med de nye regelverkene, selv om de ikke er kjent med hele omfanget. En av informantene sier: "*Spennende, men er en del risiko rundt dette. Viktig at ting blir gjort i rett rekkefølge, og at alt er klart, og at man ikke lanserer før man er klar, slik at dette er idiotsikkert. Så må vi jo huske at det er ikke sikkert kunden vet hva den går med på å godtar"* (Informant D2). Videre trekker informanten frem både risikoer og muligheter med de nye regelverkene. Av risikoer knyttet til regelverkene nevner informanten blant annet: *"[...] og så tenker jeg på id-tyveri og hacking, på hvordan andre kan få tak i en kundes informasjon når den deler denne informasjonen på tvers av ulike banker og andre operatører. Det er da viktig at dette ikke blir for enkelt, dette tenker jeg kan være en risiko."* I tillegg påpeker informanten utfordringer knyttet til kundevilkår, der kunden godtar vilkårene uten å ha lest hva de går ut på. Dette kan igjen få følger for kunden, i og med at banken skal dele opplysninger med andre aktører.

5.1.3 Konkurranse og tidspress åpner opp for mulige sikkerhetsbrudd på informasjonssikkerhetssystemene

I henhold til NSM (2017) kan manglende fokus på sikkerhet føre til tap av kontrakter og eventuelt teknologisk forsprang. Banknæringen lever i stor grad av kunder som benytter deres tjenester på digitale plattformer. Finansforetakene har benyttet digitaliseringen til å effektivisere interne prosesser, og ligger i forkant i bruk av IKT for håndtering av kundedimensjonen, som har medført komplekse informasjonssystemer og verdikjeder. Dette gjør banknæringen sårbar for tilsiktede og utilsiktede hendelser (NOU 2015:13). Dette bekreftes av informant D som sier: *"Risikoer som er relevante er at vi beveger oss for raskt og ikke klarer å henge med".* Dagens digitale systemer er fortsatt umodne, og preges av rask utvikling som skaper rom for at uvedkommende får innsyn i informasjon. De faglige ekspertene legger stor vekt på utfordringer i forbindelse med ny teknologi og nye tjenester på markedet. Dette fokuset kan føre til at brukervennlighet og "*time to market"* går foran sikkerhet og operasjonell stabilitet, og kan være med på å skape nye sårbarheter (NOU 2015:13). Informant D påpeker dette som en vesentlig faktor for uønskede hendelser, og henviser til en hendelse basert på et slikt tilfelle i deres bank kun noen få måneder tilbake.

> *[…] og så gikk tiden litt fra oss, arbeidet var noe større enn det vi hadde tenkt, og vi rakk rett og slett ikke å teste alt, før lanseringsdagen. Vi valgte da å lansere appen før all testing var gjennomført. Så viser det seg at ila 1-2 dager, så er det en såkalt security researcher som har funnet en feil,* (informant D).

Med dette kan man forstå det slik at informanten mener banknæringen er utsatt for konkurranse og tidspress ved utvikling av digitale tjenester rettet mot kundene, der det i stor grad handler om å være først ut på markedet for å skape et konkurransefortrinn. Løsninger for raskere betalinger for personkunder er en voksende trend. Dette gir personkunder i ulike banker muligheten til å gjennomføre raske betalinger til hverandre. Samtidig er ikke de norske systemene egnet til denne teknologien, som kan føre til nye sårbarheter og risikoer (Norges Bank, 2017). Dette er også utfordringer som flere av informantene viser til. Én informant utdyper blant annet at de har hatt utfordringer i forbindelse med drift av nettbanken som driftes av underleverandører: *"Vi har jo hatt hendelser som har gått på det driftsmessige"* (informant A). Dette er også noe som informant C bygger opp under når det gjelder utfordringer knyttet til automatisering og digitalisering. Andre utfordringer som banknæringen møter i forbindelse

med sikring av informasjon er i forbindelse med menneskelige feil, bruk av skytjenester og organisert kriminalitet.

5.1.4 Banknæringen, et mål for cyberangerp?

På grunn av økende organisert kriminalitet rettet mot banknæringens distribusjonskanaler, mobile løsninger og løsninger knyttet til brukersteder, er det et kontinuerlig behov for å arbeide med å sikre god informasjonssikkerhet (NOU 2015:13). Mengden cyberangrep stiger, samtidig som metodene trusselagentene anvender blir stadig mer sofistikerte. Tjenestenektangrep og kjente datavirus observeres svært ofte i motsetning til sofistikerte angripere som skjuler sporene sine, som igjen vil være vanskeligere å oppdage samt forutse (Norges Bank, 2017, NOU 2015:13). Informant D sin uttalelse bekrefter denne frykten som også fagekspertene fremhever. Organisert kriminalitet rettet mot banknæringen kan føre til finansielle og materielle tap, og de samfunnsmessige konsekvensene kan bli store. Informant C er også bekymret for intenderte angrep på deres systemer.

Informant B forteller at risikoene som er relevante for banknæringen beveger seg fra menneskelige feil utført internt i banken til intenderte angrep på deres løsninger. Grunnet stor pågang innen digital pengetransaksjon og mer sofistikerte metoder innen det kriminelle miljøet, har trusselagentene i større grad mulighet til å følge pengestrømmen på nettet. En metode som anses som svært mye brukt innen banknæringen er phishing. Gjennom e-poster som inneholder link til ondsinnede nettsider, som tilsynelatende kommer fra velkjente virksomheter utnytter trusselagentene brukernes tillit til systemer, applikasjoner, menneskene og virksomheten de kjenner (NOU 2015:13; NSM, 2015). Med andre ord utnyttes tilliten som kundene viser til en virksomhet, som banken i dette tilfellet. Det er også en utfordring at trusselagenter lanserer applikasjoner med skadevare som utnytter brukerne. I henhold til Cisco kan man ikke stole på noen ting i cyberverdenen (NSM, 2015).

Informant B og D viser også til at phishing er en svært vanlig metode for å stjele kundenes penger. Både informant B og C bekrefter at trusselagenter har forsøkt å lure deres kunder å utgi opplysninger som gir kriminelle tilgang til deres kontodetaljer. Dette er utfordringer som kan være kritiske for en bank: *"det at vi behandler kundedata på en god og trygg måte er veldig viktig for oss hvis vi skal overleve i denne bransjen"* (informant B).

I likhet med noen av informasjonssikkerhetslederne er to av mellomlederne også bekymret for hacking:

> *Det er jo hacking, det er det digitale. Både systemet vårt kan hackes, kunder kan hacke andre kunder, e-post som sendes til oss der noen andre utgir seg for å være kunde, og ønsker overføringer gjort til ulike banker. Det er den elektroniske kriminaliteten som er farlig. Det er det jeg ser som risikobildet,* (Informant C1).

Informant B1 trekker også frem hacking som en av de største risikoene for banknæringen, selv om informanten tror det er lite sannsynlighet for det. Med dette vises det til at det er en bekymring blant noen av mellomlederne for eksterne trusler. En annen mellomleder er derimot ikke bekymret for digitale angrep:

> *Jeg må jo innrømme at jeg personlig ikke er veldig bekymret for hacking fordi at jeg føler og opplever at vi har veldig gode systemer som fanger det opp. Men jeg vil jo tro at de som jobber tettere med det enn hva jeg gjør er mer bekymret eller ser mer hva som kunne truffet oss, og som ikke traff oss. Vi hører mer om det som har skjedd, eller forsøk mot våre systemer som kunne vært en krise,* (Informant D1).

Her ser man at informanten har tillit til systemene som gjør at informanten ikke er bekymret for hacking. Dette kan henge sammen med at informanten sier at de ikke er direkte involvert i utarbeidelse av ROS-analyser og andre verktøy som skal beskytte bankene fra å bli utsatt for kriminelle handlinger. Informantene fremhever to motstridende tankesett da informant D1 på sin side er ikke bekymret for utenforstående angrep, mens informant B1 og C1 mener det er hacking som er den største risikoen for banknæringen. Tre av informantene trekker frem menneskelige feilhandlinger som en av de største risikoene som banknæringen står overfor, og som hovedårsak til at informasjon kommer på avveie. Informantene fremhever spesielt feil bruk av e-post, der eksempelvis personopplysninger sendes til feil kunde som årsak.

Samtlige rådgiverne trekker også frem risikoer knyttet til intenderte handlinger på de digitale plattformene. "*Det er jo svindel, det er økende, hacking, phishing, e-mail på avveie. I stedet for bankran er det at man blir lurt. Jeg har selv ikke opplevd phishing, men vet at det er andre som er utsatt for identitetstyveri, faktisk ganske nylig"* (Informant B2). Det er spesielt hacking i form av phishing rådgiverne er bekymret for, og da spesielt angrep rettet mot kundene:

Informant D2 sier: "*Hacking, virusangrep trojaner, hva kundene går på selv – går de på en mail og tror at det er oss."* Her uttrykker informanten en bekymring for kundene, og at de utsettes for hacking. Videre belyser en av informantene utfordringen bankene har med å sikre informasjon:

> *Banken blir jo lurt daglig, sannsynligvis, med e-post spam til kunder. Kunder tror det er banken som har sendt ut, og trykker videre og gir ut sensitive opplysning for eksempel kortnummer og det er jo jevnt og trutt angrep mot datasystemene i banken, blant annet nettbank* (Informant C2).

5.1.5 Mennesket er det svakeste leddet

Mange kjenner til uttrykket "*mennesket er det svakeste leddet"*, og selv om det ikke er intensjonen, blir det begått feil av mennesker, som kan føre til alvorlige hendelser (NOU 2015:13). Mennesker er sårbare og en av sårbarhetene til mennesker er evnen til å la seg lure. Noe som utnyttes av trusselagenter gjennom sosial manipulasjon, der ansatte lures til å gi fra seg passord, beskrive vedlikeholds- og sikkerhetsrutiner eller benytte minnepinner som er infiserte (NSM, 2015). Menneskelige feilhandlinger, svak ledelse og ubevissthet kan være en årsak til at bankene opplever svekket sikkerhet som kan føre til uønskede hendelser i forbindelse med IKT-systemene. Dette kan igjen føre til at dokumenter eller kundeopplysninger blir sendt til feil mottaker, som kan føre til store konsekvenser (NOU 2015:13). De fleste informantene har opplevd utfordringer knyttet til menneskelig feil, og adresserer dette med: *"I tillegg så har vi e-post som ansatte har tilgang til, og hva de sender via e-post til kunden, er jo en sårbar kanal"* (informant C*).* En annen informant belyser et annet eksempel der: "*En ansatt med en feil sender ut en kundeliste som inneholder informasjon som de ikke er autorisert for å se" (*Informant B). Informant A og informant B påpeker ytterlige risikoer knyttet til menneskelig svikt: *"[...] den største risikoen er den menneskelige faktoren [...] men så kan du jo si det at den største risikoen kommer rett og slett ved misbruk fra kunder og ansatte. Det er der du ser menneskelige feil"* (informant A).

Menneskelige feilhandlinger kan skyldes uforsiktighet eller uvitenhet (NOU, 2015:13). Menneskelige feil er noe også informant C nevner som relevant risiko for banknæringen: *"Så her kan jeg se for meg at vi kan rote til kundenummer eller navn, og at opplysningene da kommer til feil mottaker, og det er jo kritisk."* Informant C forteller videre *"Vi kan jo ha så mange barrierer vi vil, men til syvende og sist er det vi mennesker som må forholde oss til*

sikkerhetsrutiner. Dersom det blir slakk på det området, så vil ikke barrierene ha noen verdi." Med dette viser informanten til at man ikke kan beskytte seg 100% mot menneskelig svikt, da det kan forekomme brudd på rutiner og regler, som igjen kan føre til at uønskede hendelser oppstår. En annen utfordring er at mennesker ofte lar seg lure, noe som også NSM (2015) påpeker i sin rapport. NSM (2017) viser også til at mennesker kan svekke effekten av sikringstiltak som skal ivareta konfidensialitet, integritet og tilgjengelighet til informasjon, system, objekt og prosedyrer. Dette kan være på grunn lav motivasjon for å følge rutiner og retningslinjer, samt manglende kunnskap (NSM, 2015).

Mellomlederne henviser også menneskelige feilhandlinger som en utfordring når det gjelder svikt i informasjonssikkerhetssystemene. Informant C1 mener at menneskelig svikt er hovedårsaken til at informasjon kommer på avveie. Informant A1 og D1 påpeker at brudd på rutiner kan føre til at noen andre får tak i kundeinformasjon som de ikke skal, og at ansatte som sender kundeinformasjon til feil bruker er eksempler på slike hendelser. Rådgiverne på sin side anser ikke menneskelig svikt som en stor risiko for informasjonssikkerhetssystemene. De uttrykker at det er selvfølgelig noe som kan skje, "*[...] menneskelige feil skjer jo det og, men kanskje ikke så ofte",* (informant A3).

5.1.6 Hvordan forstår de ansatte i banknæringen informasjonssikkerhet?

Begrepet informasjonssikkerhet omhandler blant annet konfidensialitet, integritet og tilgjengelighet. Der konfidensialitet omhandler sikring av informasjon mot uvedkommende, og påse at kun autoriserte personer som har tilgang til denne informasjonen. I praksis er det ikke mulig å gjenopprette et brudd på konfidensialitet i det digitale rommet (NOU 2015:13). Under intervjuene ble alle informantene spurt om hva de legger i begrepet informasjonssikkerhet. Informant D forstår informasjonssikkerhet på følgende måte: "*Jeg tenker på alt det vi gjør for å sikre at informasjon i uansett form, at den er tilgjengelig for de den skal være tilgjengelig for, og at den inneholder korrekt informasjon."* Informant C på sin side mener at informasjonssikkerhet går ut på hvordan man forvalter systemet, hvordan man sikrer dette, og lagrer informasjon. Videre viser informant C til at informasjonssikkerhet er alt man gjør i forbindelse med tiltaksplaner, risikovurderinger og beredskapsplaner. Informant B på sin side refererer til definisjonen av informasjonssikkerhet. I likhet med informant B, sier informant A at begrepet går ut på følgende:

> *Det akademiske er den CIA-triangelen. Sånn som du ser at informasjonssikkerhet blir mer og mer viktig for hele samfunnet, fordi vi endrer måten vi, samfunnet er i endring på hvordan det faktisk fungerer. Sånn at hvis man ser på for eksempel informasjon som man stolte på før i tiden, det stoler vi mye mindre på nå.*

Dette tolkes som at informantenes forståelse av informasjonssikkerhet i stor grad baserer seg på den akademiske definisjonen av informasjonssikkerhet. Tre av informantene beskriver definisjonen slik de faglige ekspertene fremstiller den, mens informant C forteller mer hva begrepet inneholder.

I intervjuene med mellomlederne der de ble spurt om hva de legger i begrepet informasjonssikkerhet, fikk man et inntrykk av at de hadde en ulik oppfatning av begrepet. Det kommer frem i fra informant C1 at informasjonssikkerhet er relatert til den elektroniske kommunikasjonen, hva bankene blir eksponert av innen det digitale bildet, og at man må lære seg å være kritiske. Informantene gir ikke en klar definisjon av begrepet, men heller en beskrivelse av hvordan man bør være kritisk til tilgjengelig informasjon. Informant A1 forklarer at informasjonssikkerhet handler om tillit mellom banken og kundene, da bankene forvalter informasjon om dem i bankene som de forventer at banken skal påse at ikke kommer på avveie. En annen informant sier: *"Jeg tenker at vi må være bevisst den informasjonen vi besitter og at vi i det hele tatt må behandle det på en riktig måte"* (Informant D1), og trekker dermed frem bevissthet og riktig behandling av informasjon som viktige elementer innen informasjonssikkerhet. I tillegg trekkes elementer som rutiner og regelverk, samt en felles forståelse mellom de ansatte. Ut i fra intervjuene med mellomlederne i de fire bankene, ser man at det forekommer motsetninger i forhold til informasjonssikkerhetsledernes forståelse av begrepet. Mellomlederne har ut fra vår tolkning av intervjuene ikke en like klar forståelse av hva begrepet informasjonssikkerhet innebærer.

Rådgiverne trekker på sin side frem elementer som omhandler hvordan de behandler informasjon, herunder taushetsplikt, unngå deling av passord, nettvett og gode rutiner som sikrer informasjon. Informant A3 fremstår som noe mer usikker: "*Da tenker jeg verne personopplysninger, er det riktig?"* Dermed kan det tolkes som at informanten ikke er helt sikker hva begrepet informasjonssikkerhet innebærer. Tillit er en faktor som informantene selv trekker frem som viktig for hvordan man jobber mot informasjonssikkerhet. Informantene trekker frem tillit til ekspertene, bankenes systemer og tillit fra kundene. Samtidig er tillit en

viktig faktor for hvordan man opplever og forstår risiko med hensyn til informasjonssikkerhet, dermed vil tillit bli nærmere belyst i neste avsnitt.

De ansatte har tillit til ekspertene, og sikkerhetssystemene

IKT-sikkerhet er en betydningsfull del av samfunnssikkerheten, og bedrifter må ha på plass systemer og rutiner for å forebygge og håndtere uønskede hendelser til IKT, og er avgjørende for å oppnå tillit fra brukerne i både privat og offentlig sektor (NOU 2015:13). I forhold til banktjenestene som leveres til kundene i Norge, er det særskilt viktig at de opplever tillit til bankene og deres kapabilitet til å ivareta kundenes personopplysninger. Tillit fra bankkunder kan være svekket dersom virksomheten opplever uønskede hendelser, som tap av personopplysninger og annen informasjon grunnet datainnbrudd (NSM, 2015).

I henhold til NSM (2015) er trygghet og tillit de mest sentrale verdiene for små virksomheter og enkeltindivider. Selv om bankene som har vært kontaktet ikke kan karakteriseres som små virksomheter, fremhever informantene at tillit fra kundene er den viktigste verdien for norsk banknæring. Derfor arbeider de ulike bankene målrettet for å bevare tilliten fra kundene. Informant D forteller i denne sammenheng at dersom de er utsatt for en uønsket hendelse, velger de å belyse dem om dette når hendelsen er under kontroll. Informanten henviser til en hendelse de har hatt, og opplyser at de opplevde en positiv kunderespons, da kundene følte seg ivaretatt og inkludert av banken. Mellomlederne og rådgiverne bekrefter på lik linje med informasjonssikkerhetslederne at tillit fra kundene er det viktigste for dem, og at de derfor arbeider strukturert for å ivareta denne tilliten. Dette gjør de ved blant annet å følge rutiner og regler, som å sikre dokumentasjon og låse pc-en før de forlater kontoret. På denne måten iverksetter de tiltak som sikrer kundeinformasjon. Videre utdyper mellomlederne at for dem er en god IT-avdeling avgjørende for å sikre opplysninger, og for å ikke bli utsatt for digitale angrep. Med dette ser man her at informantene legger sin tillit til ekspertene, som for dem er informasjonssikkerhetslederne. Dette tolkes som at mellomlederne og rådgiverne kan ha manglende kunnskap om hvordan man kan unngå svikt på deres systemer. På en annen siden kan det hende at informantene retter seg mot IT-avdelingen grunnet manglende kunnskap om fenomenet.

5.1.7 Foreløpig oppsummering

Samtlige av informantene som jobber som informasjonssikkerhetsledere forteller at banknæringen benytter seg av ISO 27000 i arbeidet med risikostyring. Videre sier de at

risikostyring er en kontinuerlig prosess der de gjennomfører nye analyser en gang i året. Når det kommer til kommunikasjon og inkludering, integrering og refleksjon er det stor variasjon i besvarelsene. Informasjonssikkerhetslederne mener at alle i organisasjonen er inkludert gjennom kommunikasjon. Mellomlederne og rådgiverne på sin side påpeker at de ikke er inkludert i selve analyseprosessen, men at blir inkludert i etterkant av en hendelse.

Innføring av nye krav, digitalisering, økt konkurranse- og tidspress medfører nye og ukjente risikoer for banknæringen, og gjør systemene sårbare for trusselagenter. Informasjonssikkerhetslederne uttrykker størst bekymring med tanke på innføringen av de nye kravene. Mellomlederne og rådgiverne på sin side er i større grad bekymret for phishing og hacking. Når det kommer til menneskelige feil, er det blant informasjonssikkerhetslederne og mellomlederne enighet at dette utgjør den største årsaken til uønskede hendelser i forbindelse med informasjonssikkerhet. Rådgiverne derimot mener det er tekniske svakheter som er den største årsaken.

5.2 Hvilke faktorer er nødvendige for å opprettholde god informasjonssikkerhet?

I det følgende vil faktorer som belyser hvordan sikkerhetskulturen, og informasjonssikkerhetskulturen er i banknæringen tatt frem. Dette belyses blant annet ved organisatoriske normer som rutiner og håndbøker, kunnskapsdeling på tvers av avdelingene og rapporteringskulturen i bankene.

5.2.1 En sikkerhetskultur preget av læring, rutiner og håndbøker

Sikkerhetskulturen i virksomheten påvirker forståelsen for digitale sårbarheter, samt evnen til implementere tilstrekkelige tiltak for å skjerme seg mot digitale trusler (NSM, 2017; NOU 2015:13). En av mellomlederne sier at digitaliseringen i bankene ikke har hatt en betydelig innvirkning på hvordan arbeidsoppgavene utføres, men at dette er noe som har skjedd gradvis i løpet av årene. For å oppnå en god sikkerhetskultur er det nødvendig at man er villig til å bruke ressurser på passende og tilstrekkelige tiltak, det er også avhengig av den generelle sikkerhetskulturen i sektoren (NSM, 2017; NOU 2015:13). I lys av dette mener samtlige av informasjonssikkerhetslederne at de har en svært god sikkerhetskultur i bankene. Informant D påpeker at dette henger sammen med at de snakker godt sammen mellom de ulike avdelingene,

og har godt oppmøte på ulike arrangementer. Likevel forekommer det også uønskede hendelser i forbindelse med informasjonssikkerhet i bankene.

Årsaker til svikt innen en organisasjon kan komme av lav brukervennlighet, samt manglende kunnskap om sikkerhetsaspektet. Dette kan medføre at menneskene opplever utfordringer med kompliserte rutiner, spesielt dersom de ikke har nok kunnskap om hvordan systemet virker. Dermed er det nødvendig at utviklere og sikkerhetsledere tar hensyn til brukerne ved utvikling av systemer og sikkerhetsrutiner. På den måten blir det lettere for brukerne å benytte systemene sikkert og riktig (NOU 2015:13). Informasjonssikkerhetslederne som er intervjuet opplyser at de forsøker å heve kunnskapsnivået til de ansatte ved å introdusere korte læringsmoduler som skal være enkle for de ansatte å forstå og gjennomføre. En av informantene trekker frem at de benytter intranett til å publisere relevante artikler i forbindelse med sikkerhet. En annen informant forteller at de i tillegg til dette benytter seg av kahoot! for å teste de ansatte i forbindelse med sikkerhetsrutiner på en morsommere måte. Informant A uttrykker at de har fokus på informasjonssikkerhet ved å tilby flere ulike opplæringsprogram som de ansatte kan gjennomføre. Dette er også noe informant C påpeker: *"Vi har månedlig nano læringskurs med forskjellige tema, der en del er sikkerhetsrelatert. Typiske ting som tas opp er: lås pcén din, bytte passord, hvordan bruke telefon når du er på ferie og lignende. De er veldig korte, på 3-5 minutter."* Videre sier informanten at de har en stor håndbok som de ansatte skal anvende for å forstå systemene i banken, der rutiner og regler blir fremlagt. Samtidig fremhever informanten "*Det er jo selvsagt aldri nok fokus på sikkerhet, men så er det jo begrensinger på hvor mye tid vi kan bruke på det og da."* NOU (2015:13) viser til at enkeltindividers holdninger og sikkerhetskulturen kan påvirke sikkerhetsnivået, der det kan oppstå konflikter når det kommer til prioritering av sikkerhetsrutiner, og å gjennomføre oppgaver tidsnok. Dermed kan man forstå det slik at informanten opplever en konflikt mellom prioritering av sikkerhet, og det å gjennomføre sine arbeidsoppgaver, noe som kan svekke sikkerheten.

Ut i fra intervjuene med informasjonssikkerhetslederne oppleves det som at det er mye fokus på læring ved å bruke sikkerhetsbevissthetsprogrammer, og at det i tillegg refereres til rutiner og håndbøker. Man kan her forstå det slik at ledelsen benytter mye tid på å bevisstgjøre ansatte i banken om farene som beveger seg innenfor informasjonssikkerhetstematikken. Videre kan det forstås slik at det forventes av den enkelte at de setter seg inn i hva det innebærer ved å følge rutiner, håndbøker, og gjennom intranettet. Dermed kan stille seg spørrende om hvorvidt

dette blir opprettholdt av hvert enkelt individ i banken, dersom disse dokumentene, rutinene eller artiklene oppleves som tungvinte.

Mellomlederne uttrykker også at de har en god sikkerhetskultur. Da man spør mer utdypende om hva de legger i god sikkerhetskultur, fremkommer det forskjeller i hva de legger i begrepet. En informant sier: "*Så på en måte det aller viktigste er at banken hele veien har kunden først, kunden som sjefen og det hjelper da på en måte på måten vi jobber på"* (Informant D1). Ut i fra dette tolkes det slik at informanten mener at sikkerhetskulturen preges av kundefokuset, og med det er kanskje kunden grunnlaget for sikkerhetskulturen. Det som muligens menes med dette er at dersom det arbeides med kundens sikkerhet, vil man naturlig arbeide med gode sikkerhetsrutiner for å få til dette. En annen av mellomlederne fremhever at deres sikkerhetskultur har blitt påvirket av de nye regulatoriske kravene: *"Særlig det siste halvåret har det vært mye fokus på sikkerhetskulturen, dette henger jo sammen med GDPR"* (Informant C1). En annen informant forteller at de har en god sikkerhetskultur, og tror at dette henger sammen med at alle avdelingene er lokalisert i samme lokale slik at det er kort avstand mellom de ulike avdelingene. Dette medfører igjen en bedre kommunikasjon, da de har kort vei mellom avdelingene. Informant B1 sier:

> *Jeg vil definere den som veldig god. Alle vet viktigheten av å være forsiktige med opplysninger, dette med å være føre-var i forhold til, ja altså for eksempel at alle skrur av pc´en når de går, dette med sensitiv informasjon som kommer på mail så har vi sikret det i forhold til at det er bare du som får sendt ut den informasjonen du har tilgang til, så jeg føler den er god.*

Informant A1 sier: *"Jeg tror nok det ligger litt i ryggraden at det er viktig"*, men påpeker at de likevel opplever at rutinene glipper. For eksempel er det ikke alltid alle låser pc-en når de forlater plassen sin, selv om dette er noe de er pålagt å gjøre. Dermed kan det tenkes at det er en kultur som tillater at dette skjer, og at de ansatte ikke alltid er like bevisst over sine handlinger. Med dette belyses en sikkerhetskultur der rutine og håndbøkene blir neglisjert fordi de er for omfattende.

Rådgiverne uttrykker delte meninger om sikkerhetskulturen i banken. En informant mener den er god uten å utdype ytterligere: *"Bra, det er fokus. Så tenker jeg det kunne vært mye mye verre"* (Informant A2). En annen informant sier *"[...] så gjør nok banken det de må gjør, de har sine*

krav og regler" (Informant A3). Med dette ser man at det ikke er fokus på sikkerhetskulturen utover det som virksomheten er pålagt. De andre informantene opplever en god sikkerhetskultur, som er preget av samarbeid og åpen dialog. I likhet med noen av mellomlederne er det også noen av rådgiverne som trekker frem kunden som en faktor som påvirker bankens sikkerhetskultur: "*Den er jo god, vi jobber alle sammen mot samme mål, at sikkerhets skal være i høyeste grad å stole på, både for banken og kunden"* (informant C2).

5.2.2 Kunnskap og kommunikasjon påvirker informasjonssikkerheten

Det er flere faktorer som er nødvendige for å sikre god informasjonssikkerhet, blant annet god sikkerhetskultur, lover og retningslinjer, verdivurderinger, brukerveiledninger, rutiner, brannmurer og systemer som er egnet til å holde på informasjon (NOU 2015:13). I forbindelse med hva som skal til for å opprettholde god sikkerhetskultur uttrykker informasjonssikkerhetslederne at det er flere faktorer som må være på plass for oppnå dette, men en fellesnevner for alle de fire bankene er læring og deling av kunnskap. *"[...] det er å dele kunnskap og forhindre taus kunnskap"* (informant D). I likhet med informant D trekker informant A frem flere av de samme faktorene: *"Det er bra opplæringsprogram, kulturprogram, det er veldig viktig å sikre at ledelsen har en felles forståelse og kommuniserer det samme ned. Du får det aldri til uten den rette tonen i fra toppen. Og så har du jo og det å holde seg oppdatert på de siste truslene."* Ut i fra dette ser man at ledelsen har en viktig rolle for å påse at alle ansatte har arbeider målrettet for å opprettholde informasjonssikkerheten på et akseptabelt nivå. Informant B påpeker at det ligger i bankkulturen å tenke sikkerhet, grunnet lang tid med fokus på dette, samt at det ligger en forventing om at man fokuserer på sikkerhet, noe som er med på å skape en god sikkerhetskultur. Videre sier informanten: *"Gode folk på sikkerhetsavdelingen".* Med dette kan man forstå det slik at sikkerhetsavdelingen har en vesentlig rolle for å påse at sikkerheten blir prioritert. Informanten forteller også at tillit er en viktig del av opprettholdelse av god informasjonssikkerhet*: "Det er egentlig å få frem det budskapet av at vi lever av og med tillit [...]. Så det er egentlig det vi fokuserer veldig på, at vi lever av og med tillit, og få det spredd ut i organisasjonen."* Informant C trekker frem forankring og kompetanse som viktig faktorer for å unngå større uønskede hendelser. Dette er også noe som NOU (2015:13) fremhever som viktige faktorer for å blant annet unngå menneskelig svikt. Samtidig opplyser informant C, at banken deres består av flere kontorer spredt utover landet. Dermed er informanten usikker om hvorvidt fokuset på god informasjonssikkerhet er lik blant alle kontorene. Samtlige av informantene opplyser at de deler erfaringer innenfor ulike forum, for å sikre god kompetanse.

> *[...] Dette er jo noe som vi håndterer i samarbeid med andre banker, for det er jo sjelden at phishing er rettet direkte mot oss, ofte er det mot de større bankene [...] Så da er det jo viktig for oss å få informasjon om hvordan dette skjer, på hvilken måte treffer det våre kunder, og hvordan kan vi forhindre at våre kunder blir lurt* (Informant B).

Samtidig opplever informant D at de kunne ha vært flinkere på kunnskapsdeling mellom seg internt i organisasjonen etter at de har blitt utsatt for en uønsket hendelse i forbindelse med organisert kriminalitet.

> *[...] i mange sammenhenger så er vi flinkere med kundene enn oss selv. Jeg har aldri arbeidet et annet sted som har så høy kundefokus som denne banken. [...] Noe som skaper utfordringer for hvordan vi lærer av uønskede hendelser. Jeg tror at vi er flinke på å oppdatere kundene, så glemmer vi kanskje raskt nok å informere internt. Dette er noe vi bør bli flinkere til* (Informant D).

Med dette viser informanten til at kundefokuset overskygger det interne arbeidet i organisasjonen.

Samholdet i de ulike organisasjonene presenteres som godt, og samtlige av informasjonssikkerhetslederne påpeker at de har en delende og lærende kultur. Tre av de fire informasjonssikkerhetslederne forteller at de deler ulike hendelser med banken på tvers av de ulike avdelingene, slik at alle vet hva som foregår, og hvordan dette påvirker deres arbeid. De påpeker også at de kommuniserer svært godt med de ulike avdelingene. Informant D sier: *"Vi har en flat struktur, som vil si at vi ser oss alle like verdifulle."* Videre sier samtlige av informasjonssikkerhetslederne at tillit er noe av det viktigste de har for å kunne drive bank. Det er også enighet om at dette oppnår de ved å ha en åpen dialog med sine kunder, slik at de også til enhver tid vet hva som foregår, og føler seg på den måten ivaretatt og inkludert. "*Vi var åpne med kundene om hendelsene, slik at de også ikke mister tillit til oss i denne prosessen"* (Informant D).

> *Vi deler først og fremst kun en hendelse med dem som er pårørende og den eventuelle ansatte som har vært med i en hendelse. Jeg deler ikke dette med resten av bedriften, da det ikke er nødvendig. Det vi eventuelt gjør i etterkant av en hendelse når ting har roet*

seg litt, er at vi tar det opp i plenum på en mer generell måte, for å sikre læring, og hva en skal være obs på. Men mitt mål er ikke å henge ut noen (Informant C1).

Når det kommer til hva som må til for å opprettholde god informasjonssikkerhet, er det en del ulikheter blant informantene på mellomledernivå. To av informantene, herunder C1 og B1, er enige om at en god IT-avdeling som kan sikre at eksterne angrep blir stanset og oppdaget før den rekker å skape betydelige skader i banken er avgjørende. *"Det er viktig at vi får systemer som er tilrettelagt dagens trusler"* (Informant C1). Med dette kan en forstå det slik at informant B1 og C1 legger vekt på gode systemer fremfor andre faktorer som kan medføre god informasjonssikkerhet. I tillegg legges ansvaret hos IT-avdelingen for å sikre systemene slik at de er rustet til å håndtere dagens trusler, men ansvaret som brukeren har av systemet blir ikke nevnt. Informant A1 og D1 beskriver andre faktorer som kan bidra til å bevare informasjonssikkerheten. *"Alle må jo ihvertfall være på det samme laget og utøve det som man enes om"* (Informant D1). Videre sier informant A1: *"Hva som skal til, jo, en ting som må til er sterkt ledelsesfokus på viktigheten av det. Fordi, det er viktig å sette det på agendaen og bruke litt tid på det."* Ut i fra dette kan det forstås som at informantene, A1 og D1, legger mer vekt på de menneskelige og organisatoriske faktorene, fremfor de tekniske. To av mellomlederne mener at kommunikasjon er en viktig faktor for en god sikkerhetskultur. Informant B1 på sin side påpeker at det er viktig med gode rutiner. En annen informant er usikker på hvilke faktorer som er viktige: *"Jeg vet ikke helt. Jeg kan ikke svare på det"* (Informant C1). Med dette kan man forstå det slik at informanten ikke har reflekter over sikkerhetskulturen, og det kan tyde på at sikkerhetskultur ikke har en sentral rolle i denne banken.

Rådgiverne mener også at rutiner er en viktig faktor for å oppnå en god sikkerhetskultur: "*Det er jo rutinene som er satt, altså påse å bruke de verktøyene vi har tilgjengelig, passe på at man prøver å følge rutinene som er forventet"* (Informant B2). En annen informant fremhever viktigheten av at alle bidrar til en god sikkerhetskultur: *"Det er viktig å vite at ikke kun en avdeling jobber for det, men at alle ansatte, avdelinger og bygg er med på det. Dette er fordi ting kan lekke ut i alle ledd"* (informant D2). En annen informant mener kommunikasjon, faglig oppdatering og det å spørre andre om råd er viktig for å sikre god informasjonssikkerhet. Videre sier en annen informant: "*Samtidig skal vi jo få jobben gjort, så vi kan ikke bli helt mørkredde heller"* (Informant B2). Med dette forstås det slik at de ansatte har flere arbeidsoppgaver, og at det er begrenset med tid de kan bruke på informasjonssikkerhet. Utover dette påpeker informant

A2: "*Så jeg tenker at det er utrolig viktig at de ansatte blir oppdatert på hva som er aktuelt nå, hvis det skjer nye typer hendelser."* Informanten mener altså at kunnskap om det aktuelle trusselbildet er en viktig faktor for å sikre informasjon. I likhet med informant A2 mener også informant A3 at det med å belyse uønskede hendelser er viktig.

5.2.3 En rapporteringskultur preget av underrapportering

Rapportering av sikkerhetstilstand kan bidra til å bedre sikkerheten, men dersom sikkerhetstilstanden ikke er kjent for virksomhetsledelsen kan det føre til at sikkerhetsmessige tiltak ikke sees i sammenheng og at nødvendige tiltak for å lukke sårbarheter ikke blir iverksatt. Dette kan medføre at virksomheten blir utsatt for høyere risiko enn den har bevissthet om (NSM, 2017). Alvorlige hendelser skal etter IKT-forskriften rapporteres. Likevel er det registrert en underrapportering i flere ulike sektorer i Norge, også bankene. Årsaken til dette kan henge sammen med at digitale hendelser ikke er like godt forklart i lovene og forskriftene som næringen benytter seg av, men det kan også være basert på frykt om at dersom en hendelse blir gjort kjent, kan ødelegge bedriftens omdømme. Det henger sammen med hva den enkelte bedrift anser som alvorlige trusler, og hva de mener kan føre til store konsekvenser (NOU 2015:13). I NSM (2015) sin rapport fremkommer det at mangelfull rapportering av IKT-hendelser, kan føre til svekket forbedring og læring innen forebyggingsarbeidet.

De fleste av informasjonssikkerhetslederne uttrykker en mistanke om at det kan forekomme en del underrapportering, men årsaken til dette kan de ikke gi klart uttrykk for. Informant D sier følgende: *"Det er nok en del underrapportering dessverre, på tross av at vi ikke er ute å ta noen hvis en feil først skulle skje. For meg og oss alle, er det viktig å lære av feilene. Men det får vi jo ikke så lenge det er underrapportering."* Informanten forteller videre at de jobber mye med underrapportering for å unngå det, og ønsker å motivere ansatte til å rapportere selv småting som ikke har ført til noen stor hendelse eller påført organisasjonen eller enkeltpersoner noen konsekvenser. Dette er også noe som informant B og C uttrykker. Informant A skiller seg ut fra de andre informantene da informanten sier at alle hendelser i deres bank blir rapportert: *"Hvis vi har uønskede hendelser så er vi jo rapporteringspliktige, så det er jo klart vi gjør det hvis vi har en uønsket hendelse."* Med dette kan man forstå det som at alle hendelser som er rapporteringspliktige blir rapportert.

Blant mellomlederne kommer det frem fra flere informanter at hvorvidt en hendelse blir rapportert, vil være personavhengig av hva den enkelte oppfatter som alvorlig nok til å

rapporteres. *"Det er jo at en person gjør en vurdering, om de synes det er viktig"* (Informant C1). Samtidig uttrykker informanten at det ikke forekommer underrapportering i deres bank. Informant D1 på sin side forteller at de har et system for hva man skal rapportere, men antar at ikke alt blir rapportert tross dette. En annen informant sier: *"Ja, altså, det kan jo være hendelser som er så små at vi ikke anser det som relevant, jeg vet ikke hvor grensene går"* (Informant B1). Her viser informanten til at det er ikke klare grenser for hvilke hendelser som skal rapporteres eller ikke, og at rapporteringen er avhengig av størrelsen på hendelsen. Informant D2 sier følgende: *"Det blir mye skriftlige oppgaver. Dersom det er en sak som må rapporteres til datatilsynet krever det mye, og det krever mye tid for å forklare alle/ eventuelle pårørende hva som har skjedd, og hvordan det har skjedd."* Ut i fra dette kan man anta at rapportering av hendelser er en tidkrevende prosess, og at det kan være en medvirkende årsak til underrapportering.

Blant rådgiverne kommer det frem at hvorvidt de rapporterer er svært avhengig av hva de anser som alvorlig nok til å måtte rapporteres til nærmeste leder. I hvilken grad dette gjøres varierer ut i fra de fire ulike bankene. Informant A2 opplyser om at alt bør rapporteres, men at det likevel vil forekomme noe avvik etter informantens mening. Informant D2 på sin side påpeker at de har en god rapporteringskultur, der de motiveres til å heller rapportere en gang for mye enn for lite. Samtidig uttrykker informanten at grunnet ulik oppfatning av hva som er alvorlig vil det også forekomme ulik oppfatning av hva som må eller bør tas videre til nærmeste leder: "*[...] men selvsagt, vil jo ulike mennesker tolke det på en ulik måte, som kan påvirke om man synes det er alvorlig liksom."* Informant B2 opplyser at de har svært lav terskel på hva som rapporteres, og påpeker at de blir oppfordret til å rapportere: "*Vi har fått beskjed at ingen sak er for dum, at vi heller skal rapportere en sak for mye enn for lite".* En annen informant fremhever at det er nærmeste leder som avgjør hvilke hendelser som skal rapporteres: "*Så i mange tilfeller er det nærmeste leder som er filteret"* (Informant C2).

5.2.4 Foreløpig oppsummering

Blant informantene er det ulike oppfatninger av hva som påvirker bankens sikkerhetskultur og dermed dens informasjonssikkerhetskultur. Informasjonslederne sier at det er et stort fokus på å bevisstgjøre ansatte i bankene om hva informasjonssikkerhet er, og hvordan man skal jobbe for å sikre informasjon. Dette gjøres ved å benytte ulike sikkerhetsbevissthetsprogrammer som e-læringsmoduler, Kahoot!, rutiner og håndbøker. Rådgiverne på sin side opplyser at gode lederegenskaper er viktig for å kunne bevisstgjøre de ansatte om hva som er viktig. I tillegg til

en god sikkerhetsavdeling som skal påse at trusselagenter ikke kan utnytte svakheter i systemet. Mellomlederne sier at kundefokus er med på å sikrer god informasjonssikkerhet. Rådgiverne påpeker at interne rutiner er det viktigste leddet i banken for å sikre god informasjonssikkerhetskultur i bankene, og at bankene har lover og krav som skal sikre at dette blir ivaretatt. I forhold til rapportering av uønskede hendelser ser man at de fleste anerkjenner det faktum at det er underrapportering av uønskede hendelser i banknæringen. Videre ser man at de fleste mellomlederne og rådgiverne mener at hva som rapporteres er personavhengig, mens noen av informasjonssikkerhetslederne på sin side henviser til lovene om hva som må rapporteres til myndighetene og at deres praksis samsvarer med dette.

6. Diskusjon

I dette kapittelet vil de empiriske funnene bli drøftet opp mot studiens teoretiske forankring og problemstilling.

Hvordan forstår og jobber banknæringen for å møte risikoen for uønskede hendelser i forbindelse med informasjonssikkerhet?

Studiens forskningsspørsmål er lagt til grunn for inndelingen i det følgende kapittelet. Flere av de teoretiske bidragene krysser hverandre, og dermed er ikke ett enkelt teoribidrag rettet mot et spesielt emne.

6.1 Hvordan forstår de ansatte i banknæringen risiko og sårbarhet knyttet til cyberangrep rettet mot informasjonssikkerhetssystemene?

Risikostyring kan være ulike tiltak og aktiviteter, som kan bidra med å gjøre risiko mer håndterbart (Aven et al., 2004). I henhold til internkontrollforskriften (1996) skal alle virksomheter gjennomføre risiko- og sårbarhetsanalyser, der handlinger og mål bestemmes på bakgrunn av et relevant risikobilde (Aven & Renn, 2010; Aven, 2015). I forhold til dette svarer samtlige av informasjonssikkerhetslederne at de gjennomfører årlige ROS-analyser i henhold til ISO 27000. Likevel er det få av informantene som utdyper hvordan dette arbeidet utføres i deres bank, og noen av informantene fremstår noe usikker når det kommer til risikostyring i bankene. Med dette kan det forstås slik at noen av informantene ikke er helt trygge på risikostyringsprosessene. På en annen side kan det tenkes at noen av informantene var redde for å gi ut for mye informasjon som kan avsløre for mye av deres arbeid, og dermed svekke sikkerheten. På grunn av dette, er det vanskelig å trekke en konklusjon om hvordan kartlegging av risiko og sårbarheter foregår i banknæringen. I denne oppgaven er det dermed valgt å fokusere på elementene som må være på plass i organisasjonen for å få til en god risikostyring, herunder kommunikasjon og inkludering, integrering, og refleksjon (Asslet & Renn, 2011).

En utfordring for sikkerhetsarbeidet er mangelfull planlegging og styring av sikkerhetsarbeidet, noe som er grunnleggende for å gjennomføre sikringstiltak. Det er også indikasjoner på at sårbarhetsreduserende tiltak ikke samsvarer med utviklingen i trusselbildet (NSM, 2017).

Kommunikasjon og inkludering

Når det gjelder kommunikasjon og inkludering sier samtlige informasjonssikkerhetsledere at de kommuniserer med ansatte i virksomheten gjennom intranett, og benytter e-moduler for å inkludere de i risikostyringen. I henhold til Löfstedt (2003) skal kommunikasjon gjenspeile et meningsfullt samspill, der kunnskap, erfaringer, tolkninger, bekymringer og perspektiver utveksles. Kommunikasjon i sammenheng med risikostyring referer til utveksling mellom beslutningstakere, eksperter, interessenter, allmennheten og hverandre. Dermed er toveiskommunikasjon en viktig faktor for å oppnå god risikostyring (Pidgeon et al., 2005). Informantene forteller at de mottar informasjon gjennom intranett, men det forstås slik at det ikke benyttes som en kilde til toveiskommunikasjon som er en viktig faktor dersom man skal kunne oppnå et meningsfullt samspill. Dermed kan det tenkes at det er i stor grad enveiskommunikasjon som praktiseres i banknæringen, som igjen vil være en svakhet for risikostyringsprosessen. Dette er fordi man ikke har oversikt om mottakerne har mottatt, og forstått beskjedene som blir gitt dersom det kun er basert på en enveis kommunikasjon. Dette kan medføre utfordringer for læring siden det ikke forekommer en utveksling av beskjeder. I tillegg kan det tenkes at skriftlig informasjon kan mistolkes, og at de ansatte ikke oppnår samme forståelse av det som søkes å formidles gjennom intranett. Dette kan føre til sårbarheter i forbindelse med arbeidsoppgavene som utføres av de ansatte, dersom de ikke innehar samme forståelse, eller oppnår læring av det som formidles fra toppen og ned.

Mellomlederne og rådgiverne på sin side sier at de i liten grad blir inkludert i risikostyringen. Informant A1 sier at de blir inkludert gjennom spørreskjema, likevel er ikke dette noe rådgiverne i samme bank trekker frem. Mellomlederne opplyser dog at de heller opplever å bli informert i etterkant av en hendelse. Utover dette bekrefter samtlige informanter at det benyttes intranett og e-moduler for å øke bevisstheten og kunnskapen. I banknæringen er det rådgiverne som stort sett behandler informasjon knyttet til kundene. Dermed kan det være hensiktsmessig å inkludere de i risikostyringen, slik at man får et helhetlig risikobilde. Dersom risikostyringen kun baserer seg på eksperter og deres kunnskap og forståelse vil det være vanskelig å få til et samarbeid på tvers av virksomhetene, siden de ansatte på lavere nivå vil ha et annet syn på risikoer og sårbarheter (Aven, 2015). Inkludering kan ta forskjellige former (Asslet & Renn, 2011; Renn, 2008), og selv om bankene kan bestå av svært mange ansatte vil det være mulig å inkludere de gjennom åpne foraer eller blandede rådgivende komiteer.

For å få til integrering er det nødvendig å inkludere alle ansatte, slik at man kan innhente relevant kunnskap og ulike risikooppfattelser, som kan benyttes for å kartlegge risikobildet i organisasjonen (Aven, 2015). Ut i fra intervjuene ser man at både toveiskommunikasjon og inkludering er fraværende i banknæringen. Dette kan føre til utfordringer i forhold til integrasjon, siden risikostyringen ser ut til å baseres på ekspertenes syn og erfaringer. Dette fører igjen til at alle relevante risikoer ikke blir tatt med i evalueringen. Dermed er manglende integrasjon en svakhet for sikkerheten i bankene, og de ansatte kan utføre risikofylte handlinger som de ikke burde, siden de ikke innehar samme kunnskap som informasjonssikkerhetslederne.

For å oppnå god risikostyring er det viktig at man reflekterer over hva som er sikkert nok, noe som kan gjøres via kollektiv refleksjon (Beck et al., 1994). Likevel blir ikke refleksjon nevnt som et verktøy innen risikostyring, verken av de faglige ekspertene eller informantene. Refleksjon kan bidra til å øke kunnskapen og skape en felles forståelse av de risikoene og sårbarhetene som er relevante. Med dette kan manglende refleksjon skape utfordringer for læring i bankene, noe som kanskje er enda viktigere i dag med tanke på den raske digitale utviklingen. Dermed kan det tenkes at mangel på læring skaper sårbarheter i bankene, og kan føre til flere uønskede hendelser med informasjon på avveie i fremtiden. Dette er fordi man fortsetter å bruke det man kjenner til fra tidligere, som trolig ikke er sikkert nok i forbindelse med dagens trusselbilde.

6.1.2 Hvordan forstår ansatte risikoer og sårbarheter i banknæringen

Risiko omhandler hendelser som kan føre til positive og negative resultater for en organisasjon (Njå et al., 2017), herunder trekker informantene frem risikoer og sårbarheter som de nye lovkravene, konkurranse og tidspress, cyberangrep og menneskelig feilhandlinger.

Når det kommer til innføringen av de nye lovkravene er dette noe som banknæringen ikke har noen særlig innvirkning på, og deres oppgave er å drifte i samsvar med kravene når de blir innført. De nye kravene medfører en omstrukturering av hvordan banken driftes, noe som kan medføre nye og ukjente sårbarheter, som kan utnyttes av trusselagenter. Dette kan igjen føre til store konsekvenser for bankens kunder, og dermed banknæringen. For å håndtere disse utfordringene kan man benytte risikoanalyser og verdivurderinger (Aven et al., 2004). Samtidig er det vanskelig å få et "korrekt" risikobilde av noe som er nytt og ukjent. Dermed kan det tenkes at banknæringen vil oppleve en økt utfordring knyttet til sikring av informasjon i fremtiden. En annen utfordring som informantene trekker frem i forbindelse med de nye

kravene er at de er ufullstendige, og banknæringen må samarbeide for å kartlegge standardene som skal bidra til at kravene blir mer fullstendige. I denne sammenheng fremstår ikke alle informasjonssikkerhetslederne som like oppdatert på lovverket, og heller ikke like bekymret, noe som kan tyde på at ikke alle har like stor interesse og kunnskap om PSD2. Dermed kan det være vanskelig å forestille seg hvordan dette samarbeidet skal foregå. Det kommer ikke frem i intervjuene hvem det er som skal samarbeide, og hvordan dette samarbeidet skal foregå. Dermed kan det tenkes at manglende interesse og kunnskap om lovkravet kan skape en utfordring når standardene skal utformes.

Bankene opplever de nye kravene som motstridende med allerede eksisterende lover, som bokføringsloven. Dette kan medføre utfordringer for banknæringen dersom kundene velger å ikke godta lagring av data og personopplysninger, noe som de nå har muligheten til å bestemme selv i lys av GDPR. Dermed står banknæringen mellom to lovverk som på den ene siden sier at de må slette all personlig data om denne personen, og bokføringsloven på den andre siden som krever at dataen skal være lagret. Informantene forteller at hvordan dette skal gjennomføres er ikke klart enda, noe som er litt rart med tanke på at det er under en måned igjen til GDPR innføres.

Informasjonssikkerhetslederne anser innføringen av de nye lovkravene som en potensiell risiko. Dette er fordi rutiner og prosedyrer må endres for å oppfylle de nye kravene, noe som kan skape rom for feilhandlinger i overgangsfasen, som igjen kan utnyttes av trusselagenter. Dette er også noe Norges Bank (2017) har vurdert som en potensiell trussel for nye risikoer. Blant mellomlederne og rådgiverne fremkommer ikke denne bekymringen like stor. Noen av dem betrakter til og med endringene som positive for banknæringen, mens andre er noe bekymret for økt cyberangrep siden PSD2 innebærer økt flyt av informasjon når kundedata skal deles med andre aktører. Dette er noe som etter vår mening underbygger vår forståelse av at kommunikasjonen på tvers i bankene ikke er tilfredsstillende, siden flere av mellomlederne og rådgiverne uttrykker liten kunnskap om regelverkene. Mangelen på kommunikasjon på tvers av avdelingene og kunnskap om hvilke risiko som anses som mest fremtredende i forhold til implementering av de nye regulatoriske kravene, kan igjen føre til økt sårbarhet når bankene skal overføre kundeinformasjon med andre aktører, dersom de ikke anser dette som en like stor risiko som informasjonssikkerhetslederne.

Konkurranse og tidspress åpner opp for mulige sikkerhetsbrudd på informasjonssikkerhetssystemene

Den raske utviklingen innen teknologien kan føre til sårbarheter og risikoer (Berg, 2012), som kan utnyttes av trusselagenter (Rausand & Utne, 2009). Fagekspertene nevner den raske teknologiske utviklingen som en potensiell risiko for at den finansielle næringen kan oppleve uønskede hendelser, som igjen kan føre til sårbarheter som trusselagenter kan utnytte (NOU 2015:13). Dette er også noe informasjonssikkerhetslederne nevner, og spesifiserer tidspress og konkurranse som en fremtredende risiko og sårbarhet som fører til at bankene opplever avvik fra tilfredsstillende informasjonssikkerhet. Leveson (2011) viser til at redusert tid til å teste ut produktene er en utfordring som kommer av kompleksiteten i et system. Særlig informant D nevner dette som en utfordring. Informanten forteller i denne sammenheng om en hendelse i deres bank som oppstod nettopp på grunn av tidspress og konkurranse. Dersom hendelsen ikke ble oppdaget så rask som den gjorde kunne den ha ført til store konsekvenser for banken og kundene. Eksempelet som informant D referer til, blir vurdert av NOU (2015:13) som en sårbarhet innen banknæringen, siden de ligger i forkant i bruk av IKT ved kundebehandling. Dette har ført til komplekse informasjonssystemer og verdikjeder, som igjen kan føre til både tilsiktede og utilsiktede hendelser. Ut i fra dette kan det tenkes at konkurranse og tidspress i sammen med nye lovkravet PSD2 som nevnt ovenfor kan føre til flere uheldige hendelser, da konkurransen på markedet blir større, og fokuset på å beholde kundene kan ta over fokuset på sikkerheten. Her kan det tenkes at bankene vil ha enda større behov for å utvikle nye applikasjoner og betalingssystemer for å beholde sin markedsandel grunnet de nye konkurrentene. Sammen med faktumet at de norske systemene i bankene ikke er egnet til denne teknologien (Norges Bank, 2017), og muligheten for at bankene velger å lansere nye applikasjoner før de er tilstrekkelig testet, kan igjen innebære nye risikoer og sårbarheter som kan utnyttes av trusselagenter.

Banknæringen, et mål for cyberangrep?

Flere av informantene trekker frem cyberangrep mot informasjonssystemene som en stor risiko for banknæringen. NOU (2015:13) trekker også frem at mengden cyberangrep stiger, og at trusselagenter benytter mer sofistikerte metoder. Dette er faktorer som kan innebære utfordringer for banknæringen når det kommer til å sikre informasjon, og kan medføre behov for økt kunnskap blant de ansatte, slik at de er bedre rustet til å sikre informasjon mot trusselagenter.

I likhet med NOU (2015:13) viser informantene til phishing som en stor utfordring for banknæringen. Ved å benytte phishing klarer trusselagenter å lure til seg informasjon fra kunder og ansatte som de benytter til egen vinning. Det er spesielt kundene som trekkes frem som ofre for phishing. Dette kan føre til tap av tillit fra kundene, og medføre at kundene velger å benytte seg av andre banker. Her kan det tenkes at banknæringen bør inkludere kundene i større grad når det kommer til arbeidet med å sikre informasjon, og dermed styrke risikostyringen i bankene. Selv om banknæringen har et stort fokus på informasjonssikkerhet, og dette er noe som de arbeider med daglig, er det kundene som er sluttbrukerne av systemene som banknæringen tilbyr. Dermed bør kundene også inkluderes i forebyggingen av uønskede hendelser. Sårbarhet er definert som systemets forutsetning for, eller manglende evne til å fungere under/etter at det har blitt utsatt for uønsket hendelse (Aven et al., 2004; Engen et al., 2016). Med dette kan det tenkes at den menneskelige faktoren er en sårbarhet for informasjonssystemene, og dermed bør være en større del av sikkerhetsarbeidet noe som belyses ytterligere i neste avsnitt.

Mennesket er det svakeste leddet

I henhold til NOU (2015:13) skyldes menneskelige feilhandlinger uforsiktighet eller uvitenhet, og er noe som kan føre til store konsekvenser for banknæringen. Menneskelig svikt kan være et resultat av lav motivasjon grunnet bestemte retningslinjer og manglende kunnskap, som kan føre til sårbarheter (NSM, 2015). De fleste informantene har opplevd hendelser knyttet til menneskelige feilhandlinger, som ofte er knyttet til feil bruk av systemene. Feilutsendelse av e-post er en ofte nevnt årsak til at uønskede hendelser finner sted. Således kan det være interessant å se på hvorfor menneskelige feilhandlinger ser ut til å være så fremtredende. Dekker (2006) mener herunder at menneskelig svikt forekommer fordi systemene tillater det. Derfor kan det være nødvendig å se på organiseringen av arbeidet i banknæringen, altså systemene og rutinene som benyttes. Det kan tenkes at systemene ikke er tilpasset menneskene som arbeider i virksomheten, eller at rutinene er så omfattende at de er vanskelige å forholde seg til. Følgelig kan det tenkes at de ansatte ikke benytter rutinene dersom de ikke forstår hva de innebærer, og fordi at det krever mye tid å sette seg inn i de. Informant C forteller i denne sammenheng at dersom det oppstår slakk på utførelse av rutiner, vil ikke deres funksjon ha noen verdi. Dette er igjen noe som kan medføre sårbarheter i sikkerhetsarbeidet, siden hensikten med rutinene er å bidra til at arbeidsoppgavene gjennomføres i henhold til virksomhetens sikkerhetspolicy. Med dette kan det tenkes at rutinene ikke oppnår sin hensikt, og bør derfor revideres og tilpasses

brukerne. Det er viktig å påse at rutiner og håndbøker er levende dokumenter slik at de hele tiden er i samsvar med hvordan arbeidsoppgavene gjennomføres på nåværende tidspunkt.

Noe som også har vist seg som et interessant funn er at rådgiverne som behandler kundeopplysninger er av en annen oppfatning. De trekker frem brudd på sikkerhetssystemene, og cyberangrep som de største risikoene og sårbarhetene for banknæringen, men trekker ikke frem menneskelig svikt som en sårbarhet for informasjonssikkerhet. Denne ulike forståelsen kan være en sårbarhet for banknæringen. Dette er fordi rådgiverne som behandler informasjon muligens ikke beskytter informasjonen på samme måte fra innsiden, siden de ikke anser dette som en like stor sårbarhet som lederne. Det kan også tenkes at rådgiverne ikke nevner menneskelig svikt som en sårbarhet fordi de er av en annen oppfatning av hvilke risikoer og sårbarheter som er aktuelle for banknæringen, som igjen kan tyde på manglende kommunikasjon, inkludering og integrering mellom ledelsen og rådgiverne.

I tillegg viser Reddick (2009) til menneskelig feil som én av hovedårsakene for at informasjonssikkerhetssystemene innen en virksomhet er utsatt for risiko og sårbarheter som åpner opp mulighetene for å bli utnyttet av trusselagenter. Årsakene til menneskelig svikt kan ifølge Reddick (2009) komme av dårlig ledelse, dette er også noe NOU (2015:13) påpeker. Dette kan henge sammen med det Dekker (2006) sier, at mennesker fokuserer på feil risikoer siden ledelsen ønsker at hovedfokuset skal være eksempelvis effektivitet og inntjening. Dette er også noe som informantene forteller da de sier at det er begrenset med tid de kan bruke på sikkerhet, siden de har sine arbeidsoppgaver som må utføres. Derfor kan det tenkes at feilhandlinger skjer grunnet tidspress, og manglende kunnskap om de risikoene og sårbarhetene som eksisterer. Det kan også tenkes at det er vanskelig å finne en balanse mellom det å øke kunnskapen, og gjennomføre arbeidsoppgaver. Derfor kan det være en fordel å gi de ansatte avsatt tid som de skal benyttes til læring og fokus på sikkerhet, utover sikkerhetsbevissthetsprogrammene.

6.1.3 Hvordan forstår informantene informasjonssikkerhet, og hva påvirker deres forståelse

Når det kommer til hvordan de ansatte i banknæringen forstår hva informasjonssikkerhet innebærer, er det flere ulike faktorer som kan være av betydning, herunder erfaring, kunnskap, grad av frivillighet, media, sunn fornuft, sosial og kulturell påvirkning, samt tillit. Likevel vil

ikke alle faktorene bli diskutert hver for seg, men det vil heller søkes å se hvordan informantene selv forstår informasjonssikkerhet, og hva de legger i begrepet.

I NOU (2015:13) legges det vekt på tre elementer, konfidensialitet, integritet og tilgjengelighet. Når det kommer til informasjonssikkerhetslederne ser man at de også i likhet med NOU (2015:13) legger vekt på den akademiske forståelsen av begrepet. Dette kan henge sammen med deres kunnskap og erfaring, da de naturligvis vil ha mer kunnskap om informasjonssikkerhet siden det er dette deres arbeidsoppgaver omhandler. I tillegg var det flere av informantene som kunne fortelle at de hadde en utdannelse innen IKT-sikkerhet, og mye erfaring fra flere ulike bransjer både nasjonalt og internasjonalt. Dette kan være faktorer som er med på å forme deres forståelse av informasjonssikkerhet. Under intervjuene var det noen av informasjonssikkerhetslederne som benyttet et svært avansert språk, og det var til tider vanskelig å forstå hva de mente og hva de prøvde å formidle. Dette kan også være en utfordring når informasjonssikkerhetslederne er i kontakt med de andre ansatte i virksomheten, som ikke har samme erfaring og kunnskap om informasjonssikkerhet som de. Følgelig kan dette føre til misforståelser mellom informasjonssikkerhetslederne og de andre ansatte, og med det svekke sikkerheten i bankene.

Mellomlederne og rådgiverne derimot gir ikke en klar beskrivelse av hva de legger i informasjonssikkerhet, men forteller mer om tiltak og faktorer som er viktige for å sikre informasjon. De trekker frem elementer som riktig behandling av informasjon, at man må være kritiske, rutiner og regelverk, og at det er viktig med en felles forståelse av begrepet. Man legger særlig merke til at de selv påpeker at felles forståelse av begrepet er viktig for å sikre god informasjonssikkerhet i banken. Likevel opplever man ulikheter i hvilke risikoer de ansatte på de ulike nivåene anser som relevante. Dette belyses med informant D1 og D2 som sier følgende: *"Jeg må jo innrømme at jeg personlig ikke er veldig bekymret for hacking fordi at jeg føler og opplever at vi har veldig gode systemer som fanger det opp"* (informant D1). Informant D2 på sin side sier: "*Hacking, virusangrep trojaner, hva kundene går på selv – går de på en mail og tror at det er oss."* Sitatene belyser hvor forskjellig trusselbildet oppfattes av mellomlederen, sammenlignet med rådgiveren. Det kan tenkes at forståelsen påvirkes av at de ansatte på de ulike nivåene har ulike oppgaver, og dermed ulik innsikt i sikkerhetsarbeidet. Samtidig kan det være en utfordring for sikkerhetstiltakene, siden de som skal benytte seg av tiltakene ikke har samme forståelse for hvorfor disse er så viktige, og med det ikke tar innover seg tiltakene som innføres.

I henhold til Sjøberg og Sjøberg (2001) vurderes risiko ulikt av lekfolk og eksperter, noe som viser seg tydelig når man analyserer forskjellene mellom informasjonssikkerhetslederne og de ansatte på lavere nivå. Når mennesker evaluerer risiko linker de blant annet forventninger, håp, frykt og følelser sammen med aktiviteter eller hendelser som har usikre utfall (Aven & Renn, 2010; Renn, 2008). Det er altså naturlig at mennesker vurderer risiko ulikt på bakgrunn av flere faktorer som har formet deres risikoforståelse. Likevel kan det være hensiktsmessig at de bekymringene som informasjonssikkerhetslederne ser i forbindelse med informasjonssikkerhet blir kommunisert ut på en slik måte at de ansatte forstår og klarer å ta innover seg risikoene med det arbeidet som de utfører. Dersom de ansatte ikke har samme forståelse for de risikoene som eksisterer kan det medføre at de ikke tar hensyn til de risikoene i deres daglige arbeid. En annen faktor som kan påvirke informantenes forståelse er tillit til systemene. Siegrist (2000) og Siegrist et al. (2000) påpeker at dersom ekspertene deler likt verdisyn med lekfolket vil dette påvirke tiltroen som lekfolket har til ekspertene. I analysen ser man at mellomlederne og rådgiverne har tillit til systemene, og stoler på at systemene skal sikre banken mot uønskede hendelser. Dette kan føre til at man tar usikre beslutninger, noe som igjen kan medføre sårbarheter som trusselagenter kan utnytte. På en annen side sier rådgiverne at uønskede hendelser kommer av svakheter i systemene, noe som tyder på at de rådgiverne legger ansvaret for sikkerheten over på sikkerhetsavdelingen og systemene.

I tillegg nevner NOU (2015:13) at bedrifter må inneha systemer og rutiner som er med på å forebygge og håndtere uønskede IKT-hendelser, og er av betydning for å oppnå tillit fra brukerne. Når kundene har tillit til banken, kan dette bidra til at de er mindre kritisk til risikoer som teknologien kan innebære. I henhold til kundetillit, ser man at dette har en stor betydning for banknæringen, noe som også kan påvirke de ansattes arbeid med å ivareta kundeforholdet.

6.2 Hvilke faktorer er nødvendige for å opprettholde god informasjonssikkerhet?

Som en del av forskningen er det valgt belyse faktorer som er nødvendige for å opprettholde god informasjonssikkerhet, og om banknæringen oppfyller disse faktorene. Med dette er det fokusert på faktorer som, rutiner og håndbøker, kommunikasjon og rapporteringskultur.

6.2.1 En sikkerhetskultur preget av læring, rutiner og håndbøker

I henhold til Reason (1997) er sikkerhetskulturen en avgjørende faktor for et proaktivt sikkerhetsarbeid. Dermed kan det tenkes at uønskede hendelser i form av cyberangrep på informasjonssikkerhetssystemene oppstår ved at en virksomhet ikke har en felles oppfatning av viktigheten med sikkerhet, og en felles tro på forebyggende tiltak. Sikkerhetskulturen fremstår som veldig god i bankene som er blitt intervjuet. Dette er noe som informantene selv påpeker, og det kommer frem at banknæringen har lange tradisjoner, der sikkerhet har vært i fokus for å sikre kundeinformasjon og deres verdier. Samtidig har banknæringen vært gjennom store endringer da verdiene i banken i dag ikke består av fysiske elementer som mennesker, papirer og valuta, men informasjon som er lagret på nett. Dermed har arbeidsoppgavene til bankansatte endret seg fra å være fysisk dialog med kunden, til å være kommunikasjon over nett og gjennom applikasjoner som bankene tilbyr. Dette kan skape utfordringer for hvordan de ansatte forstår og jobber mot å sikre informasjon.

Det kommer ikke klart frem i intervjuene hvordan digitaliseringen har påvirket de ansatte og deres arbeidsoppgaver. Likevel er det en av mellomlederne som sier at arbeidsoppgavene endrer seg gradvis, men at dette ikke er noe de tenker over. På bakgrunn av dette kan det tenkes at de ansatte ikke reflekterer over hvilke utfordringer digitaliseringen fører med seg, og at de kanskje henger etter når det kommer til sikring av informasjon i digitale systemer. Selv om dette ikke er noe informanten selv påpeker tolkes det som at informanten ikke har opplevd noen vesentlige endringer i hvordan de sikrer informasjon, men med tanke på de store endringene banknæringen har vært gjennom de siste årene, burde disse endringene vært tydeligere. Dersom dette er tilfellet kan det tenkes at banknæringen ikke er godt nok forberedt til å håndtere fremtidige angrep rettet mot informasjon.

6.2.2. Kunnskap og kommunikasjon påvirker sikkerhetskulturen

For å opprettholde og sikre god informasjonssikkerhet, er det flere faktorer som er nødvendige, blant annet: god sikkerhetskultur, lover og retningslinjer, verdivurderinger, brukerveiledninger, rutiner, brannmurer og systemer som er egnet til å holde på informasjon (NOU 2015:13). Når det kommer til hvilke faktorer informantene mener må til for å opprettholde en god sikkerhetskultur, ser man noen ulikheter i deres besvarelser.

Informasjonssikkerhetslederne sier at det er i hovedsak læring og deling av kunnskap som må til for å sikre god sikkerhetskultur. Dette samsvarer med noen av de faktorene som Reason (1997) fremhever som viktige for en god sikkerhetskultur. Ut i fra besvarelsene til de ulike informantene får man først et inntrykk av at sikkerhetskulturen i bankene bygger på en felles forståelse av hva som skal til for å sikre en god informasjonssikkerhetskultur. Det nevnes blant annet faktorer som, læring og deling av kunnskap, forhindre taus kunnskap, en god sikkerhetsavdeling/ IT-avdeling, at alle må være sammen om det, samt kommunikasjon og rutiner. Med andre ord får man et inntrykk av at det beror en god forståelse og sikkerhetskultur. Det er først når samtalene utvikler seg, at man oppdager mulige mangler og svikt, som kan tyde på at dette kun er det ytre bildet av kulturen innad organisasjonen. Blant annet nevnes det i bank C at dette er faktorer som er på plass, men at det ikke er sikkert at dette gjelder alle bankene i distriktet. Med tanke på at informant C er informasjonssikkerhetsleder for alle bankene i distriktet informanten referer til, oppfattes derfor dette som et avvik ut i fra det de først søkte å formidle. Dette tyder på at sikkerhetskulturen varierer i de ulike bankene som informanten har ansvar for. Samtidig uttrykker mellomlederen i den samme banken, at informanten ikke vet nøyaktig hva som skal til for å sikre god informasjonssikkerhetskultur. Med dette forstår kan man forstå det slik at sikkerhetskultur ikke er noe som blir fokusert på i denne banken, og det kan derfor tenkes at sikkerhetskulturen ikke er så god som den først fremstilles. Igjen, ser man et avvik fra det som man i et teoretisk bilde fremmer som en god informasjonssikkerhetskultur (Snyman & Kruger, 2017).

Mellomlederne fokuserer på andre faktorer enn ekspertene når det kommer til god sikkerhetskultur. I denne sammenheng blir blant annet, felles lokaler, stort kundefokus og fokus på de regulatoriske kravene fremhevet. Med dette ser man at det er flere ulike faktorer som blir vurdert som betydningsfulle for sikkerhetskulturen. I intervjuene med rådgiverne fra bank A er det en av informantene som viser til at banken har sine krav og regler som de må følge for å sikre en god sikkerhetskultur. Med dette kan det tolkes som at lederne i banken ikke bidrar til en god sikkerhetskultur, utover det som de er pålagt. Dette bygges opp av den andre informanten fra samme bank som sier at det er fokus på en god sikkerhetskultur, samtidig uttrykker informanten at sikkerhetskulturen kunne vært mye verre. Med dette kan det forstås som at informanten er tilfreds med sikkerhetskulturen, siden den kunne vært verre. Samtidig er det ingen av de to informantene som viser til hva som gjør sikkerhetskulturen god, og man kan forstå det som at det ikke er et fokus på å heve sikkerhetskulturen ytterligere. De tre andre rådgiverne trekker frem en god sikkerhetskultur preget av samarbeid og åpen dialog. Dermed

kan det tenkes at det er forskjeller i hvordan de ulike bankene jobber mot å sikre en god sikkerhetskultur, og hva som er viktig for de ulike informantene. Det en kan merke seg er dog at ingen av mellomlederne eller rådgiverne nevner sikkerhetsbevissthetsprogrammer som en medvirkende faktor for å styrke sikkerhetskulturen.

Alle informantene trekker frem at ledelsen har en viktig rolle, for å sikre at det er en lik oppfatning av hva som er viktig. Reddick (2009) fremhever innflytelse fra ledelsen som en viktig faktor innen en virksomhet når det kommer til informasjonssikkerhet, der han blant annet peker på at ledelsens rolle og fokus vil kunne ha en innvirkning på hvordan ansatte i virksomheten forstår og arbeider med informasjonssikkerhet. I intervjuene kommer det frem at det er noe ulik forståelse for hvilke trusler som er aktuelle, deriblant er informasjonssikkerhetslederne og mellomlederne av samme oppfattelse da de er mest bekymret for intenderte angrep og menneskelig svikt, men rådgiverne er mer bekymret for teknisk svikt og eksterne angrep. Dette kan komme av manglende innflytelsen og kommunikasjon fra ledelsen, noe som kan føre det til ulik forståelse og med det føre til en svekket sikkerhetskultur.

Reason (1997) påpeker at læring er en viktig faktor for sikkerhetskulturen, der en lærende kultur vil være villig til å samle inn, analysere og formidle informasjon fra hendelser. Dette er også noe som fagekspertene uttrykker som en vesentlig faktor for å unngå større uønskede hendelser (NOU 2015:13). Relatert til dette forteller informant D at kundefokuset er så stort i deres bank at det går utover sikkerhetskulturen ved at de glemmer å inkludere de ansatte ved uønskede hendelser, og trekker frem at kunnskapsdeling burde vært en større del av deres sikkerhetskultur. Således ser man at selv om informantene fremstiller sikkerhetskulturen som svært god i banknæringen, er det likevel noen funn som tyder på at sikkerhetskulturen kunne vært bedre. Gjennom intervjuene forstår man det slik at banknæringen benytter sikkerhetsbevissthetsprogrammer for å øke kunnskapsnivået til de ansatte. Sikkerhetsbevissthetsprogrammene består av e-læringsmoduler, rutiner, regler, håndbøker og intranett. Samtidig påpeker Furnell og Thomson (2009) at et for vidt fokus på sikkerhet, utover det som er relevant for de ansatte, kan føre til sikkerhetsutmattelse. I lys av denne teorien, sier flere informanter at de ikke alltid følger de aktuelle rutinene, og det viser seg at de har liten kjennskap til nye regelverkene. Dette på tross av at informasjonssikkerhetslederne forteller at de ansatte skal ha vært gjennom en e-læringsmodul som går nettopp på dette med de nye regelverkene. I denne studien har man ikke hatt innsyn i hva som formidles gjennom e-læringsmodulene, men flere av informantene tar for eksempel opp dette med GDPR og at de

skal ha vært gjennom en e-læringsmodul vedrørende denne. Likevel er det flere av informantene som sier at de ikke har god kjennskap til loven, og hva den vil innebære for dem og deres arbeidsoppgaver. Med dette forstås det slik at e-læringsmodulen ikke har oppnådd sin hensikt, som er å forberede de ansatte på det nye kravet som også vil gjelde for de når det blir iverksatt. Dette kan få følger for læringen internt i virksomhetene, siden de ansatte ikke vil få et utbytte av e-læringsmodulene dersom de ikke forstår og reflekterer over innholdet. Toshou et al. (2015) påpeker at sikkerhetsbevissthetsprogrammene ofte mislykkes fordi virksomheten ikke klarer å tilpasse programmene i forhold til personalet som skal bruke dem. Det som viser seg interessant er om e-læringene er tilpasset de ansatte på en slik måte at de klarer å ta innover seg innholdet. I tillegg forstår man det slik at de ansatte heller ikke forstår viktigheten av å følge rutinene, siden de selv påpeker at de ofte glemmer å følge rutinene på enkelte områder.

Bevisstgjørelse er en av de tre faktorene som Furnell og Clarke (2005) peker på for å oppnå en god sikkerhetskultur. I tillegg trekker Furnell og Clarke (2005) frem trening og undervisning som viktige elementer som påvirker sikkerhetskulturen. I forbindelse med dette er det ingen av informantene som trekker frem trening som en faktor utover bevissthetsprogrammene, og som vist tidligere i avsnittet ser det ut til at disse ikke er tilstrekkelige for å øke kunnskapen og bevisstheten blant de ansatte. Dermed kan det tenkes at bankene må revidere disse programmene, slik at de kan utnyttes best mulig.

6.2.3 En rapporteringskultur preget av underrapportering

I henhold til IKT-forskriften skal alle alvorlige hendelser rapporteres, likevel er det registrert underrapportering i banknæringen. Dette kan henge sammen med at digitale hendelser ikke er forklart og tatt opp på en tilstrekkelig måte i lovverket og forskriftene (NOU 2015:13). I henhold til NSM (2015) vil mangelfull rapportering av alvorlige IKT-hendelser kunne svekke evnen til forbedring og læring innen det forebyggende arbeidet med IKT-sikkerhet. Gjennom intervjuene forteller de fleste informantene at underrapportering er noe som jobbes mye med, og at de søker å ha en kultur der de ansatte føler de kan komme å fortelle om hendelser. Likevel er det, som nevnt tidligere, underrapportering i banknæringen. Dermed er det interessant å se på hvorfor det er slik. Det kan tenkes at det ikke oppfordres til rapportering i like stor grad som informantene gir uttrykk for. Dette kan henge sammen med at en av mellomlederne forteller at rapportering fører med seg mye ekstra arbeid, da det er mye papirer som må fylles ut. Det kan også tenkes at de ansatte er redde for hvilke konsekvenser det kan få for de om de rapporterer hendelser, altså at de opplever negative konsekvenser. Reason (1997) sier at det er viktig å ha

et tydelig skille mellom akseptabel og ikke-akseptabel oppførsel for å opprettholde troverdighet hos de ansatte. I følge flere av informantene er rapporteringskulturen i stor grad preget av subjektive holdninger, der det ikke er et tydelig skille i forhold til hva som bør rapporteres og ikke. Dermed kan det tenkes at de som opplever uønskede hendelser tenker at det ikke er så alvorlig, og at man derfor ikke trenger å rapportere hendelsen. Dette kan få følger for sikkerheten i bankene, dersom de som jobber lengre opp i systemet ikke får et reelt risikobilde av faktiske forhold i virksomheten. Dermed bør muligens bankene ha tydeligere rammer for hva som skal rapporteres, og med dette oppmuntre til rapportering av alle hendelser uavhengig av størrelse.

NOU (2015:13) viser til at underrapportering kan henge sammen med frykten for å ødelegge bedriftens omdømme. Samtlige informanter har sagt at de lever av kundens tillit. Dermed kan det tenkes at dersom en bank blir utsatt for en uønsket hendelse som blir kjent for alle, kan det medføre at kundene velger en annen bank, grunnet mangel på tillit. Ut ifra det informant A sier, at de ikke opplever noen underrapportering, kan henge sammen med at informanten frykter at dette skal bli kjent blant kunder eller potensielle kunder, og på den måten svekke deres renommé. Reason (1997) viser på sin side til at underrapportering kan komme av at det ikke eksisterer en rettferdig kultur. Dette er ikke noe som blir tatt opp av informantene, men siden det er vist at der er underrapportering kan det tenkes at frykt for konsekvensene er en av grunnene til at underrapportering eksisterer. Informantene på ledelsesnivå påpeker som tidligere nevnt, at menneskelig svikt er ansett som en av de største sårbarhetene i banknæringen. Denne holdningen kan være en årsak til at bankene opplever underrapportering, selv om informantene selv påpeker at de ikke er ute etter å henge ut noen, eller ute å ta noen, kan det tenkes at dette oppleves annerledes av rådgiverne som skal utføre rapporteringen. I forbindelse med dette viser Dekker (2006) til "*the old view*", der virksomhetene har fokus på menneskelig svikt, og mener at systemene i seg selv er sikre nok, noe som skaper utfordringer for sikkerheten. I denne sammenheng kan det se ut til at ledelsen praktiserer "*the old view*", siden de viser til menneskelig svikt som en av de største risikoene. Dette kan føre til sårbarheter i systemene, siden hovedfokuset er menneskene og man ser ikke på de underliggende faktorene til at menneskelige feil oppstår.

7. Konklusjon

I takt med økt digitalisering er informasjon blitt enda viktigere å sikre. Banknæringen står overfor flere endringer som kan få konsekvenser for sikring av konfidensialitet, integritet, og tilgjengelighet av informasjon. På bakgrunn av endringene som rammer banknæringen, og sikring av informasjon har hensikten med denne studien vært å belyse hvordan banknæringen jobber med å sikre informasjon, og hvordan de ansatte forstår informasjonssikkerhet. Det er flere faktorer som har vist seg å være av betydning for å sikre god informasjonssikkerhet. Både med tanke på hvordan de ansatte jobber for å sikre informasjon, og hvordan deres forståelse spiller en viktig rolle i sikkerhetsarbeidet. Fire banker er benyttet som case. Dermed er utvalget for lite til å kunne generaliseres for hele bransjen. Funnene anses likevel som relevante for den øvrige banknæringen, med tanke på at informasjons er en viktig verdi for hele sektoren. Følgende problemstilling er lagt til grunn:

Hvordan forstår og jobber banknæringen for å møte risikoen for uønskede hendelser i forbindelse med informasjonssikkerhet?

Risikostyring i bankene bygger blant annet på retningslinjene gitt i regelverkene, men på bakgrunn av manglende innsikt i metodene og prosessene har det ikke vært mulig å vurdere kvaliteten på risikostyringen. Likevel ser man at når det kommer til kommunikasjon og inkludering, og integrering, er det noen svakheter som kan medføre negative konsekvenser for den helhetlige risikostyringen. Bankene benytter kommunikasjonssystemer, men de benyttes i stor grad til enveiskommunikasjon. Når det kommer til inkludering burde de ansatte i større grad vært inkludert i utarbeidelsen av ROS-analyser. Ved å inkludere de ansatte vil man sannsynligvis få et bredere bilde av hvilke risikoer og sårbarheter som de ansatte står overfor når de behandler informasjon. I tillegg kan det tenkes at mellomledernes og rådgivernes erfaring og kunnskap skiller seg fra informasjonssikkerhetslederne. Med det vil man sikre at ROS-analysene baserer seg på ulik kompetanse og erfaring. På bakgrunn av manglende kommunikasjon og inkludering, samt integrering, kan det forekomme svakheter i det totale sårbarhetsbildet i banken. Dette er noe som bankene bør ha mer fokus på i fremtiden for å sikre en enda bedre sikkerhet i bankene.

Når det kommer til hvordan de ansatte i banknæringen forstår informasjonssikkerhet ser man at mellomlederne og rådgiverne har en annen forståelse for hva informasjonssikkerhet betyr

sammenlignet med informasjonssikkerhetslederne. Dette er noe som er helt naturlig med tanke på den ulike kunnskapen, interessen og erfaringene som eksisterer på de ulike nivåene. Likevel ser man at når det kommer til hvilke risikoer som de ansatte anser som relevante er det store forskjeller. Dette kan bidra til at rådgiverne som jobber direkte med informasjon ikke har samme forståelse for hvilke risikoer man skal være oppmerksomme på. For at ansatte i banknæringen skal være i stand til å forstå og arbeide målrettet mot uønskede hendelser på deres informasjonssystemer, bør det være større fokus på de organisatoriske faktorene. Banknæringen har allerede iverksatt flere tiltak for å inkludere og kommunisere med de ansatte, herunder skriftlig informasjon via intranett, rutiner og håndbøker, samt sikkerhetsbevissthetsprogrammer. Likevel ser man at dette ikke utnyttes tilstrekkelig da det ser ut til at de ansatte ikke oppnår tilstrekkelig læring av e-læringsmodulene. Dette ser man eksempelvis i forbindelse med GDPR, da mellomlederne og rådgiverne har liten eller ingen kjennskap til hva GDPR inneholder. Dette på tross av at de har hatt e-læringsmoduler, som er ment å forberede de ansatte til endringene personvernloven vil medføre for deres arbeidsoppgaver og håndtering av personopplysninger. Således kan det tenkes at ved å innføre toveiskommunikasjon og refleksjonsgrupper, kan det medføre økt kunnskap blant de ansatte, en felles forståelse for hvilke risikoer som er aktuelle, samt hvordan man kan sikre informasjon mot eksterne angrep og menneskelig svikt.

Både gjennom intervjuene og dokumentene som er anvendt fremkommer det at phishing er en av de største truslene mot informasjonssikkerhet. Derfor er det formålstjenlig å inkludere kundene, for å gjøre dem oppmerksom på hvilke trusler som er rettet direkte mot dem. Ved å iverksette tiltak rettet mot kundene om hvordan man kan sikre seg selv mot slike angrep, kan man anta at flere av phishingangrepene kunne vært unngått. I tillegg ser man også at mellomlederne og rådgiverne har stor tillit til ekspertene og systemene, noe som kan føre til at de tar usikre beslutninger i forbindelse med behandling av kundeinformasjon. Dermed bør bankene ha et større fokus på at systemene og ekspertene alene er ikke nok for å sikre informasjon, men at det er en kombinasjon av både de organisatoriske og de tekniske forholdene. Med det kan man redusere antall hendelser i forbindelse med menneskelig svikt. I tillegg har innføringen av de nye lovkravene vist seg som svært interessant, da det ikke ser ut til at næringen er godt nok forberedt til å håndtere disse, noe som kan tenkes å gjelde utover banknæringen. Dette kan medføre sårbarheter i informasjonssystemene, og svekke sikkerheten i virksomhetene. I tillegg kan det medføre store bøter for virksomhetene, noe som i verst tenkelig utfall kan medføre konkurs (Moe, 2018).

7.1 Forslag til videre forskning

Det er enkelte forhold som ikke blir tilstrekkelig ivaretatt i dette studiet, og som hadde vært interessant å studere mer i dybden. I denne studien er det fokusert på de organisatoriske faktorene som påvirker risikostyringsprosessen, men det hadde vært interessant å sett hvordan de faktisk evaluerer risiko. I tillegg benytter de fleste norske bankene seg av Evry som skal ivareta blant annet sikkerheten i betalingssystemene som bankene tilbyr kundene. Dermed hadde det vært interessant hvordan samarbeidet mellom bankene og Evry er, og i hvilken grad bankene er kjent med hvordan Evry sikrer informasjon de besitter om bankene.

Det kunne også vært interessant å sett på hvordan innføringen av PSD2 påvirker banknæringen, og dens sikring av informasjon i fremtiden. En slik studie hadde vært spennende siden regelverkene medfører flere aktører på markedet som kan benytte seg av bankenes infrastruktur. I tillegg til økt konkurranse og flyt av informasjon.

I denne forskningen er det ikke tatt hensyn til de europeiske bankene. Derfor kan det være interessant å ta forskningen videre med på et internasjonalt nivå, der man vurderer bankenes samarbeid i andre land. I tillegg kan man se på hvordan bankene sikrer informasjon som kan utnyttes av andre vedkommende til egen gevinst, og hvorvidt kulturelle forskjeller har noen innflytelse på denne prosessen.

8. Litteraturliste

Aven, T. (2007) *Risikostyring: Grunnleggende prinsipper og ideer.* Oslo, Universitetsforlaget

Aven, T. (2015). Risikostyring: *Grunnleggende prinsipper og ideer.* Oslo, Universitetsforlaget

Aven, T., Boyesen, M., Njå, O., Olsen, K.H. & Sandve, K. (2004) *Samfunnssikkerhet.* 3. utgave. Oslo, Universitetsforlaget.

Aven, T. & Renn, O. (2010). *Risk Management and Governance: Concepts, Guidelines and Applications*. Springer Berlin Heidelberg: Imprint: Springer

Beck, U., Giddens, A. & Lash, S. (1994). *Reflexive modernization: Politics, tradition and aesthetics in the modern social order.* Cambridge: Polity Press.

Berg, F.R. (2012). *Risiko og sårbarhet i IKT-systemene i finanssektoren.* Universitetsforlaget. Praktisk Økonomi & Finans, Vol.28. s.37-48

Beierle, T.C. (2000). *The quality of stakeholder-based decisions: Lessons from the Case Study Record*. Hentet fra: https://ageconsearch.umn.edu/bitstream/10686/1/dp000056.pdf

Blaikie, N. (2010). *Designing social research.* Cambridge: Polity Press.

Brinkmann, S. & Kvale, S. (2009). *Det kvalitative forskningsintervju.* Oslo: Gyldendal Norsk Forlag AS.

Camillo, M. (2016): Cybersecurity: *Risks and management of risks for global banks and financial institutions.* Henry Stuart Publications. Vol. 10, 2. Journal of Risk Management in Financial Institutions. Hentet fra: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/jrmfi-mark-camillo-article-mar-2017.pdf

Charley, S. & Engelbert, B. (2005). *Evaluating public participation in environmental decision-making: EPA's superfund community involvement program.* Hentet fra: http://people.uncw.edu/imperialm/UNCW/PLS_506/superfund_eval.pdf

Chen, Y. K. Ramamurthy & K. W. Wen. (2014). *"Organizations' Information Security Policy Compliance: Stick or Carrot Approach?"* Journal of Management Information Systems, 29 (3): 157–188. Winter 2012–13. Hentet fra: http://www.tandfonline.com/doi/abs/10.2753/MIS0742-1222290305

Christensen, Clayton. M. (1997). *The innovator's dilemma: when new technologies cause great firms to fail.* Harper Business Essensials, New York

COSO. (2004). *Helhetlig risikostyring - et integrert rammeverk. Sammendrag Rammeverk.* Committee of Sponsoring Organizations of the treadway Commission, % AICPA. Jersey City, NJ 07311-3881, USA.

Datatilsynet (2016). *EUs personvernreform.*. Hentet fra: https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/eus-personvernreform-/

Da Veiga, A., and N. Martins (2015). *"Improving the Information Security Culture Through Monitoring and Implementation Actions Illustrated Through a Case Study."* Computers & Security 49: 162–176. Hentet fra: https://ac.els-cdn.com/S0167404814001862/1-s2.0-S0167404814001862-main.pdf?_tid=cfae2590-170c-11e8-b115-00000aab0f6b&acdnat=1519220623_a35df936747625724a223dbe646f5236

Dekker, S. (2006). *The Field Guide to Understand Human Error.* Lund University, Sweden: Ashgate

Denning, S. (2014). Can Banks Master Disruptive Innovation? Hentet fra https://www.forbes.com/sites/stevedenning/2014/12/05/innotribeswift-can-banks-master-disruptive-innovation/#4c4d05ba580a

Dhillon, G. R. Syed & C. Pedron (2016). *"Interpreting Information Security Culture: An Organizational Transformation Case Study."* Computers & Security 56: 63–69. Hentet fra: https://www.sciencedirect.com/science/article/pii/S016740481500139X

Direktoratet for forvaltning og ikt - Difi (2013). *Hva er ISO/ IEC 27001?* Hentet fra: http://internkontroll.infosikkerhet.difi.no/hva-sier-isoiec-27001

Direktoratet for samfunnssikkerhet og beredskap (2012). *Nasjonalt risikobilde 2012.* Hentet fra: https://www.dsb.no/rapporter-og-evalueringer/nasjonalt-risikobilde-2012/

Direktoratet for samfunnssikkerhet og beredskap (2014). *Nasjonalt risikobilde 2014.* Hentet fra: https://www.dsb.no/rapporter-og-evalueringer/nasjonalt-risikobilde-2014/

Earle, T.C. & Siegriest, M. (2008). *On the relation between trust and fairness in environmental risk management.* Hentet fra: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6924.2008.01091.x

Engen, O.A., Kruke. B.I., Lindøe, P.H., Olsen, K.H., Olsen, O.E., Pettersen, K.A., (2016). *Perspektiver på samfunnssikkerhet.* Livonia Print SIA, Latvia: Cappelen Damm.

Evry (uå). *PSD2 – Strategic opportunities beyond compliance.* Hentet fra: https://www.evry.com/globalassets/bransjer/financial-services/bank2020/wp_psd2/psd2_whitepaper.pdf

Frewer, L. (2004). *The public and effective risk communication. Toxicology Letters 149, 391–397. doi:10.1016/j.toxlet.2003.12.049*

Fukuyama, F. (1996). *Trust: The Social Virtues and the Creation of Prosperity.* London, UK: Penguin Books.

Furnell, S. & Clarke, N. (2005). *Organisational Security Culture: Embedding Security Awareness, Education and Training.* Network Research Group, School of Computing, Communications and Electronics, University of Plymouth, Plymouth, United Kingdom. Hentet fra: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.678.9294

Furnell, S. & Thomson, K.L. (2009). *From culture to disobedience: Recognising the varying user acceptance of IT security.* Hentet fra: https://www.sciencedirect.com/science/article/pii/S1361372309700193

Giovannetti, E., Kagami, M., & Tsuji, M. (2003). The Internet revolution: a global Perspective. Cambridge University Press.

Grimen, H. (2009). *Hva er tillit.* Oslo: Universitetsforlaget.

Guo, K. H., Y. Yuan, N. P. Archer, and C. E. Connelly. (2011). *"Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model."* Journal of Management Information Systems 28 (2): 203–236. Hentet fra: http://www.tandfonline.com/doi/pdf/10.2753/MIS0742-1222280208?needAccess=true

Hannemyr, G. (2015). *Digitale medier: teknologi, anvendelser, samfunn* (3. utg.). Universitetsforlaget.

Hong, K., Chi, Y., Chao. L. R. & Tang, J. (2003). *An integrated system theory of information security management.* 11(5), 243-248. doi: 10.1108/09685220310500153

Hylland-Eriksen, T. (2005). *Internett i praksis: om teknologiens uregjerlighet.* Scandinavian Academic Press.

IKT-systemer. (2003). Forskrift om bruk av informasjons- og kommunikasjonsteknologi m.v. av. 7. desember 1956 nr. 1. Hentet fra https://lovdata.no/dokument/SF/forskrift/2003-05-21-630?q=ikt

Internkontrollforskriften (1996) Forskrift om systematisk helse- og miljø- og sikkerhetsarbeid i virksomheter m.v. av. 4. februar 1977 nr. 4. Hentet fra https://lovdata.no/dokument/SF/forskrift/1996-12-06-1127?q=internkontroll

ISACA (2018). *What is COBIT 5?* Hentet fra: http://www.isaca.org/cobit/pages/default.aspx

Jacobsen, D. I. (2010). *Forståelse, beskrivelse og forklaringer.* Kristiansand: Høyskoleforlaget.

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

Johnsen,W. L. G. (2009). *Risikovurdering. Praktisk risiko- og sårbarhetsanalyse i virksomheter.* Oslo: Gyldendal Norsk Forlag AS.

Kraemer, S. & Carayon, P. (2006). *Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists.* Hentet fra: *https://ac.els-cdn.com/S000368700600041X/1-s2.0-S000368700600041X-main.pdf?_tid=3bff5a36-664e-4a27-80b6-c69fd659f3de&acdnat=1528876684_bf67e1f1c8987111bafb600694fbd1d2*

Leveson, N. (2011). *Engineering a safer world: systems thinking applied to safety.* London, MIT Press.

Lincoln, Y. S. og Guba, E. G. (1985). *Naturalistic Inquiry*. California: Sage Publications

Lorch-Falch, S. (2014, 19.10). Finans Norge tror Norge i praksis er kontantfritt innen fem år. E24. Hentet 31.02.18 fra http://e24.no/article/23315341

Lorentzen, M. (2016). Landets tredje største sparebank kutter 100 årsverk: – En digitalisering vi ikke har sett maken til. E24. Hentet 01.02.18 fra http://e24.no/article/23608259

Löfstedt, R.E. (2003). *Risk communication: Pitfalls and promises.* European Review 11, no. 3: 417–35. Hentet: https://www.cambridge.org/core/journals/european-review/article/risk-communication-pitfalls-and-promises/0786AEEEE569C62AB45AC36F0B8FA4BF

Mehta, R. (2017). One in three cyber attacks in banks are successful: Report. Hentet fra: https://economictimes.indiatimes.com/industry/banking/finance/banking/one-in-three-cyber-attacks-in-banks-are-successful-report/articleshow/58396453.cms

Moe, S. (2018). *Fire av ti selskaper ikke klare for ny lov.* Hentet fra: https://e24.no/lov-og-rett/personvern/fire-av-ti-selskaper-ikke-klare-for-ny-lov-konsekvensen-kan-bli-erstatningssoeksmaal-og-gebyr-i-millionklassen/24283489

Njå, O., Solberg, Ø. & Braut, G.S. (2017). Uncertainty - it´s ontological status and relation to safety. In Motet, G. & Bieder, C. (red.), *The illusion of risk control: What would it take to live with uncertainty?* Cham: Springer.

Norges Bank (2017). *Finansiell infrastruktur.* Hentet fra: https://static.norges-bank.no/contentassets/0af5e6ca88d54c7ca6ab9cd8b44257c8/finansiell_infrastruktur_2017.pdf?v=05/18/2017145640&ft=.pdf

NOU 2012:10. (2012). *Nasjonalstrategi for informasjonssikkerhet.* Hentet fra: https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

NOU 2015:13. (2015). *Digital sårbarhet - sikkert samfunn.* Hentet fra: https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

NOU 2016:19. (2016). *Samhandling for sikkerhet — Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* Hentet fra: https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/

NSM (2015). *Nasjonal sikkerhetsmyndighet.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2015-web.pdf

NSM (2017). *Risikoer og sårbarheter i en ny tid.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf

Personopplysningsloven. (2001). Lov om behandling av personopplysninger m.v. av 1 januar 2001. Hentet fra https://lovdata.no/dokument/NL/lov/2000-04-14-31?q=personopplysningsloven

Pidgeon, N.F, Poortinga, W., Rowe, G., Jones, T.H., Walls, J. & O´Riodan, T. (2005). *Using Surveys in Public Participation Processes for Risk Decision Making: The Case of the 2003 British GM Nation? Public Debate.* Hentet fra: https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1539-6924.2005.00603.x

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H. & Pahnila, S. (2004). *Consumer acceptance of online banking: an extension of the technology acceptance model. Internet Research, 14(3), 224–235.* http://doi.org/10.1108/10662240410542652

Rahima, S., Mahatb F., Nassirb, A., Yahyab, M. (2015) Re-thinking: Risk Governance? International avvounting and business conference. IABC. S.689-698 Hentet fra (15.02.18): https://ac.els-cdn.com/S2212567115011570/1-s2.0-S2212567115011570-main.pdf?_tid=71442962-1245-11e8-a715-00000aacb360&acdnat=1518695198_326b3288abc0b7b22f1bea5e765aca5b

Rausand, M. & Utne, I. B. (2009). *Risikoanalyse - teori og metoder*. Trondheim: Tapir Akademiske Forlag

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

Reddick, C. G. (2009). *Management support and information security: an empirical sudy of Texas state agencies in USA.* ss. 361 - 377.

Renn, O. (2008) *Risk Governance. Coping with uncertainty in a Complex World.* London. Earthscan

Siegrist, M. (2000). The influence of Trust and Perceptions of Risk and Benefits on the Acceptance of Gene Technology. *Risk Analysis, Vol. 20, No.2.* Hentet fra: http://onlinelibrary.wiley.com/doi/10.1111/0272-4332.202020/epdf

Siegrist, M. Cvetkovich, G. & Roth, C. (2000). *Salient Value Similarity, Social Trust, and Risk/Benefit Perception*, 20 (3), 353-362. DOI*:* 10.1111/0272-4332.203034

Sjøberg, L. & Drottz-Sjøberg, B. M. (2001) *Fairness, risk and risk tolerance in the sitting of a nuclear waste repository*. Journal of Risk Research, Vol 4, s. 75-101

Skuterud, E. (2003). *Sikring av forretningskritiske systemer*. Hentet fra: https://www.magma.no/sikring-av-forretningskritiske-systemer

Slovic, P. (1999). *Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield.* Risk Analysis, Vol. 19, No.4 (1999). Hentet fra: https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1539-6924.1999.tb00439.x

Slovic, P. & Peters, E. (2006). *Risk Perception and Affect.* doi: 10.1111/j.1467-8721.2006.00461.x

Snyman, D. & Kruger, H. (2017) "*The application of behavioural thresholds to analyse collective behaviour in information security."* Information & Computer Security, Vol. 25 Issue: 2, pp 152-164. Hentet fra: https://doi.org/10.1108/ICS-03-2017-0015

Soomro, A. Zahoor., Shah, H., Mahmood. & Ahmed, J. (2016). *Information security management needs more holistic approach: A literature review. International journal of information management, 36(2), 215-225. doi:10.1016/j.ijinfomgt.2015.11.009*

Stirling, A. (2007). *"Opening Up" and "Closing Down" Power, Participation, and Pluralism in the Social Apprasial of Technology*. Science, Technology, & Human Values, 33(2), 262-294. *doi: 10.1177/0162243907311265*

Sviggum, S. (2017). *Finanstilsynets funn fra tematilsyn innen operasjonell risiko er nå tilgjengelig.* Hentet fra: http://blogg.pwc.no/finansbloggen/finanstilsynets-funn-fra-tematilsyn-innen-operasjonell-risiko-er-n%C3%A5-tilgjengelig

Thagaard, T. (2013). *Systematikk og innlevelse.* Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Tsohou, A., Karyda, M., Kokolakis, S. & Kiountouzis, E. (2015). *Managing the introduction of information security awareness programmes in organisations.* Hentet fra: https://www-tandfonline-com.ezproxy.uis.no/doi/abs/10.1057/ejis.2013.27

Ula, M., bt Ismail. Z., Sidek. M. (2011). *A framework for the Governance of Information Security in Banking Systems.* doi: 10.5171/2011.726196

van Asselt, M.B.A. & Renn, O. (2011). *Risk governance*. Journal of Risk Research, 14:4, 431-449. Hentet fra: https://doi.org/10.1080/13669877.2011.553730

von Solms, R. & van Niekerk, N. (2013). *From information security to cyber security.* doi: 10.2016/j.cose.2013.04.004

WEF (2015). *The Global Competitivness Report 2015-2016.* Hentet fra: http://www3.weforum.org/docs/gcr/2015-2016/Global_Competitiveness_Report_2015-2016.pdf

Yildirim, E.Y., Akalp, G., Aytac, S. and Bayram, N. (2011). "*Factors influencing information security management in small-and medium-sized enterprises: a case study from Turkey*", International Journal

of Information Management, Vol. 31 No. 4, pp. 360-365. Hentet fra: https://www.sciencedirect.com/science/article/pii/S0268401210001520

Yin, R. K. (2014). *Case Study Research. Design and methods.* California: Sage publications, California.

Vedlegg 1: Informasjonsbrev

Dagens samfunn er preget av store digitale endringer, noe som er med på å skape store muligheter for fremtidig drift og bruk av banktjenester. Samtidig vil dette føre med nye utfordringer og sårbarheter, som bør studeres nærmere. Vår masteroppgave innen studiet samfunnssikkerhet ved Universitetet i Stavanger omhandler informasjonssikkerhet i banknæringen. Med dette ønsker vi å intervjue informanter fra deres bank. Det er ønskelig å intervjue en informasjonssikkerhetsleder, en mellomleder og en rådgiver fra hver bank. Gjennom intervjuene ønsker vi å kartlegge hvordan informasjonssikkerhet blir ivaretatt i bankene, og hvilke tiltak dere gjør for å sikre informasjon.

Målet er å intervjue flere ulike banker for å se om det fellestrekk eller ulikheter i hvordan bankene sikrer informasjon, og hvilke faktorer som er av betydning for sikkerhetsarbeidet. Vi deler selvsagt våre funn med dere, noe som kan bidra til læring hos dere og. Dersom dere har kjennskap til noen andre vi kan intervjue setter vi pris på om dere kan sette oss i kontakt med dem. Alle bankene og informantene som deltar i studien vil anonymiseres, og dere kan få tilsendt intervjuguiden på forhånd slik at dere er forberedt på hva vi ønsker å snakke om. Vi håper på en positiv tilbakemelding, slik at vi kan sette en dato for en hyggelig og informativ samtale.

Med vennlig hilsen
Stine Ertenstein og Julia Slettemoen

Vedlegg 2: Samtykkeerklæring

I forbindelse med vår masteroppgave i samfunnssikkerhet ved Universitetet i Stavanger, skal vi gjennomføre flere intervjuer. Oppgaven omhandler informasjonssikkerhet i banknæringen. Formålet med studien er å belyse hvordan banknæringen jobber med å sikre informasjon, og hvordan de ansatte forstår informasjonssikkerhet. Intervjuene vil omhandle risikostyring, risikopersepsjon og sikkerhetskultur.

Konfidensialitet etterstrebes, og vi benytter NSD sine retningslinjer for oppbevaring av sensitive opplysninger. Under intervjuene er det ønskelig å benytte diktafon, slik at vi som gjennomfører intervjuene kan delta aktivt i samtalen uten å bli distrahert av å måtte ta notater. For å ytterligere sikre konfidensialitet vil informantene bli anonymisert ved å bli omtalt som "informant A", "informant B", og så videre. På denne måten sikrer vi at alle opplysninger vil bli behandlet anonymt og fortrolig. Om ønskelig har dere også muligheten til å godkjenne endelig tekst som benyttes i oppgaven før den leveres inn.

Ved å skrive under på denne erklæringen godtar du at alle opplysninger som blir gitt under intervjuet kan benyttes videre i oppgaven.

…… ……..

Stine Ertenstein Julia M. Slettemoen

Masterstudenter i samfunnssikkerhet

……....

Respondent

Vedlegg 3: Intervjuguide

Nr.	Spørsmål	Kommentar
Innledende		
1.	Hvor lenge har du jobbet her?	
2.	Hvor mange ansatte er dere?	
3.	Hva er gjennomsnittsalderen i organisasjonen?	
4.	Hvordan er kjønnsfordelingen av ansatte?	
5.	Hvilke arbeidsoppgaver har du?	
6.	Hvordan kommer dine arbeidsoppgaver i berøring med informasjonssikkerhet?	
7.	Er dere flere som jobber med informasjonssikkerhet?	
8.	Har du jobbet med informasjonssikkerhet tidligere? Hvis ja, hvilke ulikheter er det i hvordan dere jobber mot informasjonssikkerhet her sammenlignet med tidligere stillinger?	
Risiko- og sårbarheter		
9.	Hvordan kartlegger dere risiko- og sårbarheter?	
10.	Hva kan være en typisk kritisk hendelse i forhold til sensitiv kundeinformasjon på avveie?	
11.	Hva kan årsaken til slike hendelser?	
12.	Hvordan håndterer dere uønskede hendelser?	
13.	Hva kan være typiske tiltak?	
14.	Hvordan blir tiltakene fulgt opp?	

15.	Hva må til for å opprettholde god informasjonssikkerhet?	
16.	Har dere egne retningslinjer utover lovkravene som skal bidra til god informasjonssikkerhet?	
17.	Bruker dere underleverandører til deres banktjenester?	
18.	Er det ulik praksis i organisasjonen for hva og hvor mye som rapporteres?	
Risikoforståelse		
19.	Hvilke risikoer anser du som relevant for banknæringen? • Er dette noe du er redd for at skal ramme deres organisasjon? • Hvorfor/hvorfor ikke?	
20.	Hva legger du i begrepet informasjonssikkerhet?	
21.	Hvordan knytter du dette begrepet opp mot banknæringen?	
22.	Hvordan er samarbeidet med andre banker? og hvordan er samarbeidet på tvers i organisasjonen?	
23.	Hvordan påvirker hendelser deres risikoforståelse og barrierer mot sikkerhetsbrudd?	
Organisatoriske normer		
24.	Hvordan vil du definere organisasjonskulturen i deres bank?	
25.	Hvilke organisatoriske faktorer mener du er viktige for å oppnå god informasjonssikkerhet?	
26.	Hvordan motiveres du til å tenke sikkerhet ved behandling av sensitiv informasjon?	
27.	Hvordan motiverer du de andre ansatte til å tenke sikkerhet ved behandling av sensitiv informasjon?	
28.	Hvordan er samarbeidet med andre banker?	

29.	Hvordan er samarbeidet på tvers i virksomheten?	
30.	Rapporteres alle uønskede hendelser? • Hvordan håndterer dere rapporterte hendelser?	
31.	Hvordan blir tiltak og sikkerhetsrutiner formidlet til resten av organisasjonen?	
32.	Er det ulik praksis i organisasjonen for hva og hvor mye som rapporteres?	
Avsluttende		
33.	Er det noe mer du ønsker å legge til?	
34.	Kan vi komme tilbake til deg om det er noe vi lurer på?	

Ta kontakt hvis du lurer på noe.