Universitetet
i Stavanger

Cyberangrep mot bank og finans

Hvordan kan en bank som en organisasjon beskytte kundene deres mot cyberangrep?

Jeannett Hansen

Masteroppgave våren 2019

Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Samfunnssikkerhet	Vårsemesteret, 2019 Åpen
Forfatter: Jeannett Hansen	Jeannett Hansen
Fagansvarlig: Bjørn Ivar Kruke Veileder: Riana Steen	
Tittel på masteroppgaven: Cyberangrep i bank og finans Engelsk tittel: Cyber attack in bank and finance	
Studiepoeng: 30	
Emneord: Risiko, sikkerhetskultur, resilience engineering, cyberangrep, sårbarhet, trussel, tillit	Sidetall: 96 + vedlegg/annet: 125 Stavanger, 13.06.2019

Forord

Først og fremst så vil jeg takke mine gode studiekollegaer. Uten dere så ville ikke studietiden blitt så kjekk som den har vært. Gjennom studietiden har vi lært oss å samarbeide på tvers av utdanningsbakgrunn og kompetanse, noe som har vært utrolig spennende og givende. Takk for to innholdsrike år!

En stor takk går til Stig Andersson for din entusiasme og interesse i min oppgave. Du har bidratt til å gjøre min forskning mulig, og jeg setter stor pris på ditt bidrag som både informant og kontaktperson i SpareBank 1 SR-Bank.

Den største takken går til min veileder Riana Steen. Dine tanker og ideer har hjulpet meg på veien til å bli en bedre student og forsker. Du har også bidratt til å øke min motivasjon ved å sette høye krav til meg, noe jeg er svært takknemlig for. Takk for at du har delt din kunnskap med meg!

Sist, men ikke minst, jeg ønsker å takke familie og venner for utrolig bra støtte gjennom studietiden. Dere har vært der når motivasjonen var på bunn, og har bidratt med gode ord og hjelp slik jeg at har kommet meg gjennom denne tiden. Å skrive en masteroppgave er veldig spennende og givende, men det er også veldig stressende og krevende, og da har dere vært der til å bidra som positive mennesker rundt meg. Takk!

Stavanger, juni 2019.

Jeannett Hansen.

Sammendrag

På bakgrunn av dagens risikobilde i det norske samfunnet så har digitalisering og teknologisk utvikling resultert i en økende sårbarhet i bank og finans. Faren for at cyberangrep skal treffe norske banker og deres kunder har økt, noe som danner det tematiske grunnlaget for denne studien. Hensikten med oppgaven er å vurdere SpareBank 1 SR-Bank sin tilnærming til sikkerhetskultur og evne til motstandsdyktighet. Problemstillingen som er gjeldende for oppgaven er som følger:

«Hvordan kan en bank som en organisasjon beskytte sine kunder mot cyberangrep?»

For å besvare denne problemstillingen har to forskningsspørsmål blitt diskutert: (1) Hva kjennetegner en resilient cybersikkerhetskultur i bank, og (2) på hvilken måte kan banker arbeide for å imøtekomme kundenes interesser med tanke på behov for beskyttelse. Denne diskusjonen er basert på teori om sikkerhetskultur og resilience engineering som danner det teoretiske grunnlaget for videre diskusjon. Gjennom en spørreundersøkelse om bankkunders forventinger til norske banker, en dokumentanalyse om relevante nasjonale og internasjonale rapportert og 12 dybdeintervjuer i SpareBank 1 SR-Bank så det blitt etablert et empirisk grunnlag for diskusjon.

Analysen viser at SpareBank 1 SR-Bank har en tilstedeværende sikkerhetskultur som danner rammene for muligheten til å danne en form for motstandsdyktighet i henhold til cyberangrep. Analysen viser videre at SpareBank 1 SR-Bank på mange måter oppnådd en viss form for motstandsdyktighet gjennom å tilfredsstille krav til teorien om resilience engineering. Konklusjonen brukes til å besvare problemstillingen som viser at bruk av sikkerhetskultur og resilience engineering samtidig som banker tar hensyn til de lovverk og anbefalinger som foreligger, så er det mulig å opprette en viss form for beskyttelse.

Abstract

Reviewing the background of today's level of risk in the Norwegian society, digitalization and technological development has resulted in an increased vulnerability in the bank and finance sector. The risk of cyber-attacks on Norwegian banks and their customers have increased, which is the thematic basis for this thesis. The purpose with this thesis is to evaluate SpareBank 1 SR-Banks approach to safety culture and the ability to be resilient. The thesis question that is relevant to this study is:

"How can a bank as an organization protect their customers against cyber-attacks?"

To answer this thesis question in the best possible way, two research questions will establish a discussion about: "What characterizes a resilient cybersecurity culture in banks?" and "How can banks work to improve their customers interest regarding their need for protection?". This discussion will be based on theory about safety culture and resilience engineering that will be the theoretical basis for further analysis. A survey based on bank customers expectations to Norwegian banks, a document analysis about relevant international and national reports and 12 interviews in SpareBank 1 SR-Bank will establish the empirical basis for further analysis.

The analysis shows that SpareBank 1 SR-Bank 1 as a case study has a present safety culture that opens up the possibility for the bank to be able to establish resilience regarding cyberattacks. The analysis also shows that SpareBank 1 SR-Bank in many ways has achieved a certain form for resilience by responding to requirements of abilities that are necessary in resilience engineering. The conclusion shows that by using security strategies like safety culture and resilience engineering combined with laws and relevant guidelines, it is possible to establish protection for bank customers regarding cyber-attacks.

Liste over forkortelser

Forkortelser	Forklaring
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
DDoS	Distributed Denial of Service
E-tjenesten	Etterretningstjenesten
EU	Europeisk Union
EØS	Europeisk Økonomiske Samarbeid
GDPR	General Data Protection Regulation
ID	Identifikasjonsdokument
IKT	Informasjons- og kommunikasjons teknologi
IRT	Incident Respons Team
KRIPOS	Kriminalpolitisentralen
MMR	Mixed Method Research
NAT	Normal Accident Theory
NATO	North Atlantic Treaty Organization
NOU	Norsk Offentlig Utredning
NSM	Nasjonal Sikkerhetsmyndighet
PSD2	Payment Service Directive 2
PST	Politiets Sikkerhetstjeneste
RE	Resilience Engineering
SWIFT	Society for Worldwide Interbank Financial Telecommunications
WEF	World Economic Forum

Liste over definisjoner

Cyberkriminalitet: Samlebetegnelse for kriminalitet som gjennomføres via datamaskiner knyttet til internett (Finans Norge, 2017, s. 7).

Cybernettverk: Betegnelse på en informasjonsteknologisk mediert virkelighet formet gjennom digital representasjon, kommunikasjon og presentasjon hvor systemer og infrastruktur i økende grad består av felles teknologi, tjenester og komponenter (E-tjenesten, PST & NSM, 2010, s. 21).

Cyberresilience: The ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents (BCBS, 2018, s. 8)

Cybersikkerhet: Beskytte alt som er sårbart fordi det er koblet til, eller på en annen måte er avhengig av informasjons- og kommunikasjonsteknologi (NOU, 2015:13, s. 34).

Digitalisering: Å tilrettelegge for generering av digital informasjon, samt håndtering og utnyttelse av informasjonen (Dvergsdal, 2019).

Identitetstyveri: Når noen skaffer seg, besitter, overfører, benytter eller fremstår som rette innehaver av et identifikasjonsbevis eller personopplysningen til en person for å begå økonomisk svindel, bedrageri eller annen kriminalitet (Datatilsynet, u.å.).

Kultur: Kultur er det komplekse hele som inkluderer kunnskap, tro, kunst, lover, moral, skikker og alle ferdigheter og vaner som folk har lært i egenskap av å være samfunnsmedlemmer (Tylor, 1871).

Personvern: Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet (Grunnloven, 1814, §102).

Resiliens: Den kapasitet et sosialt system har til å motstå og tilpasse seg forventede og uforventede forstyrrelser, og til å gjenopprett funksjonaliteten etter alvorlige påkjenninger fra slike forstyrrelser (Engen, Kruke, Lindøe, Olsen, Olsen & Pettersen, 2014, s. 48).

Risiko: Refererer til usikkerhet om og alvorligheten av hendelser og konsekvenser (eller resultater) av en aktivitet med hensyn til det mennesker verdsetter (Aven & Renn, 2010, s. 3).

Sikkerhetskultur: Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd (Nasjonal Sikkerhetsmyndighet, 2014).

Sårbarhet: Et systems evne til å opprettholde sin funksjon når det utsettes for påkjenninger (Aven, Boyesen, Njå, Olsen & Sandve, 2004, s. 124).

Tillit: En tilstand der man aksepterer sårbarheter basert på positive forventinger til intensjonen til en annen (Engen et.al., 2014, s. 327).

Trussel: En mulig årsak til en uønsket hendelse (NOU, 2015:13, s. 31).

Uønsket hendelse: Hendelse eller tilstand som kan medføre skade på mennesker, miljø, materiell eller annen form for økonomisk tap (Vatnelid, 2018, s. 124).

Oversikt over tabeller:

Oversikt over figurer:

Innholdsfortegnelse

1. Innledning

1.1 Oppgavens bakgrunn

Krigføring og angrep gjennom cybernettverket er en stor trussel mot verdenssamfunnet i dag. Som et resultat av teknologisk utvikling og digitalisering, kan selv de minste angrep få store konsekvenser på den infrastrukturen som vestlige samfunn består av. World Economic Forum (WEF) sin globale risikorapport anno 2019 viser at cyberangrep er en av de største truslene verden står ovenfor i dag. De aktivitetene som truer samfunnet mer enn cyberangrep er utilsiktede hendelser som naturkatastrofer og hendelser knyttet til klimakrisen (World Economic Forum, 2019, s. 5). Rapporter fra blant annet Det hvite hus i USA, North Atlantic Treaty Organization (NATO) og norske myndigheter fastslår at cyberangrep er den mest asymmetriske trusselen mot den vestlige verden i den tiden vi lever i nå. Trusselen fra cyberangrep øker i samsvar med den moderne digitaliseringen, som utvikler seg hurtigere enn noen gang (E-tjenesten, Politiets Sikkerhetstjeneste & Nasjonal Sikkerhetsmyndighet, 2010, s. 3).

Den økende bruken av teknologi og digitalisering av systemer har ført til at komplekse systemer gjennom elektronikk og programvare er blitt normalisert. Denne endringen resulterer i økt sårbarhet og konsekvensene av eventuelle angrep kan få mer alvorlige utfall (Clarke & Knake, 2010, s. 7-11). Teknologi fortsetter å ha en viktig rolle i dagens utvikling, og har på mange måter ført til at dagens samfunn kan kalles den fjerde industrielle revolusjon (World Economic Forum, 2019, s. 7).

I 2015 var Norge et av verdens ledende land innenfor bruk av informasjons- og kommunikasjonsteknologi (IKT) (NOU 2015:13, s. 15). Gjennom et forskningsprosjekt utført av den finske organisasjonen Etlatieto ble det avdekket at Norge var det mest digitaliserte landet i verden. Forskningen ble basert på funn fra et digi-barometer utført i 2017, hvor nivået av digitalisering, bruken av digitalisering og hva digitaliseringen produserer ble essensielle faktorer (NRK, 2017). Det norske samfunnet og den norske Regjeringen har jobbet med digitalisering i flere tiår, og globalisering, automatisering og teknologisk utvikling har bidratt til at Norge har vært kapabel til å ta det neste steget for å bli et mer kompleks og digitalisert samfunn (Nasjonal Sikkerhetsmyndighet, 2018, s. 7).

1.2 Digitalisering i banknæringen

I 1994 ble Norges bank- og pengevesen sett på som én av de viktigste samfunnsfunksjonene Norge har for å kunne ha og opprettholde et trygt og stabilt samfunn. Det var allerede da et spesielt fokus på elektronisk betalingsformidling og andre bank-funksjoner som var viktige for kunder av norske banker. Denne elektronikken er blitt avgjørende for hvordan bank- og pengevesenets normaldrift skal foregå, og avhengigheten til denne teknologien skaper økt sårbarhet (Justis- og politidepartementet, 1994). I dag, 15 år senere, fortsetter finansnæringen i Norge å tilby et mangfold av teknologiske og digitaliserte tjenester og produkter. Risikoen for cyberangrep har økt og sårbarheten er blitt større, og et cyberangrep vil få betydelige konsekvenser på både personlige og nasjonale interesser (Finans Norge, 2017, s. 5). Banknæringen blir hyppigere preget av flere angrep i flere banker rundt om i verden. Det kan brukes flere metoder ved hacking av en bank, bl.a. gjennom overføringssystemet «Society for Worldwide Interbank Financial Telecommunications» (SWIFT), utpressingsprogramvare, ta kontroll over banksystemer som bankautomat, stjele fra fond eller gjennom ID-tyveri. Slike cyberangrep kan forklares som et angrep med lav risiko og som gir høy fortjeneste, noe som kan antas å være en forklaring til den økte hyppigheten (Hovland, 2017).

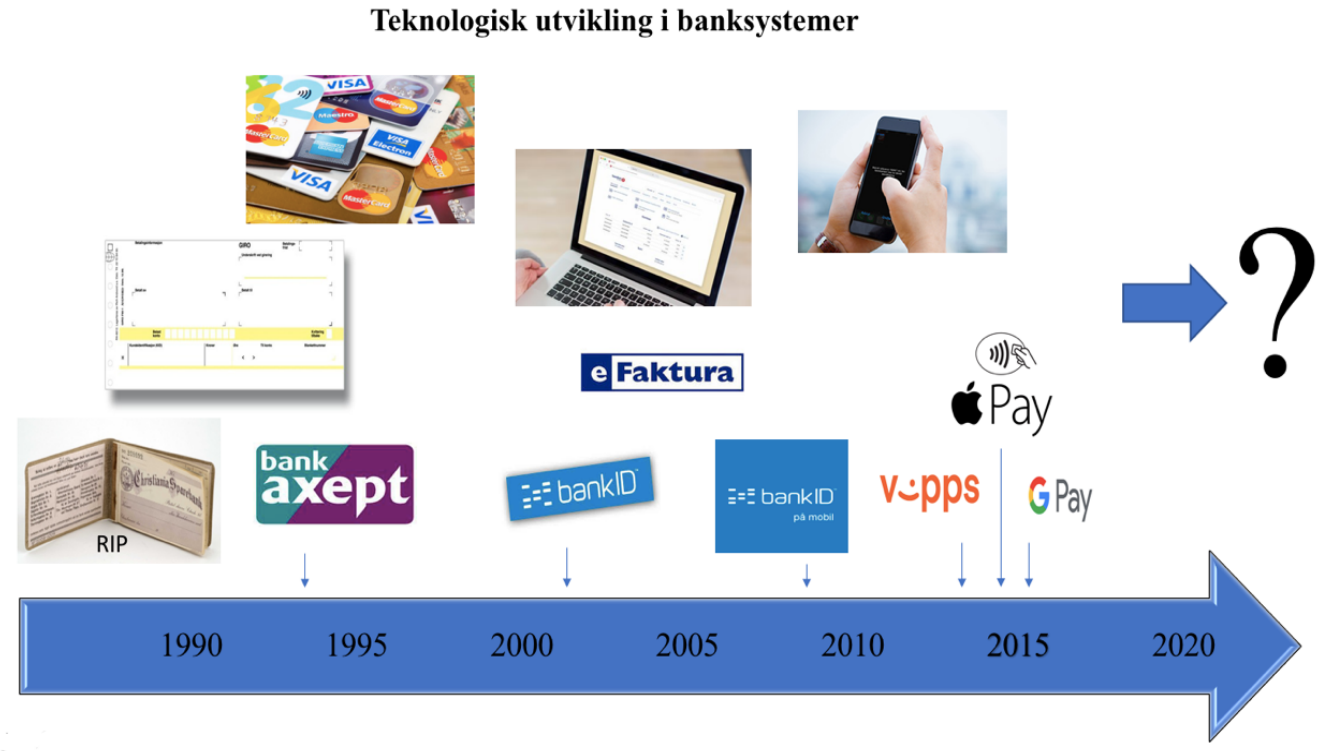
Gjennom hackingen av sentralbanken i Bangladesh i 2016, klarte hackerne å bruke SWIFT-nettverket til å overføre 100 millioner dollar. Som et resultat av dette angrepet ble retningslinjer i bruk av SWIFT endret, samt at direktøren i sentralbanken måtte tre av (Hammer, 2018). Angrepet på sentralbanken i Russland i 2017, fikk også økonomiske konsekvenser da hackerne stakk av med rundt 6 millioner dollar ved bruk av samme hackemetode som i Bangladesh. Denne gangen hadde hackerne fått tak i en PC og brukt SWIFT-nettverket til å overføre pengene (Stubbs, 2018). I 2018 ble det gjennomført et såkalt Distributed Denial of Service (DDoS) angrep på den britiske Lloyds Bank. Dette angrepet fikk ikke økonomiske konsekvenser, men resulterte i at bankens kunder ikke fikk bruke bankens nettside for å sjekke deres kontoer på flere dager (Bond, 2018). Angrepet på Bank of America i 2012 fikk heller ikke økonomiske konsekvenser, men angrepet innebar at hackerne avviklet nettsiden som flere banker bruker, noe som resulterte i flere forsinkelser for bankenes kunder (Dugan, 2018).

Det digitale bildet i banknæringen som stadig er i forandring, utvikler seg raskt, og det endrer

da også trusselbildet, med tilhørende risiko, raskere enn noen gang. Fokus på å sikre de interessene bankene har, og arbeid med forebygging og avdekking av kriminelle anslag får større fokus nå enn før. Det er krevende arbeid, men nødvendig arbeid for å sikre både finansnæringen og mer relevant til denne studien, personlig kundeinformasjon (Finans Norge, 2017, s. 6).

1.3 Problemstilling og tilhørende forskningsspørsmål

Figur 1 viser forandringene i teknologien i banksystemer de siste 30 årene. Fra å bruke sjekkhefter til å innføre bankkort, til deretter å videre innføre digitale tjenester som bankID, ApplePay og Vipps viser store forandringer. Digitaliseringen har oppstått både på grunn av effektivitet, og for å gjøre det enklere for kunden. Ved å opprette mobilbank og tjenester via internett og mobil, har bankene fått mulighet til å redusere sin bemanning som i utgangspunktet tok seg av tjenester som regningsbetaling og overføring av penger til både innenlands- og utenlands kontoer. Denne digitale og teknologiske utviklingen skjer samtidig som ulike lovgivninger blir implementert for å forbedre sikkerheten av personvernet til kunder innenfor betalingssystemer.



Figur 1: Teknologisk utvikling

Det er ingen tvil om at digitaliseringen som har utviklet seg i Norge har stor påvirkning på bankvirksomheten i landet. Spørsmålene som stilles og kan forstås som bekymringsverdige er den økte risikoen som følger med når kompleksiteten i systemene økes. Den nye teknologien som brukes i betalingssystemer og identifiseringssystemer sammen med nye lovgivninger gjør at rammeverket for personvern blir påvirket med tilhørende sårbarheter fra økt risiko. For å kunne forstå hvordan bank- og finans-Norge best mulig skal stå rustet og bevare de tillitsforholdene bankene har til kundene sine, så vil det være interessant å se på hvordan bankens rådgivere og sikkerhetsavdeling arbeider for å forsikre kundene sine om at deres personlige informasjon er sikker hos dem. I forhold til overnevnte tema så vil følgende problemstilling være relevant:

«Hvordan kan en bank som en organisasjon beskytte sine kunder mot cyberangrep?»

I et forsøk på å spesifisere forskningsstudien så vil problemstillingen opptre som et overordnet spørsmål, mens to forskningsspørsmål vil bidra til å gjøre at forskningen får mer dybde. De to forskningsspørsmålene vil bidra til å belyse hvordan banker som organisasjon vurderer trusselbildet, hvordan de jobber mot å forbedre hvordan de håndterer eventuelle risikoer og hva de gjør for å opprettholde et godt tillitsforhold til de kundene de har gjennom å betrygge dem om at de jobber for å redusere den risikoen de står ovenfor. Dette blir presentert gjennom to forskningsspørsmål:

1. **Hva kjennetegner en resilient cybersikkerhetskultur i bank?**
2. **På hvilken måte kan banker arbeide for å imøtekomme kundenes interesser i forhold til behov for beskyttelse?**

Formålet med denne studien og de valgte forskningsspørsmålene er å danne et bilde ved å belyse hvordan en bank som organisasjon jobber mot de truslene som er erkjent, og å drøfte hvordan banker kan opprette ulike tiltak som har til hensikt å sikre og eventuelt styrke kundens tillit til organisasjonen. I denne studien så skal det bli intervjuet flere ansatte i en norsk bank i Stavanger for å få dybde i forskningen. Dette skal bidra til å skape et så korrekt bilde av virkeligheten som mulig. I tillegg vil en generell spørreundersøkelse som blir spredd ut til offentligheten kunne bidra til å besvare spørsmål når det gjelder tillit og bankforholdet

mellom kunde og rådgiver. For å kunne diskutere og drøfte problemstillingen og de underliggende forskningsspørsmålene så er relevant teori og empiri essensielt for å kunne få frem en god diskusjon.

1.4 Oppgavens oppbygging

Tabell 1 viser systematisk hvordan denne oppgaven er bygget opp. Oppgaven består av 7 kapitler pluss en egen del med referanser.

Tabell 1: Oppgavens struktur og oppbygning

	Fokusområde
1: Innledning	Presentasjon av bakgrunn og tema for studien, og deretter relevant problemstilling og forskningsspørsmål og dens formål. Avgrensninger og beskrivelse av utforming vil også være i denne delen.
2: Introduksjon av casestudies	I denne delen presenteres SpareBank 1 SR-Bank som deltaker i casestudiet, samt en del om regler og lover som banker i Norge og Europa må forholde seg til.
3: Teoretisk grunnlag	Her presenteres relevant teori med en terminologiforståelse, og videre teori om sikkerhetskultur og resilience engineering.
4: Metode	I dette kapittelet skal forskningsmetoden beskrives og den tilnærmingen som blir brukt skal vurderes. Den kvalitative og kvantitative forskningen skal forklares, og videre skal empiriens reliabilitet og validitet vurderes.
5: Presentasjon av empiri	Her blir sentrale funn presentert systematisk ved bruk av blant annet tabeller og figurer.
6: Drøfting	I denne delen skal empirien knyttes sammen med teorien, og forskningsspørsmålene skal diskuteres og drøftes.
7: Konklusjon	I den siste delen av denne oppgaven skal det presenteres en konklusjon og avslutning som skal forme et svar på problemstillingen, samt refleksjoner og aspekter rundt de to forskningsspørsmålene studien inneholder.
8: Referanseliste	I dette kapittelet ligger det en litteraturliste over brukte referanser.

1.5 Avgrensing

Tid og kapasitet gjør det nødvendig med avgrensninger i denne studien. Det omfanget av trusler norske banker står ovenfor i dag er stort og komplekst. Ettersom det ikke er mulig å ta for seg hele trusselbildet så vil bankers kunder med hensyn til vern av personlig informasjon bli satt i fokus. Den empiriske innsamlingen vil også være avgrenset til å fokusere på en dybdeundersøkelse av SpareBank 1 SR-Bank og deres ansatte. Informasjonsuthentingen vil også være begrenset der hvor utfordringer vedrørende sikkerhetsklarering og taushetsplikt vil gjøre at noe informasjon ikke vil være tilgjengelig. En videre avgrensning er at det kun blir vektlagt informasjon som bankene er villige til å dele, og ikke basere oppgaven på spekulasjoner eller andre informasjonskanaler når det gjelder forskningsspørsmålene. Som en del to av den empiriske innsamlingen så vil det være en avgrensning i forhold til den kvantitative spørreundersøkelsen. Dette er nødvendig på grunn av tidskapasitet, og spørreundersøkelsen vil derfor kun være tilgjengelig via Facebook i en bestemt periode. For å gjøre det teoretiske rammeverket så relevant som mulig vil det være nødvendig med avgrensninger. En terminologiforståelse som innebærer begreper som «risiko», «sårbarhet», «usikkerhet», «tillit», «kultur» og «cyberdomenet» er essensielt for å forstå grunnlaget for denne studien. Videre vil teori om teknologiske uønskede hendelser og sikkerhetsstrategier som sikkerhetskultur og resilience engineering være sentralt.

2. Presentasjon av case studie og oppgavens kontekst

Uttalelser fra Paul Meen og Til Schuerman (2018) om at cyberangrep kan skape den nye finanskrisen støttes av norske finanseksperter som Jan Digranes og Rune Bjerke (Bjerknes, 2018). Lignende uttalelser har også blusset opp i Storbritannia og Steve Buck uttalte at «.. a cyber-attack could stop the country». Disse uttalelsene har skapt diskusjoner og frykt for at teknologiske betalingssystemer vil kunne påvirke infrastrukturen negativt (Wall, 2018). Kripos la frem i 2015 at cyberkriminalitet nå er blitt et reelt samfunnsproblem, og oppdagelsesrisikoen og fortjenestepotensialet av slike kriminelle handlinger er skremmende. Det er stadige forsøk på hacking av personlig informasjon og ID-tyveri for å innhente informasjon som kan brukes til senere kriminelle handlinger (NOU, 2015:13, s. 55-56; Politiet, u.å.). Økningen i antall cyberkriminelle handlinger som kredittkortsvindel, ID-tyveri, hacking av e-post-konto og nettfiskeforsøk er hårreisende. Denne økningen samt den kontinuerlige utviklingen av avansert infrastruktur og avhengighet til internett, gjør at Norge har blitt et attraktivt offer for cyberangrep fra utviklingsland. Banker i seg selv har mye ansvar for hvordan de velger å håndtere den økte risikoen og sikkerhetsutfordringen som Norge står ovenfor i dag. Bankens ledelse og ansatte må ta valg om hvordan de skal velge å håndtere trusler og sårbarheter, samtidig håndtering av bankens kunder sin usikkerhet når det kommer til teknologiske forandringer og den økte risikoen (NOU, 2015:13, s. 60).

2.1 SpareBank 1 Sr-Bank

SpareBank 1 SR-Bank er en norsk bank som er en del av SpareBank 1 gruppen AS, og denne banken har hovedkontor i Bjergsted, Stavanger. SpareBank 1 SR-Bank har 38 underkontorer som er spredd utover Sør- og Vestlandet, og i Oslo ((1), u.å.). Det var i 1996 at SR-Bank ble en del av SpareBank 1 gruppen, som ble en allianse av ulike banker rundt om i Norge med SpareBank 1 som paraplyorganisasjon. I denne alliansen samarbeider bankene om bl.a. forsikringsprodukter, fondsforvaltning, finanstjenester, teknologi og merkevarebygging ((5), u.å.). Visjon og verdier er fundamentalt i SpareBank 1 SR-Bank, hvor bankens drøm er å være førstevalget på Sør- og Vestlandet, med kunden som sin viktigste prioritering. For å nå dette målet er det viktig å utføre arbeid etter verdiene ansvar og respekt, engasjement og handlekraft. Det er hensikten, visjonen og verdiene i SpareBank 1 SR-bank som gjør at deres konsern, ansatte og kultur får muligheten til å utvikle seg ((4), u.å.).

Når det gjelder personvern som er gjeldende for denne studien, så har SpareBank 1 SR-Bank en personvernerklæring som sier (oppdatert 25/6-2018) ((2), u.å.):

«Vi i SpareBank 1 SR-Bank har taushetsplikt, og vi sørger for at dine personvernopplysninger blir behandlet på en sikker måte etter persovernsopplysningsloven og EUs personvernforordningen General Data Protection Regulation 2016/679 (GDPR)»

SpareBank 1 SR-Bank har fokus på å sikre kundens personlige informasjon, og dette gjøres gjennom en taushetsplikterklæring og kontinuerlig oppdatering av systemene. Gjennom overvåkning får banken mulighet til å observere feil og arbeide for å forhindre at kundeopplysninger blir spredd på noen som helst måte. Risikoen og sikkerhetsløsninger blir vurdert opp mot funksjonaliteten i banken slik at det skal være mulig å unngå svakheter så langt det lar seg gjøre. Det er en egen gruppe som arbeider med å håndtere sikkerheten og risikovurderingene som SpareBank 1 SR-Bank står ovenfor, og vurderer om det er sikkerhetshull som kan sette personlig informasjon i fare. I tillegg arbeider SpareBank 1 SR-Bank med å bruke sikkerhetsteknologi som kryptering og brannmurer for å opprettholde sikkerheten i systemene de bruker. De ansatte er også lært opp til å forstå et eget styringssystem som brukes for informasjonssikkerhet, tilgangskontroll, avvikshåndtering og opplæring, slik at de som behandler den personlige informasjonen skal ha oppdatert kunnskap om hva som må gjøres for å holde informasjon konfidensiell ((3), u.å.).

2.2 Lovgivning til banker i Norge

Lover fastsettes av Stortinget for å binde organisasjoner til å følge lovgivende makts regler og gjøremåter. Det er krav som blir stilt i ulike lover og forskrifter, og i denne sammenheng så vil det være interessant å nevne et par risikobaserte krav, hvor det er krav til metoder og fremgangsmåter for å identifisere og håndtere risiko for ulike banker i Norge (Aven et.al., 2004, s.28). Det er Finansdepartementet som er ansvarlig for håndtering og tilsyn av lovgivninger og forskrifter, gjennom blant annet Finanstilsynet, som er laget for banker i Norge. Gjennom forskriften om risikostyring og internkontroll så er alle som er under denne lovgivningen pliktige til å fortløpende vurdere de risikoene som er knyttet til virksomheten. Denne forskriften gjør at banker slik som SpareBank 1 SR-Bank skal arbeide for å ha definerte mål og strategier knyttet til sikkerhet for deres organisasjoner, hvor det skal gjennomføres risikovurderinger minst en gang årlig. Det må være en systematisk

gjennomgang slik at de tilstrekkelig kan håndtere bankenes identifiserte risikoer på en forsvarlig måte (Forskrift om risikostyring og internkontroll, 2009, §6). I 2018 ble det også blitt introdusert en ny lov med tiltak mot hvitvasking og terrorfinansiering som skal gjelde for bl.a. bankvirksomhet. Hvitvaskingsloven har som formål å forebygge og avdekke hvitvasking og terrorfinansiering, hvor da dette har blitt vurdert som et voksende problem i norske banksystemer. Denne loven skal beskytte det finansielle og økonomiske systemet i norske banker (Hvitvaskingsloven, 2018, §1). Forskrift for informasjons- og kommunikasjonsteknologi (IKT-forskriften) bidrar til å sikre at norsk banknæring fastsetter overordnede mål, strategier og sikkerhetskrav. Denne forskriften inneholder også retningslinjer for hvordan utkontrakteringsavtaler fungerer, noe som er høyst aktuelt for SpareBank 1 SR-Bank da de har flere eksterne leverandører på utkontrakteringsavtaler (Forskrift om IKT-systemer i banker mv., 2003)

2.3 Personvern

Ettersom digitaliseringen og flyten av informasjon gjennom cybernettverket har økt og blitt mer komplekst, så har EU satt i gang en ny lovgivning, *General Data Protection Regulation* (GDPR), og et nytt og oppdatert direktiv *Payment Service Directive 2* (PSD2). Begge har som til hensikt å beskytte personvern. Som medlem i EØS får norsk finansnæring og norske forbrukere tilgang til det europeiske markedet. Norge er et av fire land i EØS som også har blitt påvirket av endringene. I EU og EØS tilstrebes det lik konkurranse og lik beskyttelse som gjør at alle må følge de samme lovgivningene og retningslinjene. De juridiske endringene i EU gir mulighet til å overvåke og håndtere den risikoen som truer den finansielle stabiliteten i hele EØS-området, og derfor har Norge blitt nødt til å delta i implementeringen av både GDPR og PSD2 (Finanstilsynet, 2017).

Den nye lovgivningen, GDPR, ble etablert i EU i 2016, og loven skal omhandle: *«...on the protection of natural persons with regard to the processing of personal data and on the free movement of such data..»* (GDPR, 2016). Formålet er å styrke og harmonisere personvern i prosessen vedrørende personlig informasjon innenfor EU og EØS. Denne lovgivningen som har blitt innført til Norge gjennom EØS har blitt implementert i personopplysningsloven fra Justis- og beredskapskapsdepartementet (Personopplysningsloven, 2018). Denne lovgivningen ble innført i Norge 20.juli 2018, og har som formål om å verne fysiske personer

i forbindelse med behandlingen av deres personlige informasjon og om fri utveksling av disse opplysningene (ibid., §1).

Det andre direktivet som er blitt innført i EU og som er på vei inn i Norge nå kalles PSD2. Dette direktivet skal omhandle *«..on payment services in the internal market...»,* og er en oppdatering av «Payment Services Directive 1» (PSD1) (PSD2, 2015). PSD1 ble innført for å bidra til økning i handel på tvers av landegrenser innenfor EU hvor det ble satt krav til varslingsfrister, informasjon om prising og ansvarsforhold, samt at de åpnet for at andre betalingssystemer enn banker kunne tilby betalingstjenester. Det dette direktivet manglet var at det ikke dekket alle typer betalingstjenester som kunne tilbys, og derfor ble det nødvendig med en revidert versjon i PSD2 (Finans Norge, u.å.). PSD2 har blitt implementert i betalingstjenestedirektivet utstedt av Finansdepartementet i Norge (Endringslov til finansforetaksloven mv., 2018). Formålet med betalingstjenestedirektivet vil være å oppdatere lovverket slik at det skal samsvare med den utviklingen betalingstjenester står ovenfor. Utviklingen som foregår innenfor finansmarkedet har fått økt risiko, og da vil en modernisering bidra til å sikre tekniske betalingsløsninger (Finans Norge, 2017, s. 5). Betalingstjenestedirektivet vil gjøre det mulig for ulike betalingssystemer å dele informasjon om deres kunder med andre aktører for betalingssystemer. Betalingssystemer kan forklares som bl.a. PayPal, Vipps, BankAxept og banksystemer (ibid., s. 5). Ved å innføre dette direktivet så vil intensjonen være å øke konkurransen mellom ulike betalingstjenester samt å fremme innovasjon og styrke sikkerheten for nettbetaling og tilgang til kontoer (Finans Norge, u.å.).

Personopplysningsloven og betalingstjenestedirektivet kan forstås som komplementære og konkurrerende på samme tid. Dette gjør at de vil være interessante å ta med inn i en diskusjon hvor beskyttelse av personvern i bank er i fokus. Ved å implementere disse endringene i det norske lovverket, så vil dette bidra til å øke ivaretakelsen av samfunnsansvaret staten har for å ha forsvarlig drift og ivareta brukerinteresser av de som benytter seg av betalingstjenester i Norge (Finans Norge, 2017, s. 5).

3. Teoretisk grunnlag

I dette kapittelet presenteres det valgte teoretiske begrepsapparatet og perspektiver som bidrar som et utgangspunkt for drøftingen av det empiriske datamaterialet som blir samlet inn. Dette teorigrunnlaget utgjør et rammeverk og brukes som et verktøy for å belyse problemstillingen, og de underlagte forskningsspørsmålene. Den første delen av teorikapittelet vil inneholde en terminologiforståelse som skal bidra til å danne et felles utgangspunkt av begrepsbruk og definisjoner. Terminologiforståelsen vil bestå av en utdypning av de begrepene som blir definert på siden med listen over definisjoner. Den siste delen av det teoretiske grunnlaget i denne oppgaven handler om James Reason sin teori om sikkerhetskultur og Erik Hollnagel sin teori om resilience engineering.

3.1 Terminologiforståelse

3.1.1 Cyberdomenet

Digitalisering handler om å bruke bestemte forretningsmodeller og prosesser for at man skal dra nytte ut av informasjon som man har konvertert fra analogt til digitalt. Den digitale transformasjonen infrastrukturen står ovenfor nå er en endring som har på oppstått på ulike fagfelt vedrørende økonomi, institusjoner og samfunn. Denne endringen skjer på grunn av at informasjon har blitt digital og systemer har blitt opprettet for å kunne utnytte denne digitale informasjonen (Unruh & Kiron, 2017). Teknologi og internett er blitt en del av hvordan vi lever, både i kjøleskapet, telefonen, garasjen, bilen og postkassen, men også kritisk infrastruktur som sykehus, kraftstasjon og politistasjon. Avhengigheten av IKT for det norske folk og det norske samfunn er enorm og stadig økende (NOU 2015:13, s. 18). Digitalisering skaper muligheter som kunstig intelligens og automatisering, og på mange måter skaper den også et mer sikkert samfunn med oppdatert teknologi. Nye digitale kommunikasjonsløsninger bidrar til bedre støtte i krise- og beredskapsarbeid og økt funksjonalitet. Moderne IKT-arkitektur bidrar til kvalitet og effektivitet i sikkerhetsarbeid, og digitalisering i seg selv øker effektiviteten og gir kostnadsbesparelser (Nasjonal Sikkerhetsmyndighet, 2018, s. 7).

Cybernettverket er overalt hvor det er en PC, både i arbeidslivet og hverdagslivet. Så lenge du har en PC, eller en prosessor eller kabel som er koblet til PC-en, så vil dette omtales som cybernettverk. Cybernettverket er ikke bare lenger det som er koblet til Internett, men også de

programmene som kan brukes uten internett (Clarke & Knake, s. 69-70). Et cybernettverk kan defineres ifølge E-tjenesten, PST og NSM slik (2010, s. 21):

«Betegnelse på en informasjonsteknologisk mediert virkelighet formet gjennom digital representasjon, kommunikasjon og presentasjon hvor systemer og infrastruktur i økende grad består av felles teknologi, tjenester og komponenter.»

Et cyberangrep er en fellesbetegnelse for alle typer uønskede angrep gjennom cybernettverket. Hackerangrep gjennom cybernettverket er blitt en voksende affære. En hacker er en person som får tak i klassifisert og konfidensiell informasjon gjennom et IKT-system (Gordon & Loeb, 2006, s. 175). Det er ulike årsaker til at en hacker gjennomfører et angrep, men vanlige årsaker kan være at det skal være et strategisk angrep, organisert kriminalitet, politisk aktivisme, eller politisk, teknologisk og økonomisk etterretning. Ulike teknikker og metoder kan brukes, hvor mye av det vanlige inneholder filformater, verktøykasser eller botnet som distribueres gjennom E-mail, nettsider, USB-enheter eller sosial manipulering (E-tjenesten, Politiets Sikkerhetstjeneste & Nasjonal Sikkerhetsmyndighet, 2010). Felles for alle teknikker og metoder er at det klassifiseres som cyberkriminalitet hvor et angrep gjennom cybernettverket skjer «..at the speed of light» (Clarke & Knake, s. 31). Cybersikkerhet kan forklares som en beskyttelse av det som er sårbart på grunn av dens tilkobling eller avhengighet til informasjons- og kommunikasjonsteknologi (NOU, 2015:13, s. 34). Gordon og Loeb definerer cybersikkerhet slik som dette (2006, s. 174):

«Protection of information that is accessed and transmitted via the Internet or any other computer network»

Gjennom cybersikkerhet skal man arbeide for å redusere cyberkriminalitet og redusere den trusselen samfunnet står ovenfor, som kan forklares som en potensiell handling som kan forårsake ødeleggelser i IKT-systemer (Gordon & Loeb, 2006, s. 177).

3.1.2 Risikobegrepet

I forsøk om å forstå risikobegrepet så er det en viss evne som bør ligge til grunn. Denne evnen handler om å forstå at en hendelse kan føre til skader, hvor skadene kan enten oppstå umiddelbart, eller på sikt. Hvordan man forstår risiko står i sammenheng med hvilke

erfaringer man har, noe som blir forklart gjennom risikopersepsjon og -kompensasjon (Vatnelid, 2018, s. 123).

Tabell 2 viser til flere tilnærminger til risiko. Tabellen er presentert av Terje Aven og Ortwin Renn, og kan bidra i denne studien ved å vise hvor mange ulike forståelser av risiko som eksisterer.

Tabell 2: Ulike tilnærminger til risiko (Aven & Renn, 2010)

Definisjoner av risiko	**Fellestrekk**
Risiko tilsvarer forventet tap	Risiko uttrykt ved hjelp av sannsynligheter og forventede verdier
Risiko tilsvarer forventet unytte	
Risiko er et mål på sannsynligheten for og alvorligheten av tilhørende konsekvenser	
Risiko er kombinasjonen av sannsynligheten for og rekkevidden av konsekvenser	
Risiko tilsvarer 'the triplet' (Si, Pi, Ci), hvor S er scenario nr i, P er sannsynligheten av det scenarioet, C er konsekvensen av scenario i, og i=1,2,…,N,	
Risiko refererer til usikkerhet i forhold til resultat, handlinger og hendelser	
Risiko er en situasjon eller hendelse hvor noe mennesker verdsetter (inkludert mennesker selv) er i fare og hvor resultatet er usikkert	Risiko uttrykt gjennom hendelser/ konsekvenser og usikkerheter
Risiko er en usikker konsekvens av en hendelse eller en aktivitet i forhold til noe mennesker verdsetter	
Risiko er en effekt av usikkerhet knyttet til mål	
Risiko tilsvarer den to-dimensjonale kombinasjonen av hendelser/konsekvenser og assosierte usikkerheter (vil hendelsene skje, og hva vil bli konsekvensene)	

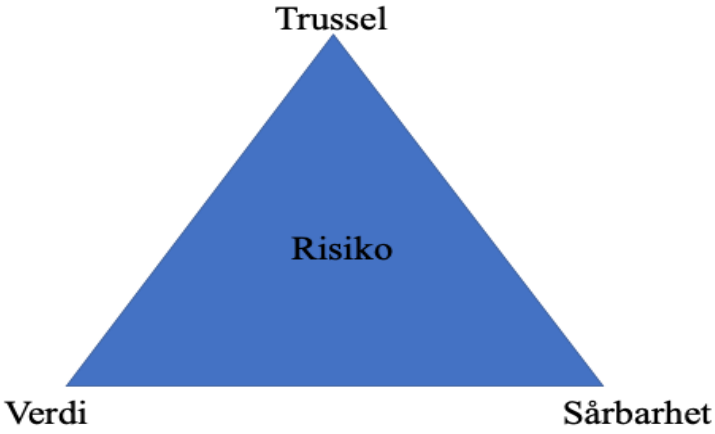
I denne tabellen blir det spesielt lagt fokus på risiko gjennom sannsynlighet og forventet tap, eller risiko gjennom hendelser/konsekvenser og usikkerhet (Aven & Renn, 2010, s. 3). En teknologisk definisjon av risiko kan relateres til de fire første tilnærmingene til risiko. Denne definisjonen tar for seg kombinasjonen av sannsynlighet og konsekvens som vil være et mål på virkningen av en hendelse. Sannsynligheten handler om hyppighet av hendelsen, mens konsekvensene sier noe om resultatet av hendelsen (Vatnelid, 2018, s. 17). Den teknologiske definisjonen av risiko blir forklart av Aven som et ingeniørperspektiv på risiko og er som følger (2015, s. 14):

«Risiko = forventet tap (tap multiplisert med sannsynlighet)»

Som en forskjell fra denne definisjonen, så vil et økonomisk perspektiv på risiko kunne inkludere faktoren om usikkerhet, og ta hensyn til uvitenhet om hva som kan bli konsekvensene av hendelsen. Usikkerhet blir også nevnt i de seks siste tilnærmingene som Aven og Renn presenterer i sin tabell. En definisjon som vil være fra det økonomiske perspektivet og som inkluderer usikkerhet har blitt utarbeidet av Aven og er som følger (2015, s. 41):

«Risiko = usikkerheten rundt forventningsverdien»

En annen tilnærming som skiller seg fra både ingeniørperspektivet og det økonomiske perspektivet på risiko, er en tilnærming som tar for seg forholdet mellom trussel, verdi og sårbarhet. Dette forholdet blir omtalt som risikotrekanten vist i figur 2.



Figur 2: Risikotrekanten (Nasjonal Sikkerhetsmyndighet, 2015)

Tilnærmingen til risiko er basert på at tilsiktede uønskede hendelser i de fleste er tilfeller uventet. Trusselbildet en organisasjon eller et samfunn må forholde seg til er derfor diffust og utenfor deres kontroll. Identifisering er en faktor som er gjeldende i denne tilnærmingen til risiko, hvor det bør være et kontinuerlig arbeid for å prøve å identifisere trusselbildet så langt det lar seg gjøre (Nasjonal Sikkerhetsmyndighet, 2015b, s. 12). De neste faktorene som er avgjørende i denne definisjonen er de faktorene som det er mulig å gjøre noe med. I denne definisjonen handler det om å identifisere verdier og arbeide for å redusere sårbarheten. Definisjonen til Nasjonal Sikkerhetsmyndighet (NSM) er som følger (2015a, s. 10):

«Forholdet mellom faktorene verdier, trusler og sårbarheter»

Disse tre faktorene trenger ikke nødvendigvis være likevektige. Det er organisasjonen eller virksomheten som bestemmer hvilken faktor de ønsker å vektlegge og fokusere på. Den vanlige tilnærmingen er å fokusere på verdi og sårbarhet, hvor faktoren trussel er en faktor organisasjonen ikke kan gjøre noe med (Nasjonal Sikkerhetsmyndighet, 2015b, s. 12). I denne oppgaven ville bruk av denne definisjonen vært mangelfull, fordi den ikke inkluderer aspektet hvor risiko er en hendelse eller en konsekvens av en hendelse. For at noe skal vurderes som risikabelt så må disse hendelsene og/eller konsekvensene være subjekt av usikkerhet, og at noe som er verdifullt for oss mennesker står på spill (Aven et.al., 2011, s. 1). I forskningen til Aven og Renn har de ikke funnet de nevnte definisjonene av risiko som fullstendige og presenterte derfor en ny som tar for seg både uønskede og ønskede resultater, fokus på usikkerhet og hvordan resultatet vil påvirke de berørte. Denne definisjonen er som følger (2010, s. 3):

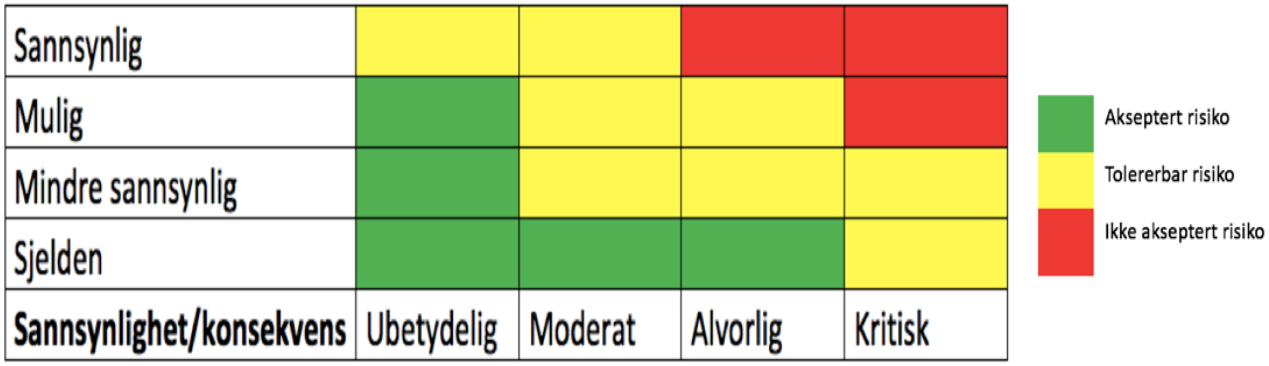
> *«Risiko refererer til usikkerhet om og alvorligheten av hendelser og konsekvenser (eller resultater) av en aktivitet med hensyn til det mennesker verdsetter.»*

Denne definisjonen av risiko er relevant i denne studien da den unngår en negativ realisme hvor risiko blir sett på som en objektiv kategori, eller at risikovurderinger er subjektive refleksjoner av makt og interesser. Ved å inkludere de nevnte komponentene så vil denne definisjonen kunne vurderes som tverrfaglig, noe som vil være høyst relevant til denne oppgaven hvor teknologiske-, økonomiske- og samfunnsvitenskapelige perspektiver inkluderes (Renn, 2008, s. 1-7).

Risikopersepsjon, -kompensasjon og -kommunikasjon

Hvordan man opplever, håndtere og aksepterer risiko er forskjellig fra person til person og kan variere fra situasjon til situasjon. Hvordan man opplever risiko vil påvirke hva man kan akseptere av risiko. Hva som er akseptabel risiko kan på mange måter sees i sammenheng med faktorer som verdier, tid og geografiske områder (Justis- og beredskapsdepartementet, 2012, s. 10-11). En måte å rangere risiko på er bruk av en risikomatrise med kategorisering av sannsynlighet og konsekvens. Sannsynlighet blir forklart av Aven som et uttrykk for usikkerhet. I defineringen av risiko så vi at sannsynlighet er en del av risikobegrepet, og sannsynlighet er en avgjørende faktor som åpner opp for forståelse av risiko. Sannsynlighet er basert på bakgrunnsinformasjon og kunnskap, og brukes som et hjelpemiddel for å vurdere

risiko (Aven, 2007, s. 747). Konsekvensen kan forklares som tap og resultat av hendelsen. Det kan resultere i form av tap i spesielle funksjoner, økonomisk tap, dårlig omdømme og nasjonale interesser. I oppgavens tilfelle vil det være konsekvenser knyttet til tilgjengelighet, konfidensialitet og integritet relatert til personvern og ansvarlighet (ibid., s. 746).



Figur 3: Risikomatrise (Justis- og beredskapsdepartementet, 2012)

Figur 3 viser hvordan en risikomatrise ser ut med skille mellom akseptabel risiko i fargen grønn, tolererbar risiko i fargen gul og ikke-akseptert risiko i fargen rød. Denne matrisen skal kunne brukes som et verktøy for å vurdere den risikoen man står ovenfor og videre kunne vurdere hvilke tiltak som bør implementeres for å håndtere risikoen. Dersom en risiko vurderes som ikke-akseptert, bør den aktiviteten som fører til denne risikoen fjernes. Hvis risikoen vurderes som tolererbar bør risikoreduserende tiltak gjennomføres, og dersom risikoen vurderes som akseptabel trengs ikke tiltak å implementeres. En slik risikomatrise vil som regel inngå i en risiko- og sårbarhetsanalyse (ROS-analyse) som brukes for å kartlegge risiko og sårbarheter (Justis- og beredskapsdepartementet, 2012, s. 10-11).

Den subjektive oppfattelsen av risiko handler om risikopersepsjon, og hvordan man velger å håndtere og akseptere denne risikoen handler om risikokompensasjon (Aven et.al., 2004, s. 40). Risikopersepsjon er den subjektive vurderingen av sannsynligheten om at en ulykke skal skje, og hvor bekymret vi er for konsekvensene av denne hendelsen (Sjöberg, Rundmo & Moen, 2004, s. 8). Risikokompensasjon handler om hvor mye man må kompensere for å få risikoen på det nivået man vurderer som akseptabelt. Det er vanlig å strebe etter balanse mellom oppfattet risiko og akseptabel risiko, som vil være en miks av risikopersepsjon og risikokompensasjon (Wilde, 1998). Risikokompensasjon vil på mange måter kunne ses på som en faktor som kan påvirke hvordan vi selekterer og oppfatter informasjon når det gjelder risiko (Engen et.al., 2014, s. 97). Det er flere faktorer som kan være med på å påvirke hvordan ens risikopersepsjon er, og hvordan man velger å akseptere denne risikoen. Dette kan være

faktorer som blant annet tillit, tro på egne ferdigheter og kompetanse, og ikke minst om man har stått i situasjonen før eller har måttet håndtert denne type risiko før (Knuth, Kehl, Hulse & Schmidt, 2014, s. 1287).

En viktig faktor som påvirker risikopersepsjonen til et individ er hvordan risikoen blir kommunisert. Risikokommunikasjon har som mål å gjøre et samfunn mindre sårbart ved å bruke kommunikasjon til å øke forståelsen for hva risikoen innebærer, samt forsøke å øke motstandsdyktigheten til befolkningen. Risikokommunikasjon kan på mange måter sies å ha fire roller. Den første er å opptre som en opplysningsfunksjon og gi ut informasjon, den andre er å forsøke å drive risikoreduksjon gjennom atferdsendring. Den tredje er å skape gode tillitsforhold, mens den fjerde er involvering av interessegrupper og berørte grupper i risikovurderinger. Ved å informere om risikoen man står ovenfor og hvilke konsekvenser dette får for sårbarheten vil dette kunne påvirke risikopersepsjon som resulterer i økt tillit til formidlerne. En stor del av risikokommunikasjon er nettopp dette: tillitsbygging. Tillit til den som formidler risikoen vil kunne bidra til demping av risiko, mens mistillit vil få motsatt effekt og vil kunne forsterke risikoopplevelsen (Renn, 2008, s. 201-204). I oppgavens tilfelle vil det være interessant å vurdere hvordan en bank som har kontakt med kunder kommuniserer om risiko. Ved å informere om den sårbarheten banken står ovenfor med økt digitalisering og nye lovgivninger vedrørende personvern, så vil måten dette formidles på trolig kunne ha stor betydning.

3.1.3 Sårbarhet

Sårbarhet er når et samfunn, land, aktivitet og personer står ovenfor en hendelse uten å vite kombinasjonen av mulige konsekvenser og tilhørende usikkerhet. Når vi snakker om risiko så nevnes ofte sårbarhet som et resultat av økt risiko. Risiko og sårbarhet går hånd i hånd, for når risikoen økes så økes også sårbarheten (Aven et.al., 2004, s. 124). Sårbarhetsutvalget valgte å legge frem en definisjon av sårbarhet slik (NOU, 2015:13, s. 31):

«*Et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet*»

En alternativ definisjon av sårbarhet er en forenklet versjon av sårbarhetsutvalget sin definisjon og legger vekt på forutsetninger og evner ved en uønsket hendelse (Engen et.al.,

2014, s. 47):

«Et systems forutsetninger for eller manglende evne til å fungere under og etter at det utsettes for en uønsket hendelse»

Denne definisjonen er lik Aven sin tilnærming av sårbarhet, hvor det forklares at dette er en faktor som ødelegger evnen til å stå imot en trussel eller komme tilbake til en stabil tilstand. Denne tilnærmingen til sårbarhet kan antas å være det samme som resiliens, som forklares som en motstandsdyktighet og en ny metode for risikohåndtering (Aven, 2018, s. 745). Sårbarhet er en del av risikohåndtering hvor en analyse av sårbarheter er implementert i en risikoanalyse. Årsaken til en slik analyse er for å kunne gi kunnskap i valg av metoder for å håndtere risiko. I en identifisering av sårbarhet kan ulike metoder benyttes, eksempelvis benytte seg av en sjekkliste for å finne sårbarheter med å se på egenskaper knyttet til både fysiske objekter, cyber nettverk og infrastruktur, men også menneskelige og sosiale faktorer (Aven, 2007, s. 751).

Sårbarhet kan betraktes som det motsatte av robusthet. Definisjonen til Renn kan brukes til både å definere sårbarhet og robusthet. Robustheten handler om den motstandskraften et system har mot en uønsket hendelse, og den evnen systemet har til å gjenoppta sin virksomhet etter at hendelsen har inntruffet. Robusthet kan på mange måter sies å gå hånd i hånd med sårbarhet, hvor økt sårbarhet reduserer robustheten i et system. Definisjonen er som følger (2008, s. 69):

«I hvilken grad det risikoabsorberende systemet reagerer på stress/påkjenninger påført av risikoagenten»

Selv om sårbarhet og robusthet går hånd i hånd, så er det også forskjeller. Sårbarhet kan forstås som en reaktiv egenskap i et system. Denne egenskapen er noe som kan utvikle seg over lenger tid, og som ofte ikke blir lagt merke til. Til motsetning fra dette er robusthet proaktivt, og det er en egenskap som er ønskelig å implementere inn i et system. Derfor kan forskjellen mellom sårbarhet og robusthet forklares som at robusthet er ønskelig, mens sårbarhet er noe man streber etter å redusere eller fjerne (Engen et.al., 2014, s. 47).

3.1.4 Usikkerhet

En del av forståelsen av risiko innebærer å forstå hva usikkerhet betyr. Når vi snakker om usikkerhet så handler det om at det foreligger en risiko i forhold til hendelser hvor konsekvensene av denne handlingen er ukjent. En kjent definisjon av usikkerhet blir presentert av Aven (2016):

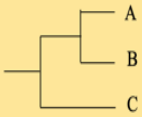
«Usikkerhet = ikke vite sann verdi av en størrelse eller fremtidige konsekvenser av en aktivitet»

Det kan skilles mellom to ulike typer usikkerhet som Renn kaller for *aleatory*- og *epistemic uncertainty*. Aleatorisk usikkerhet er usikkerhet basert på variasjon i kjente populasjoner og tilfeldigheter, mens epistemisk usikkerhet er usikkerhet som baseres på manglende kunnskap om kjente fenomener (Renn, 2008, s. 70-72). Usikkerheten som er basert på tilfeldigheter kan forklares gjennom terningkast, hvor man kan beregne sannsynlighet for hendelsen ved hjelp av probabilistiske modeller. Usikkerhet basert på mangel på kunnskap kan eksemplifiseres med klimaspørsmål, ny teknologi og økosystemet. Forskjellen på usikkerhet er at ved sistnevnte foreligger det en faktor hvor man ikke alltid er klar over hvilken usikkerhet man kan forvente (Lindøe, Kringen & Braut, 2012, s. 63). Ved hjelp økt kunnskap om aktiviteten vil man kunne få mer informasjon som reduserer denne usikkerheten, men selve usikkerheten vil man aldri bli kvitt dersom hendelsen ikke har skjedd før. Dersom lignende hendelser har skjedd før så kan man forberede seg i forhold til beredskap, noe som er relevant i forhold til den førstnevnte type usikkerhet (Renn, 2008, s. 70-72).

En annen tilnærming til usikkerhet poengterer at usikkerhet ikke bare handler om mangel på informasjon. Det kan også være usikkerhet i situasjoner hvor man har mye informasjon, og denne informasjonen kan også være årsaken til økt usikkerhet. Dette er spesielt gjeldende i komplekse systemer, og derfor er denne tilnærmingen til usikkerhet gjeldende i denne studien (Walker, Harremoes, Romans, van der Sluijs, Van Asselt, Janssen & Krayer von Krauss, 2003, s. 8). Determinisme handler om å finne den ideale situasjonen hvor man har nøyaktig informasjon om absolutt alt. En definisjon av usikkerhet som tar for seg dette aspektet ser slik ut (ibid., s. 12):

«..any departure from the unachievable ideal of complete determinism»

Denne tilnærmingen handler om å strebe etter full sikkerhet, og vil argumenteres for å være et uoppnåelig ideal (Walker, Lempert & Kwakkel, 2016, s. 2-3). I tilnærmingen til usikkerhet legger Warren Walker med flere (2003) frem en teori om å kategorisere usikkerhet. Med full sikkerhet på den ene polen og total uvitenhet på den andre, er to ekstreme nivåer blitt etablert. Både full sikkerhet og total uvitenhet er å anse som idealer og som sjelden, om ikke aldri, oppstår. I figur 4 nedenfor vises de fem nivåene av usikkerhet som står rangert mellom full sikkerhet og total uvitenhet (ibid., s. 3-4). Hensikten med en slik kategorisering er å forbedre kommunikasjonen angående usikkerhet hvor man har en felles tilnærming til usikkerhet. En felles tilnærming vil også gjøre det lettere å identifisere og effektivisere prioritering av håndteringen av usikkerhet (Walker et.al., 2003, s. 6).

	Kontekst	Systemmodell	Systemutfall	Konsekvenser	
Nivå 1	En klar nok fremtid 	En enkelt systemmodell	Punktestimater med følsomhet	Et enkelt estimat av konsekvenser	***Total sikkerhet***
Nivå 2	Alternativ fremtid med sannsynligheter 	En enkelt systemmodell med en probabilistisk parametrisering	Flere sett med punktestimater med konfidensintervall med sannsynlighet knyttet til hvert sett	Flere sett med konsekvenser med en sannsynlighet knyttet til hvert sett	
Nivå 3	Alternativ fremtid med rangeringer 	Flere systemmodeller hvor en modell er mest sannsynlig	Flere sett med punktestimater rangert etter deres oppfattede sannsynligheter	Flere sett med konsekvenser rangert etter deres oppfattede sannsynlighet	
Nivå 4	Et mangfold av troverdige alternativ uten rangeringer 	Flere systemmodeller med forskjellige strukturer	Et kjent utvalg av resultater	Et kjent utvalg av resultater	
Nivå 5	Ukjent fremtid 	Ukjent systemmodell	Ukjente systemutfall	Ukjente konsekvenser	***Total uvitenhet***

Figur 4: Nivå av usikkerhet (Walker et.al., 2003)

Håndtering av usikkerhet blir diskutert i artikkelen til Raanan Lipshitz og Orna Strauss som ble publisert i 1997. Artikkelen hadde som mål om å besvare spørsmål relatert til årsak-, håndtering- og konseptualiseringen av usikkerhet. Definisjonen av usikkerhet som Lipshitz og

Strauss baseres på deres forskning er som følger (1997, s. 150):

«Doubt that threatens to block action»

Med denne definisjonen så vil usikkerhet forklares som en tvil som truer en bestemt handling. Måten man håndterer usikkerhet på er å møte usikkerheten med å innhente mer informasjon, eller å prosessere informasjonen som er hentet inn på en bedre måte. Deres definisjon av usikkerhet er basert på fokus på beslutningstaking. Årsaken til denne kategoriseringen er for å kunne håndtere en usikkerhet, så må den kategoriseres og forstås før man kan implementere ulike strategier for å redusere usikkerhet. Den første og vanligste typen usikkerhet handler om utilstrekkelig forståelse, og bør ifølge Lipshitz og Strauss kunne håndteres med fokus på å redusere usikkerheten (1997, s. 158). Usikkerhet på bakgrunn av mangel på informasjon bør anerkjennes, mens usikkerhet basert på motstridende alternativer bør håndteres med diskusjon av for og imot (ibid., s. 149).

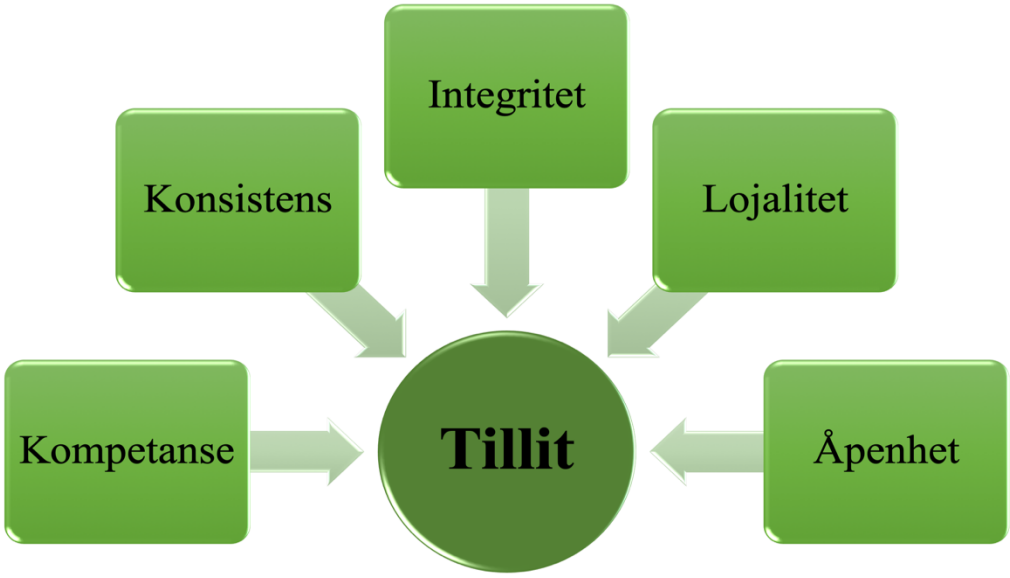
3.1.5 Tillit

For å kunne opprettholde robustheten og motstandsdyktigheten i et samfunn så er tillit sentralt (Engen et.al., 2014, s. 49). Tillit er noe man har og det kan være til både institusjoner, organisasjoner og systemer, men det kan også være noe medmenneskelig og noe man har til «folk flest» (Skulberg, 2017). En vanlig definisjon av tillit ble i 1998 presentert av Denise M. Rousseau, Sim Sitkin, Colin Farrell Camerer og Ronald S. Burt og er som følger:

«Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another»

Denne definisjonen fremmer at å ha tillit til noe eller noen er en psykologisk tilstand, hvor personen som har tillit er innforstått med å være sårbar. Tillit handler om et menneske sine følelser av andre sin godhet, ærlighet og dyktighet som resulterer i at man velger å ha tillit til dem. Når man har tillit til noe eller noen så foregår det en overføring av makt da de man har tillit til skal handle på andre sine vegner med en forventning om å handle i deres beste interesse. Tillit er noe som oppstår over tid og skapes av trygghet (Skulberg, 2017).

For å kunne skape et godt tillitsforhold så er det enkelte kjerneelementer som må ligge til grunn. Figuren 5 viser til fem elementer som kan forstås som elementer som utgjør at det er mulig å skape et tillitsforhold.



Figur 5: Kjerneelementer i tillit (Kaufman & Kaufman, 2015)

Elementet integritet betyr at den man har tillit til skal vise til at det er samsvar mellom hva som blir sagt og hva som blir gjort. Dette elementet kan oppfattes som et kritisk element da det ligger til grunn for å måle troverdighet. Kompetanse er et element som også må ligge til grunn hvor det viser til en person eller en organisasjon sine kunnskaper og ferdigheter. Det tredje elementet er konsistens som handler om en person sin forutsigbarhet, mens det fjerde elementet er lojalitet. Med lojalitet som betyr det at det skal representere en villighet til å stille opp for noen andre og ikke vil handle opportunistisk. Det siste kjerneelementet for tillit er åpenhet, og åpenhet handler om å skape trygghet gjennom ærlighet (Kaufman & Kaufman, 2015, s. 82)

Det kan skilles mellom generalisert-, intergruppe- og institusjonell tillit. Generalisert tillit til noen man ikke kjenner personlig, mens partikulær tillit er tillit til folk man kjenner personlig. Intergruppe tillit er tillit mellom sosiale identitetsgrupper i samfunnet. Institusjonell tillit er den siste typen tillit, og det er den som er mest relevant til denne oppgaven. Det er tillit til at samfunnets organisasjoner, institusjoner og sosiale systemer fungerer. Denne type tillit kan være basert på tre ulike typer tillitsrelasjoner som derrent-, kunnskapsbasert- og identifikasjonsbasert tillit. Ved institusjonell tillit så baseres det hovedsakelig på

kunnskapsbasert tillit som er basert på erfaringer, mens identifikasjonsbasert tillit som handler om gjensidig forståelse og verdsettelse (Kaufman & Kaufman, 2015, s. 84).

Tillit relatert til risiko og samfunnssikkerhet kan forklares på denne måten: «A sin forventning er at B ikke vil skade A, selv om B er i stand til det». I denne forbindelse så vil kjerneelementene i tillitsrelasjonen være basert på sårbarhet, risiko og usikkerhet. Sårbarheten er hos A da det er den som gir tillit, risikoen er ved å eksponere disse sårbarhetene overfor den som mottar tillit, mens usikkerheten ligger i at A ikke kan kontrollere B sin respons (Kaufman & Kaufman, 2015, s. 83). Denne type forståelse for tillit sammen med en institusjonell tilnærming til tillit er det som legger grunnlaget for videre diskusjon av tillit i denne oppgaven. Et slik tillitsforhold er noe som oppstår over tid og påvirkes av risikokommunikasjon (Engen et.al, 2014, s. 49).

3.1.6 Kultur

Kultur er et begrep som er mye brukt i ulike settinger, og det har flere ulike betydninger. Måten man kan forstå kultur vil avhenge av hvilken sammenheng begrepet brukes i. En av de mest tradisjonelle måtene å definere kultur på er Edward B. Tylor sin definisjon hentet ut fra det antropologiske forskningsfeltet. Denne definisjonen er fra 1871, men kan likevel fortsatt sies å være relevant. Kultur av Tylor blir definert på følgende måte:

«That complex whole which includes knowledge, belief, art, morals, law custom and any other capabilities and habits acquired by man as a member of society»

En annen tilnærming til en definisjon av kultur ble presentert av James Reason i 1997 knyttet til hans studie om teknologiske ulykker. I den forbindelse definerte han organisatorisk kultur på følgende måte (1997, s. 192):

«Shared values and belief that interact with an organization`s structures and control systems to produce behavioral norms».

Denne tilnærmingen til kultur er knyttet til organisasjoner og fokuserer på hva som er viktig, hvordan ting fungerer og hvordan ting fungerer innad i organisasjonen. Slik som flere andre begreper så er kultur og organisasjonskultur vanskelig å definere, både på bakgrunn av stor uenighet og stort mangfold i ulike tilnærminger. De nevnte definisjonene blir likevel brukt i

denne oppgaven som en terminologiforståelse uten videre diskusjon, og de begrepene legger grunnlaget for å kunne diskutere sikkerhetskultur. En sikkerhetskultur er den delen av organisasjonskulturen som har innvirkning på sikkerheten i en kultur. NSM definerer sikkerhetskultur på denne måten (2014):

«Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd»

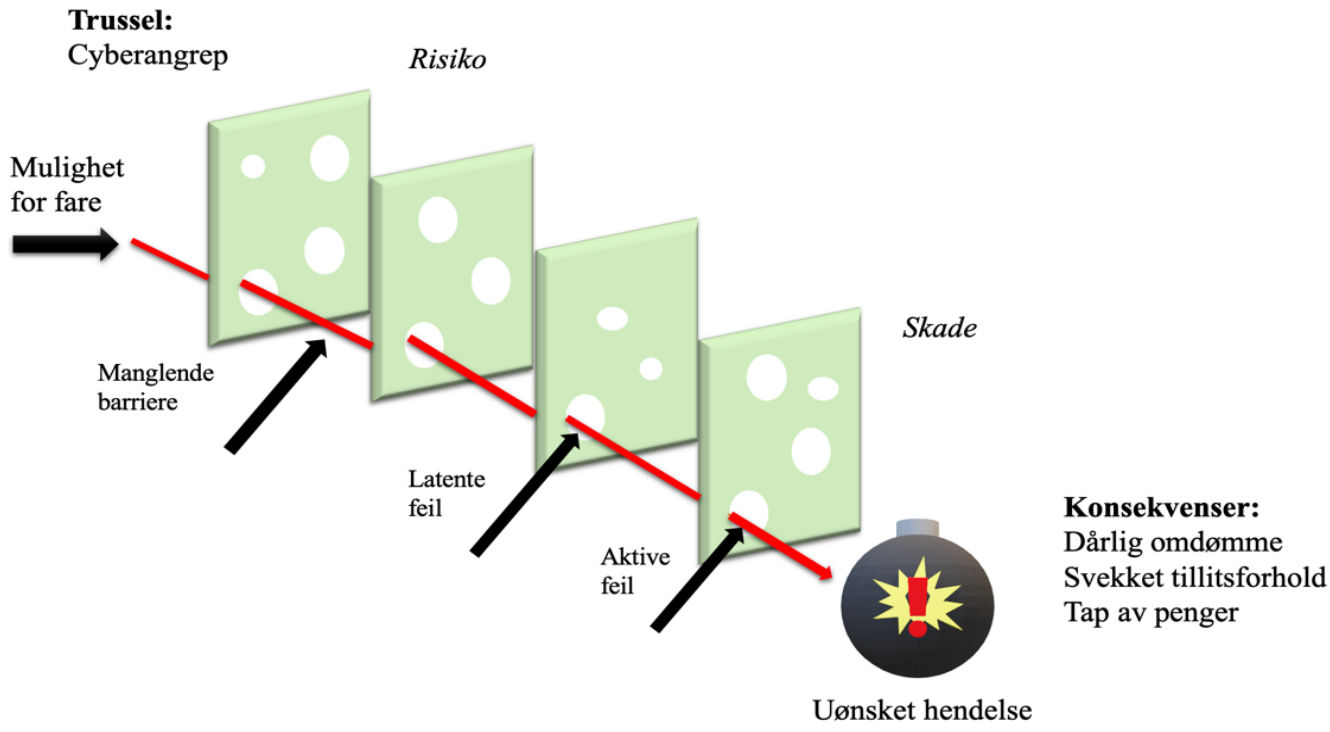
For å skape en sterk sikkerhetskultur så må det være en felles annerkjennelse av mål, normer og verdier på alle nivåer i organisasjonen (Reason, 1997, s.193). Alle organisasjoner har en form for sikkerhetskultur, og om den er god eller dårlig vil først være avgjørende dersom et sikkerhetsbrudd eller uønsket hendelse truer sikkerheten (Nasjonal Sikkerhetsmyndighet, 2014).

3.2 Sikkerhetskultur

Teknologiske uønskede hendelser er sjeldne, men kan oppstå innenfor komplekse, moderne systemer som kan få fatale konsekvenser. Uønskede hendelser i komplekse, moderne systemer kan få stort skadeomfang og kan resultere i ringvirkninger til andre personer/organisasjoner som i utgangspunktet ikke var involvert i hendelsen. Teknologiske uønskede hendelser er noe som har blitt mer vanlig i moderne tid, hvor systemer har blitt mer og mer komplekse. Det er vanskelig å forstå og kontrollere disse typer hendelser, for de oppstår sjelden, har ulike mønstre og er vanskelige å forutse (Reason, 1997, s. 1-2). Hvorfor de oppstår, hvordan de kan forhindres og hvordan de kan forebygges, er forsøkt å bli forklart av flere teoretikere ved bruk av ulike metoder.

Reason sin forskning, presentert i 1997, er basert på forståelsen av hvorfor teknologiske ulykker skjer, og hva man kan gjøre for å forhindre at de skal oppstå. Hans teori baserer seg videre på individuelle, menneskelige feilhandlinger som ofte kan være utløsende til at teknologiske uønskede hendelser oppstår, men at disse ikke er forskyldt mennesket i seg selv. Menneskelige feil kan forklares som en feil som resulterer i at en planlagt sekvens ikke klarer å oppnå det tiltenkte resultatet, og det er ikke basert på tilfeldigheter. To viktige begreper Reason bruker i sin forklaring av uønskede hendelser i teknologiske systemer er “aktive” og

"latente feil" (1997, s. 11-12). Aktive og latente feil bidrar til at mennesket gjør feilgrep. En aktiv feil er den utløsende årsaken til at en uønsket hendelse oppstår. Slike feil er ofte individuelle feil forårsaket av dårlige arbeidsforhold og -betingelser. En aktiv feil er i utgangspunktet ikke en feil som vil utløse en uønsket hendelse alene, men kan være avgjørende i et system hvor det foreligger latente feil som anses å være høyst alvorlig (ibid., s. 11). Latente feil er feil som ikke blir satt frem i lyset og som virker i det skjulte (Gundersen, 2018). En latent feil er en underliggende årsak som man ikke har kontroll over, og det er disse som ofte blir omtalt som de største sikkerhetstruslene i komplekse systemer. Grunnen til det er fordi de er skjulte og ukjente, og kan potensielt få katastrofale følger. Disse to typene feil henger sammen hvor latente feil omtalt i "the blunt end" utløses av aktive feil i "the sharp end" (Reason, 1997, s. 11).

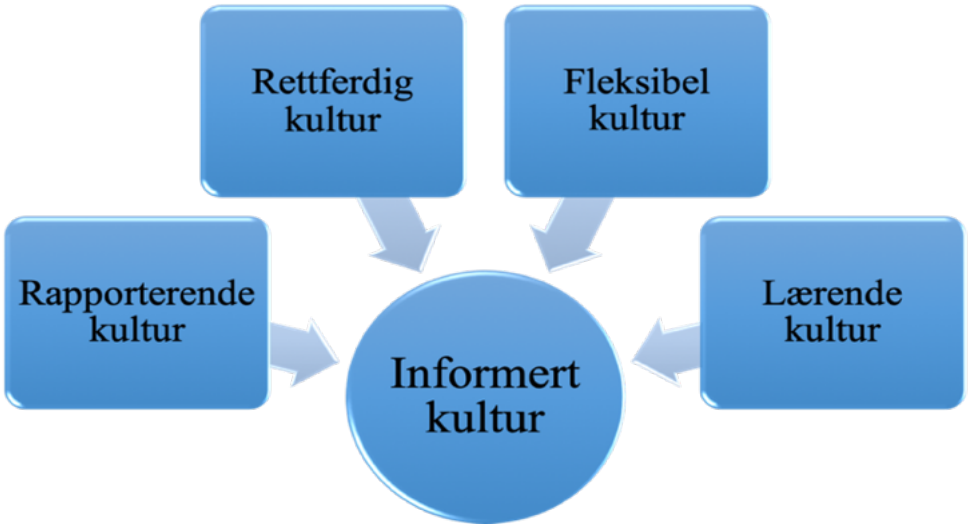


Figur 6: Sveitserostmodellen (Reason, 1997)

Reason sin teori er basert på sveitserostmodellen hvor sikkerhetsrutinene og beskyttelsen i en organisasjon i utgangspunktet ikke skal ha svakheter i barrieren (1997, s. 12). En barriere er et element som enkeltvis eller til sammen skal bidra til å redusere muligheten for at konkrete feil skal resultere i uønskede hendelser. De kan være tekniske, operasjonelle eller organisatoriske, og skal kunne begrense eller forhindre skader (Vatnelid, 2018, s. 122). Hullene som vises i sveitserostmodellen oppstår på grunn av aktive og latente feil. Hullene som oppstår på grunn

av latente feil kan være beslutninger tatt på grunnlag av design, systemet i seg selv og ledelsen. Disse hullene kan fremprovosere feil som kan bli "fastboende" i systemet som for eksempel tidspress, underbemanning og mangel på utstyr, og langvarige hull i systemets forsvar gjennom upålitelige alarmer, manglende prosedyrer og svake indikatorer. Aktive feil i slike systemer kan være glipper, blundere, feil, mangler eller brudd på prosedyrer. Disse oppstår når mennesket har direkte kontakt med systemet. Når de aktive feilene utløses og det foreligger flere hull på en linje så vil den aktive feilen trigge latente feil som utløser en uønsket hendelse (Reason, 2000).

Ettersom at systemer har blitt mer komplekse, så har dette ført til at flere latente feil oppstår. I utgangspunktet vil det ikke være skadelig med latente feil i systemet, men faren oppstår når flere latente feil står på rekke og rad. Da vil ikke barrierene kunne opptre som beskyttelse, sikkerheten i systemet vil svekkes og faren for at uønskede hendelser skal utløses på grunn av aktive feil økes (Reason, 1997, s. 12). De latente feilene kan forøvrig forebygges og forhindres, slik at aktive feil ikke får like fatale konsekvenser som kan være mulig. Reason er en av flere teoretikere som argumenterer for at fokus på sikkerhetskultur i organisasjoner som har komplekse systemer, vil være forebyggende for uønskede hendelser. Det Reason kaller for en god sikkerhetskultur er en informert kultur. Når en informert kultur forklares så er det fire faktorer som er viktige for at kulturen i en organisasjon skal være informert, slik som figur 7 viser (Reason, 1997, s. 192).



Figur 7: Sikkerhetskultur (Reason, 1997)

3.2.1 En rapporterende kultur

Å ha en rapporterende kultur handler om at de ansatte skal rapportere feil, avvik og hendelser som vil ha påvirkning til eventuelle fremtidige uønskede hendelser. Gjennom rapportering skal det være mulig å forhindre at latente feil blir liggende i systemet og bidra til svikt. For at man skal kunne rapportere inn når man gjør feil, så er det essensielt at ledelsen legger opp til motivasjon og velvillig deltakelse. Å være ærlig når man gjør en feil er ikke alltid den enkleste handlingen og ærlige tilståelser er ofte vanskelige. Frykten for straff gjør at flere kvier seg fra å rapportere, enten det er straff for seg selv eller kollegaer. Det er ledelsen som er ansvarlige for å skape et miljø hvor det er akseptabelt å rapportere inn feil. Reason presenterer fem faktorer til hvordan ledelsen kan bidra til å motivere de ansatte til å rapportere:

1. Beskytte ansatte mot disiplinære konsekvenser så langt det gjør seg mulig.
2. Mulighet til å rapportere anonymt.
3. Ha en egen gruppe som evaluerer og analyserer rapportene som er uavhengig av de som har myndighet til å gi disiplinære konsekvenser.
4. Tilbakemeldinger skal skje effektivt.
5. Det bør være enkelt å rapportere uønskede hendelser.

Fokuset må være åpenhet og fremme et fokus på sikkerhet, enn fokus på straff og skyld (Reason, 1997, s. 196-204).

3.2.2 En rettferdig kultur

Rettferdighet er en viktig faktor som bidrar til å skape en god kultur i organisasjoner. Tradisjonelt sett så kan rettferdighet defineres slik som dette (Sagdahl, 2016):

«Den type forhold der mennesker behandles på en rimelig måte og i overensstemmelse med moralske prinsipper»

Denne tilnærmingen til rettferdighet er den som ligger til grunn for å skape rettferdighet i en organisasjon som fokuserer på å danne en sikkerhetskultur. Ulikheter mellom ansatte kan skape uro og vil øke mistilliten til ledelsen. Det er derfor viktig med fokus på å skape en rettferdig kultur hvor det er en atmosfære av tillit, og hvor de ansatte blir oppmuntret til å informere om relevant sikkerhetsrelatert informasjon og kunnskap. Slik som i mange andre situasjoner så er 100% rettferdig så og si umulig, og Reason legger til grunn at dette er også uoppnåelig i organisasjoner med komplekse systemer. Det er derfor viktig at ledelsene i

sammen med de ansatte skaper enighet om hvor linjen skal gå mellom hva som er akseptable og uakseptable handlinger basert på intensjon, handling og konsekvenser. Det bør etableres et skille mellom hvilke hendelser ledelsen skal gi straff for, og hva man skal la gå ettersom det kan bidra til å forhindre uønskede hendelser i lengden. Dette kan gjøres gjennom å skille mellom hendelser som er gjort på bakgrunn av dårlige intensjoner, og hendelser som er på bakgrunn av en uskyldig feil. Dette kan bidra til å gjøre det mer effektivt for ledelsen å vite når man skal gi sanksjoner, og når dette ikke vil være hensiktsmessig (Reason, 1997, s. 205-212).

3.2.3 En fleksibel kultur

Fleksibilitet kan forstås som å være tilpasningsdyktig og ses på som en evne til å være tilbøyelig (Malt, 2018). Når ny informasjon blir tilgjengelig handler det om å håndtere informasjonen på korrekt måte, og implementere forandringer så fort som mulig. Dette gjør at organisasjoner med komplekse systemer bør ha en fleksibel kultur. Med dette mener Reason at det bør være et mål å skape en fleksibilitet hvor det er en flat byråkratisk ledelse med fokus på kollegial autoritet og lite formalitet når det gjelder rang og roller. Det må være en evne til å tilpasse seg og en effektivitet til å kunne endre prosedyrer på en rask, men ordentlig måte. Reason argumenterer også for at valg og avgjørelser bør tas av den som har best og mest kompetanse på det området som diskuteres, men at kommunikasjon og samarbeid også skal kunne bidra til å skape et miljø med profesjonalisering av teamsamarbeid (1997, s. 213-218).

3.2.4 En lærende kultur

En lærende kultur er på mange måter den enkleste kulturen å etablere innenfor en organisasjon. Dette omfatter en informasjonshåndtering gjennom blant annet observasjon, analyser og tolkning gjennom refleksjon, planlegging og design, og handling gjennom gjennomførelse og testing. En lærende kultur åpner opp for at det skal være lov å gjøre feil så lenge det foreligger en åpenhet om rapportering. Dette vil kunne bidra til at både de ansatte og ledelsen skal få mulighet til å få et læringsutbytte av hendelsen. En lærende kultur vil også innebære at de ansatte og ledelsen er kritiske til den eksisterende praksisen, slik at man har vilje til å kunne implementere nye endringer, tiltak og reformer. For å vurdere om en organisasjon har en lærende kultur så bør det evalueres om i hvilken grad organisasjonen er i stand til å lære av egne feil for å unngå uønskede hendelser (Reason, 1997, s. 218-220).

3.2.5 En informert kultur

Organisasjoner som har en informert kultur vil gjøre at de ansatte stadig søker etter ny informasjon for å øke sikkerheten. Gjennom ny informasjon kan organisasjonen få muligheten til å implementere eventuelle nye revisjoner og justeringer i de prosedyrene og de arbeidspraksisene organisasjonen har for å ivareta sikkerheten (Reason, 1997, s. 197). Når en organisasjon har oppnådd det Reason kaller en informert kultur, så har organisasjonen og de ansatte hatt som mål om å ha den beste og mest oppdaterte kunnskapen om den informasjonen om sikkerhet som er tilgjengelig. Gjennom innhenting av data om hendelser som har en påvirkning på sikkerheten, så gjør organisasjonen det mulig å implementere proaktive tiltak for å øke sikkerheten. For at dette skal være oppnåelig må alle de fire faktorene være bidragsytere. Gjennom å ha en ideell informert kultur så skal kulturen fungere som en sikkerhetsstrategi som driver organisasjonen og dets systemer mot et mål om full sikkerhet. En sikkerhetskultur som fungerer slik som dette er verd å strebe etter hvor kulturen skal forhindre at uønskede hendelser oppstår som resultat av at barrierer har blitt nedbrutt (1997, s. 192-197).

3.3 Resilience Engineering

I 2018 ble det gjennomført en test av resiliens i banker i Storbritannia. Målet med testen var å observere evnen til å stå imot cyberangrep og se hvor lang tid det tok før bankene var tilbake til normaltilstanden. Det var Bank of England og det britiske National Cyber Security Centre som var ansvarlige for testen, hvor testen skulle bidra til å gjøre britiske banker klar over de sårbarhetene de står ovenfor. Et viktig resultat som ble publisert etter testen var frykten for en «ripple-effect», hvor angrep på en bank kan få katastrofale konsekvenser for andre banker og finansnæringen på grunn av den raske spredningen (Monaghan, 2018).

Slik som eksempelet ovenfor viser så har det i nyere tid blitt et miljøskifte i fokus på sikkerhet. Fokuset har flyttet seg fra å fokusere på reaktive barrierer og forsvar til sikkerhetsstyring gjennom resiliente prosesser. Det har i lang tid vært fokus på å søke etter måter hvor begrenset og uregelmessig menneskelig ytelse kunne skape feil i systemer. Denne tilnærmingen har blitt endret til å fokusere på at sikkerhetsstyring er avhengig av at arbeidstakere og ledere er stadig oppdaterte på endring i sårbarheter, og får oppdatert informasjon som vil påvirke deres evne til å utvikle metoder for å kunne møte de nye

sårbarhetene (Hollnagel & Woods, 2006, s. 3-5). For å kunne forstå hva resilience engineering (RE) er og innebærer så er det enkelte begreper som må redegjøres for først.

3.3.1 Resiliens

Når sårbarhet og robusthet diskuteres så har resiliens vokst frem som et sentralt begrep. En enkel forklaring på resiliens er å forstå det som en motstandsdyktighet, og en kjent definisjon av resiliens er (Engen et.al., 2014, s. 48):

> *«Den kapasitet et sosialt system har til å motstå og tilpasse seg forventede og uforventede forstyrrelser, og til å gjenopprett funksjonaliteten etter alvorlige påkjenninger fra slike forstyrrelser»*

Slik som de fleste andre begreper og fenomener som skal defineres så oppstår det uenighet. Begrepet resiliens skiller seg ikke fra andre begreper her og dette kommer klart frem i studiene til Erik Hollnagel. Tidlig på 2000-tallet presenterte han sin første definisjon av resiliens, men har gjennom sine studier av RE videreutviklet sitt syn på denne definisjonen. Han startet med å forklare resiliens som et alternativt syn på sikkerhet, men fant ut at resiliens ikke bare handlet om svakheter og feil. Videre så han også mangler hvor han ikke lenger kun hadde fokus på en dynamisk tilstand, men også på å kunne opprettholde funksjonaliteten (2017, s. 14-15). Hollnagel sin siste definisjon av resiliens presenterer han i boken sin i 2017, og er som følger (s. 15):

> *"Resilience is an expression of how people, alone or together, cope with everyday situations – large and small – by adjusting their performance to the conditions. An organisation's performance is resilient if it can function as required under expected and unexpected conditions alike (changes/ disturbances/opportunities)"*

Resiliens kan forstås på tre ulike måter, som proaktiv, reaktiv og resiliens basert på improvisasjon. Proaktiv resiliens handler om tilpasning forut en alvorlig hendelse. Dette betyr at man har evne til å tilrettelegge og håndtere endringer uten at det skal være en katastrofe, en feil eller en ulykke som har forårsaket endringen. En annen type resiliens handler om gjenoppretting og kan forstås som en evne til å respondere på og raskt komme tilbake til normaltilstand etter en uønsket hendelse. Resiliens basert på improvisasjon der bruk av kreative metoder brukes for å håndtere situasjoner man ikke forventet skulle oppstå (Engen

et.al., 2014, s. 153-154).

Hollnagel sitt fokus på resiliens tar også for seg at resiliens ikke handler bare om hvordan en organisasjon arbeider for å opprettholde sikkerheten, men også hvordan organisasjonen utfører alle former for aktiviteter (2017, s. 15). I RE forstås resiliens som en måte man utfører oppgaver på, og fokuset går ut på organisasjonens mulighet for å utføre oppgaver på en resilient måte og organisasjonens potensiale for resiliens (Hollnagel, 2017, s. 15). En organisasjon kan ikke være motstandsdyktig, hvor dette er en måte å håndtere aktiviteter på. Resiliens i en organisasjon er noe man kontinuerlig streber etter (Hollnagel, 2015, s. 1).

3.3.2 Paradigmeskiftet: fra safety-I til safety-II

En stor del av teorien om RE innebærer det å være «safe» og ha fokus på «safety». Direkte oversatt så betyr «safe» det å være sikker eller trygg. Det Hollnagel forklarer som «safe» er utfallet av en aktivitet som er blitt gjennomført på den måten man ønsket det skulle bli gjennomført på. Dette betyr at alt vil gå slik som det skal og aktiviteten kan forklares som en suksess (Hollnagel, 2014, s.3). Begrepet «safety» har også en egen betydning, og blir generelt forklart som fraværet av uønskede utfall av aktiviteter. Denne forklaringen kan se på som en henvisning til det å være «safe». Hollnagel presenterer en definisjon som inkluderer flere detaljer for å gjøre definisjonen mer relevant til RE. Definisjonen er som følger (2014, s. 1):

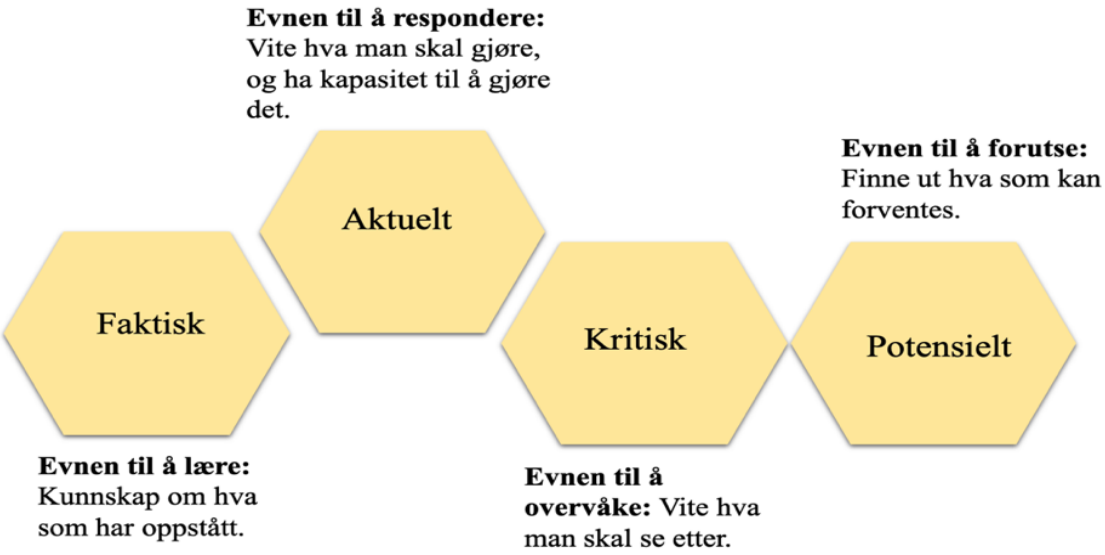
«Safety is the system property or quality that is necessary and sufficient to ensure that the number of events that could be harmful to works, the public, or the environment is acceptably low»

Hollnagel skiller mellom safety-I og safety-II. RE har lenge argumentert for at safety-I perspektivet er for *«oversimplified and misdirected»*. På grunn av den sosial-økonomiske og teknologiske utviklingen som fortsetter å vokse og bli mer og mer komplisert og kompleks, er det nødvendig å også utvikle de metodene som brukes til å styre disse systemene. Den ideen som ble presentert i safety-I er ikke lenger kapabel til å levere de nødvendige strategiene som er nødvendig for å drive sikker sikkerhetsstyring. Synet på sikkerhet ble endret fra safety-I til safety-II med fokus på å gå fra *«avoiding that something goes wrong»* til *«ensuring that everything goes right»* (Hollnagel, 2016). Årsaken til denne endringen er at ved å fokusere på at ting går bra, så gjør det at mennesker blir bedre til å forholde seg til endringene som stadig oppstår. For at dette skal fungere så bør det være eksiterende på alle nivåer i en organisasjon,

fra de administrerende direktører til sekretærer til renholdsarbeidere. Gjennom denne tilnærmingen vil de ansatte lettere merke når noe er på vei til å gå galt, og de vil øyeblikkelig gå inn og gjøre endringer for å forhindre at uønskede hendelser ikke oppstår. Dette er en proaktiv metode å drive sikkerhetsstyring på, og gjennom et safety-II perspektiv vil sikkerhetsstyringen ha stadig fokus på det som går godt og at den daglige driften fungerer bra (Hollnagel, 2016). Safety-II er ikke direkte RE, men RE vil være en tilnærming av safety-II med elementer fra safety-I. Disse begrepene er kun forståelser av hva som er sikkerhet, mens det er RE som legger frem en strategi og plan for hvordan man skal drive sikkerhetsstyring.

RE er et paradigme for sikkerhetsstyring som fokuserer på hvordan å hjelpe mennesker til å takle press i komplekse situasjoner for å kunne oppnå suksess. En organisasjon som fokuserer på RE har høyt fokus på sikkerhetsstyring. Hensikten med RE er å forsikre seg om at organisasjoner har mulighet til å arbeide effektivt i hverdagslige tilstander, samtidig som de skal ha evnen til å håndtere situasjoner som ikke tilhører den hverdagen de er vant til. Målet med RE er å kunne ha den evnen til å håndtere de uforventede hendelsene både når de har mulighet til å skape brudd i systemet og når de gir muligheter til forbedring (Hollnagel, 2017, s. 15).

Tre trinn må etableres for å kunne utvikle RE. Disse trinnene er først og fremst å analysere, måle og overvåke den nåværende resiliensen som allerede er i deres organisasjon. Det neste trinnet handler om å sette fokus på å forbedre organisasjonens resiliens, mens det siste trinnet tar for seg å vurdere de kort- og langsiktige effektene av endringen og styringen i organisasjon basert på resiliens og risiko (Hollnagel & Woods, 2006, s. 6). For å kunne bli motstandsdyktig og øke den resiliensen organisasjonen har til å stå imot uønskede hendelser, så handler det om å være kapabel til å justere seg. Denne justeringen kan være proaktiv og reaktiv, som betyr at man skal ha evne til å justere seg både før og etter en hendelse. Ifølge Hollnagel er et resilient system basert på fire grunnleggende egenskaper. Disse fire egenskapene er evnen til å «respond», «monitor», «anticipate» og «learning». Det er ikke mulig å ha et resilient system med mindre man har alle de fire egenskapene, hvor de er alle gjensidig avhengige av hverandre (Hollnagel, 2015, s. 3). Figur 8 viser til de fire egenskapene: evnen til å respondere det aktuelle, evnen til å lære det faktiske, evnen til å overvåke det kritiske og evnen til å forutse det potensielle. Disse egenskapene danner grunnlag for videre vurdering av empirisk datainnsamling.



Figur 8: Egenskaper i RE (Hollnagel, 2015)

3.3.3 Evnen til å respondere

Den første egenskapen er «the ability to respond», som betyr evnen til å respondere og reagere. Evnen til å reagere og respondere handler hovedsakelig om håndtering ved å ha fokus på gode handlinger i øyeblikket. Som en resilient organisasjon skal man ha evnen til å handle på det riktige tidspunktet og ha evnen til å vite når dette tidspunktet er. For å kunne etablere en slik evne så må organisasjonen og dens ansatte ha en god situasjonsvurdering og håndtere de mest aktuelle endringene. Ved å ha en slik evne så vil organisasjonen oppleves som å være god på resiliens i øyeblikket. Et annet aspekt ved evnen til å respondere handler om å vite når ressursene i systemet er mangelfulle. Organisasjonen skal ha en evne til å kunne vite om barrierene og sikkerhetssystemene er kapable til å håndtere den vurderte sårbarheten. Dette er evnen til å respondere på regulære og irregulære trusler på en fleksibel og robust måte. Den viktigste faktoren ved evnen til respons er å vurdere om de evnene organisasjonen har er fullkomne, og vet hvordan man skal håndtere forandringer i organisasjonens systemer (Hollnagel, 2011, s. 284-286).

3.3.4 Evnen til å overvåke

Når en organisasjon har evnen til å overvåke, «the ability to monitor», innebærer dette at organisasjonen først og fremst har kunnskap om hva som skal overvåkes. For å kunne etablere en slik kontroll så må organisasjonen har god kunnskap om hva som er omgivelsene, det fysiske miljøet rundt og i organisasjonen, og vite hva som kan påvirke organisasjonen og dens

systemer. Når en organisasjon har overvåkning som en del av deres arbeidsoppgaver så må de også ha en evne til å kunne bruke denne informasjonen på riktig måte, og vite om denne informasjonen vil ha en positiv eller negativ effekt på systemet. Kunnskap er en av de viktigste verktøyene en organisasjon må ha for å kunne ha evnen til å overvåke. Desto mer og korrekt kunnskap en organisasjon har, desto lettere er det å observere om noe går galt eller er på vei til å gå galt. Det er også viktig å ha kunnskap om ting som går riktig, hvor det er en pekepinn på hvordan man skal handle i forhold til å være en resilient organisasjon. For å kunne holde på denne mengden av informasjon så må de ansatte være fleksible og samarbeide for å kunne utnytte denne informasjonen på best mulig måte. En siste del av evnen ved overvåkning er å kontrollere og overvåke basisfunksjoner i organisasjonen. Disse funksjonene må vurderes kontinuerlig og revideres jevnlig for å opprettholde motstandsdyktigheten i organisasjonen (Hollnagel, 2011, s.286).

3.3.5 Evnen til å forutse

«The ability to anticipate» er den tredje evnen Hollnagel beskriver som essensiell i et resilient system. Den evnen Hollnagel sikter til er evnen til å forutse. Denne evnen innebærer en del faktorer som bl.a. evnen til å vite hva man skal forvente, evnen til å forstå hvordan en aktivitet kan påvirke en annen, og evnen til å gjenkjenne endringer i systemet som krever rask respons og justeringer. Han uttrykker at det handler om å kunne handle i øyeblikket og at organisasjonen skal kunne ha en evne til å opprettholde kontrollen til tross for at det oppstår endringer og hindringer. Riktignok handler denne evnen om å kunne forholde seg til ikke bare negative endringer som potensielle trusler, men også positive endringer som å ta vare på nye muligheter (Hollnagel, 2011, s.286).

David Woods legger frem seks ulike mønster man kan se etter dersom man er engstelig for at et resilient system står overfor feil og mister tilpasningsevnen, buffere eller at reservelagrene tømmes, og ikke minst dersom man er nødt til å endre målsetningene organisasjonen har. De seks ulike mønstrene blir forklart som evner hvor den første evnen er evnen til å gjenkjenne når evnen til tilpasning avtar. Dette kan gjenkjennes dersom en hendelse oppstår og organisasjonen må slakke ned farten på systemet for å kunne hente seg inn igjen. Dersom dette skjer vil man kunne si at systemet enten er på et vippepunkt eller er på vei inn mot dekompensasjon (Woods, 2011, s. 121). Den andre evnen som nevnes er evnen til å se når buffere og reservelagre enten er utmattet eller uttømt og må fornyes. Det vanskeligste med denne evnen er å erkjenne at et system ikke er perfekt og det vil alltid være nødvendig med

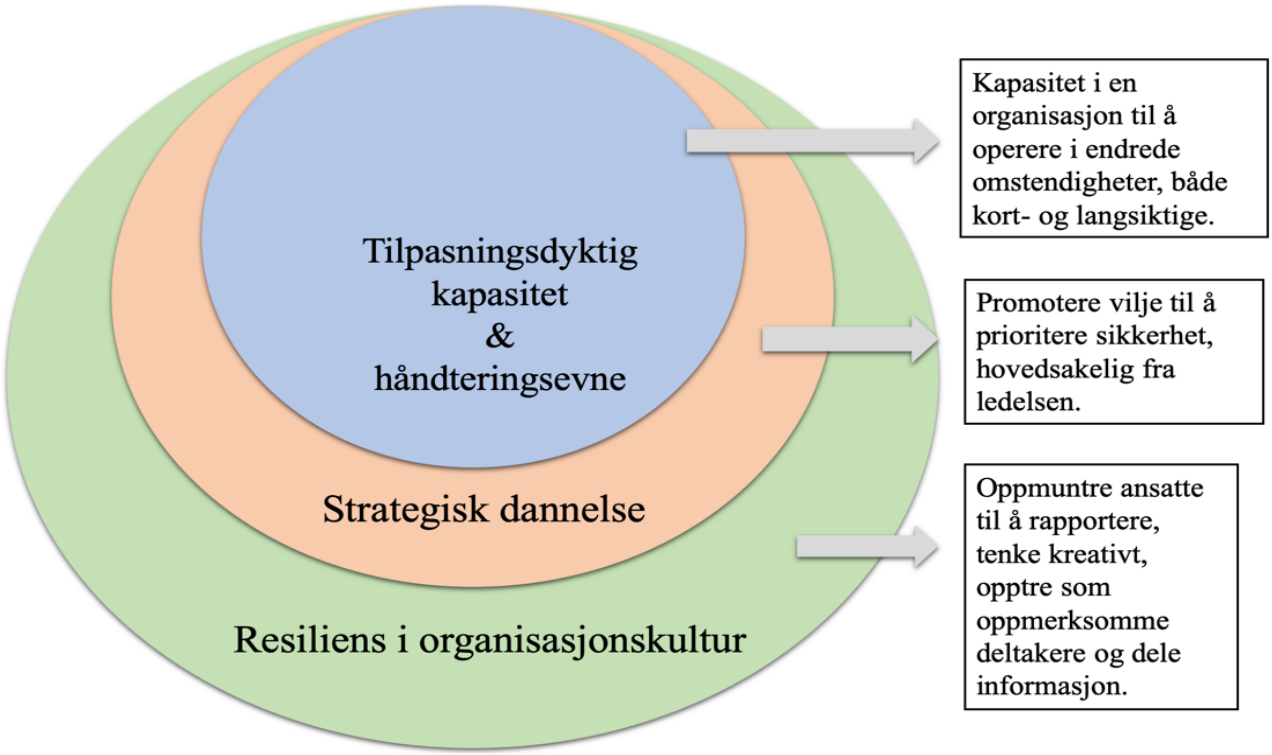
vedlikehold og endringer for å opprettholde den ønskede kvaliteten på systemet. Det er også nødvendig med endringer dersom forutsetningene eller målsetningen for organisasjonen endres (Woods, 2011, s. 122). Den tredje evnen som er nødvendig for å kunne oppnå evnen til å forutse handler om å se når det er nødvendig med kompromisser på tvers av målsetningene. Det handler om evnen til å foreta beslutninger som kan gå på bekostning av andre mål, som for eksempel fokusere på sikkerhet i stedet for å øke produksjonen (ibid., s. 123). Den fjerde evnen går ut på å endre perspektiver og bruke disse perspektivene til tross for at de kan stå i kontrast med det normative i organisasjonen. Denne evnen går ut på å etablere et rammeverk som kan bidra til å effektivisere den proaktive identifikasjonen av risiko og følgende konsekvenser (ibid., s. 123). Den femte evnen til å kunne være et resilient system går ut på å styre endringer mellom avhengigheter. Organisasjonen må være i stand til å navigere mellom funksjonsavhengigheter uavhengig av aktiviteter, nivå, roller og målsetninger (ibid., s. 124). Den siste evnen handler om evnen til tilpasning ved bruk av nye metoder. Ved å være kapabel til å reflektere over det systemet man er en del av, kan dette bidra til å identifisere svakheter og dermed etablere nye metoder for å kunne redusere og fjerne disse svakhetene (ibid., s. 125).

3.3.6 Evnen til å lære

Evnen til å lære kan forklares som en oppfattelse av hva som har skjedd og hvordan man kan lære av de hendelsene som oppstår. Det innebærer også å vite hva man skal lære av og hvordan dette skal brukes i tiden videre. Dersom det skal være en mulighet til å kunne etablere læreevnen må det foreligge tre forhold i organisasjonen. Det første forholdet må være at det foreligger muligheter for å lære. Med dette utrykker Hollnagel at det må skje nok aktivitet i organisasjonen til at det skal være muligheter å lære av aktivitetene. Dette gjelder ikke bare når det oppstår uønskede hendelser, men også når alt går slik som det skal. Et viktig prinsipp i RE er å fokusere på situasjoner hvor alt går slik som det skal. Det neste forholdet handler om at det skal foreligge muligheter for å kunne sammenlikne. I dette tilfellet gjelder det både å sammenlikne konsekvenser og årsaker slik at man skal kunne tillate en viss generalisering. Dette kan oppnås ved å finne likheter og ulikheter mellom ulike hendelser. Det siste forholdet som må ligge til grunn for at læring skal oppnås er å kontrollere at det som blir evaluert og videreformidlet er riktig. Evnen til å lære er basert på flere faktorer hvor man skal ha erfaring, organisasjonen må ha evnen til å analysere og forstå hendelsen, i tillegg til at organisasjonen skal kunne ha evnen til å tilpasse seg endringer (Hollnagel, 2011, s. 287).

3.3.7 Sammenheng mellom resilience engineering og sikkerhetskultur

De fire nevnte egenskapene er grunnleggende for RE, og selv om de er selvstendige egenskaper, så er alle like viktige og nødvendige. Alle fire egenskapene må være tilstede for at en organisasjon kan oppnå full motstandsdyktighet, i følge Hollnagel. Hvordan forholdet mellom RE og sikkerhetskultur er relevant for denne oppgaven skal videre reflekteres over. I RE så kan resiliens vurderes som to ulike fenomener: mulighet til å oppnå resiliens gjennom gode strukturer og kultur, og mulighet til å oppnå resiliens ved å følge Hollnagel sin teori ved å strebe etter å ha de fire nevnte egenskapene.



Figur 9: Resiliens og sikkerhetskultur (Steen, 2019)

Figur 9 viser til et forhold mellom sikkerhetskultur og resiliens, som viser at det er nødvendig med gode strukturer og kultur i henhold til sikkerhet for å kunne oppnå å være motstandsdyktig. De fire egenskapene som ble nevnt ovenfor er grunnleggende for resiliens, men for å oppnå full motstandsdyktighet er også faktorer som robusthet, effektivisering, redundans og ressursfullhet viktig. De to sistnevnte handler om at det må foreligge en håndteringsevne og tilpasningsdyktig kapasitet i organisasjonen slik som figuren ovenfor viser. Det må også foreligge en strategisk dannelse hvor sikkerhetsrelaterte problemer blir prioritert av ledelsen. Dette er grunnleggende i en god sikkerhetskultur, og derfor er det mulig

å hevde at det er viktig å se det store bildet når det gjelder sikkerhet og resiliens (Steen, 2019, s. 11-16).

3.4 Sammendrag av teorikapittel

Denne studien tar for seg Sparebank 1 SR-Bank og deres tilknytning til sikkerhetskultur og resilience engineering (RE). Disse teoriene brukes for å se på hvordan banken som organisasjon kan beskytte sine kunder mot cyberangrep. Cyberangrep er noe som skjer hyppigere i dag enn før, og slike angrep er med på å øke risikoen for kunder med å ha informasjon i banken samt at trusselen øker for banken i seg selv. Det teoretiske rammeverket startet med en forklaring av relevante begreper som brukes gjennomgående i oppgaven. Cyberdomenet handler om digitalisering og IKT. Cybersikkerhet handler om den sikkerheten og barrierene som etableres for å kunne beskytte seg mot trusler gjennom cybernettverket. Den definisjonen av risiko som brukes er at risiko refererer til usikkerhet om og alvorligheten av hendelser og konsekvenser/resultater av en aktivitet med hensyn til det mennesker verdsetter. Hvordan vi forstår risiko vil også avhenge av hver enkelt individ sin persepsjon og risikokompensasjon, men organisatorisk sett så brukes en ROS-analyse for å kartlegge hva som er risiko og sårbarheter i en organisasjon. Sårbarhet forstås i denne oppgaven som graden av motstandsdyktighet og robusthet når en uønsket hendelse oppstår, og usikkerhet handler om noe som er ukjent og som vi ikke kan forutse. Tillit forklares i studiens sammenheng som institusjonell tillit som forstås som et forhold som skaper over tid og gjennom trygghet. For å forstå videre teorigrunnlag så blir kultur forklart som en felles forståelse i organisasjonen, hvor da sikkerhetskultur er sammensetningen av alle i organisasjonen sin kunnskap, motivasjon, holdninger og atferd som brukes for å nå et sikkerhetsbasert mål. Alle de nevnte begrepene henger sammen og utgjør begrepsgrunnlaget for denne studien.

Videre i teorikapittelet presenteres to grunnleggende teorier for sikkerhet, hvor begge teoriene fokuserer på å bygge opp en organisasjon som streber for å unngå uønskede hendelser. James Reason sin teori om sikkerhetskultur ble først presentert ved å forklare hvorfor han mener uønskede hendelser oppstår. I en organisasjon hvor det er mangel på sikkerhetskultur så vil det på grunn av manglende rapportering oppstå latente feil, som videre kan utløses av aktive feil, som regel en menneskelig feil. For å unngå at uønskede hendelser oppstår så bør en sikkerhetskultur bli dannet i organisasjonen. En sikkerhetskultur ifølge Reason er en informert

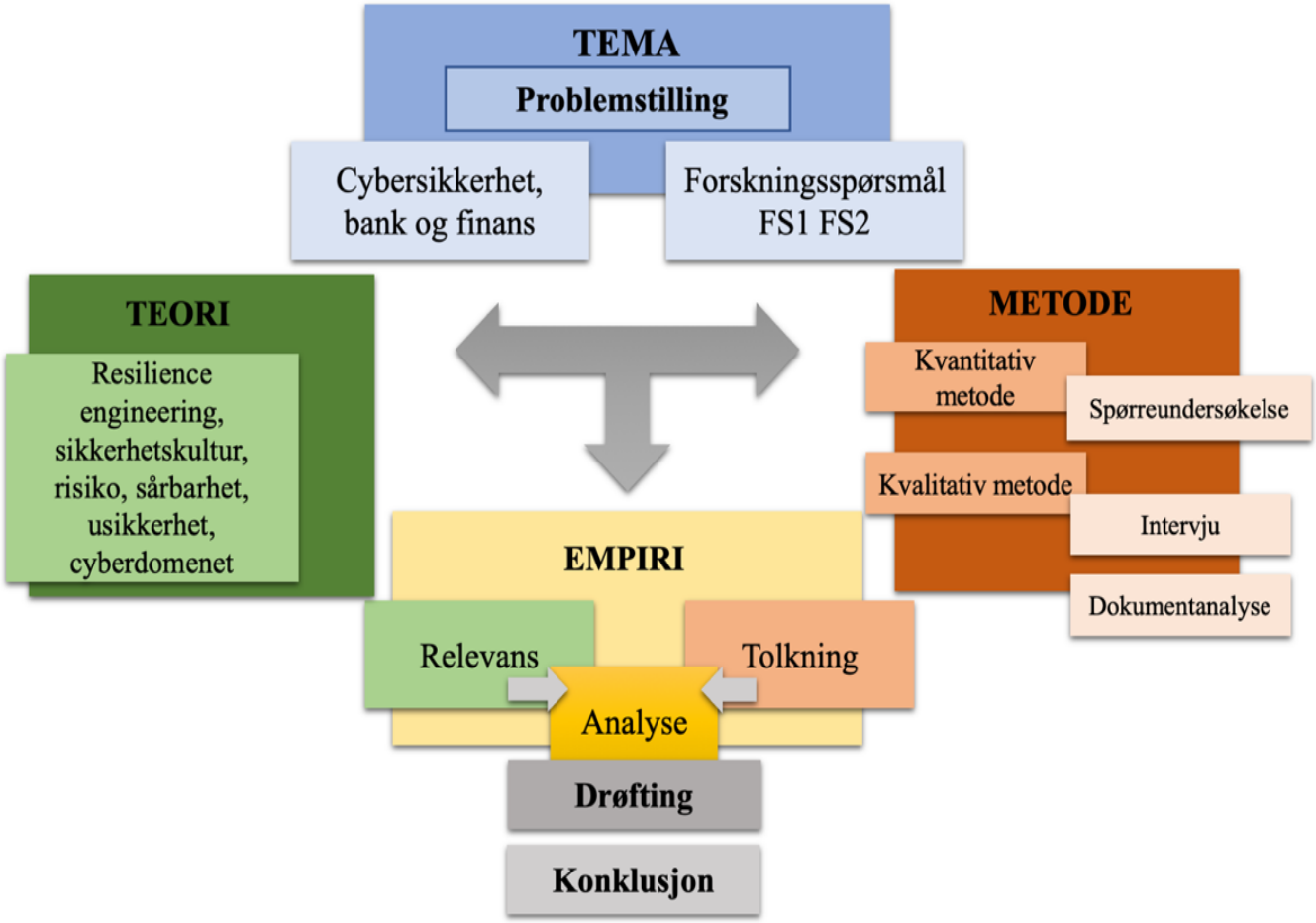
kultur bestående av faktorer som rettferdighet, rapportering, læring og fleksibilitet. Den andre teorien som blir vektlagt i denne oppgaven er Erik Hollnagel sin teori om RE. Han presenterer en ny tilnærming til sikkerhet som har endret seg fra et safety-I-perspektiv til et safety-II-perspektiv. Synet på risiko har gått fra å fokusere på hendelser som får negative konsekvenser, til å se på hendelser hvor alt går godt. For å kunne være en organisasjon med et optimistisk syn på sikkerhet så bør organisasjonen strebe etter å bli motstandsdyktig gjennom RE. En resilient organisasjon har fire egenskaper som er grunnleggende for sikkerhetsstyringen, og disse er evnen til respons, evnen til læring, evnen til overvåkning og evnen til å forutse. Til slutt så vises det til en figur som presenterer forholdet mellom sikkerhetskultur og RE, da disse to bør ses på som to komplementære måter for å oppnå gode resultater knyttet til sikkerhet.

4. Metode

I dette kapittelet skal jeg forklare bruk og valg av forskningsmetode. Valgt metode for datainnsamlingen skal bli redegjort for, og jeg skal beskrive hvorfor den valgte metoden skal kunne bidra til å gi et svar på problemstillingen og de tilhørende forskningsspørsmålene. Valgt metode skal ikke bare bli forklart, men jeg skal også vise til den prosessen jeg har vært gjennom for å evaluere valgt metode. Jeg skal også forsøke å vise til den forskningsprosessen jeg har brukt og hvordan datainnsamlingen skal oppfylle krav til reliabilitet og validitet. Den sentrale dataen som brukes i denne oppgaven er primærdata. Primærdata er først og fremst den dataen som samles inn av forskeren selv (Halvorsen, 2014, s. 114). Datainnsamlingen bestod av en kvantitativ del og to kvalitative deler.

4.1 Forskningsdesign

For å kunne besvare problemstillingen og de tilhørende forskningsspørsmålene, så har jeg valgt å samle inn empirisk data gjennom spørreundersøkelse i form av kvantum, dokumentanalyse og dybdeintervju for å fremme kvalitet. Å bruke både spørreundersøkelser, dokumentanalyse og intervjuer er det som beskrives som en blandet metode, «Mixed Method Research» (MMR). Denne metoden kan forklares som en intellektuell og praktisk blanding av kvalitativ og kvantitativ forskningsmetode. MMR kan vurderes som det tredje store paradigmet når det gjelder forskningsmetode og er en metode som får økt aktualitet i forskningsprosjekter (Johnson, Onwuegbuzie & Turner, 2007, s. 112). Når man bruker denne metoden så legges det til rette for bruk av både kvalitativ og kvantitativ datainnsamling, hvor poenget er å ta hensyn til viktigheten ved begge de to tradisjonelle metodene. Fordelen med denne metoden er at ved bruk av begge metodene så vil dette bidra til å hente inn den mest informative, fullverdige, balanserte og nyttige informasjonen. Dette vil resultere i at datainnsamlingen blir suksessfull som igjen vil føre til verdifulle forskningsresultater (ibid., s. 129). Datainnsamlingen i forhold til MMR ble i denne studien gjennomført i to omganger, slik som figuren 10 viser.



Figur 10: Forskningsdesign

4.2 Spørreundersøkelse

Begrepet kvantitativ kommer fra ordet kvantum som betyr mengde. Det er det kvantitativ datainnsamling går ut på: å innhente informasjon i store mengder for å kunne generalisere et problem eller få et representativt resultat. I studiens tilfelle ønsker jeg å forstå hvordan respondentene oppfatter risiko i forhold til bank og cyberangrep, og hvordan dette påvirker tillitsforholdet mellom bank og kunde. For å kunne innhente denne informasjonen på mest mulig effektiv måte og for å få flest mulig respondenter på kortest mulig tid så valgte jeg å bruke en spørreundersøkelse bestående av åtte spørsmål som ble publisert på sosiale medier med Facebook som hovedaktør. Gjennom hele spørreundersøkelsen brukte jeg begrepet hackerangrep i stedet for cyberangrep. Dette var for å forsøke å gjøre respondentene klar over hva man snakker om, da begrepet cyberangrep kan være for vidt. Jeg valgte også å bruke flere forklaringer av situasjoner og scenarioer som kan oppstå for å klargjøre hva jeg mente med et hackerangrep. Dette er gjennomgående i flere av spørsmålene hvor jeg så det nødvendig med

en ytterligere forklaring på bakgrunn av en forståelse om at alle respondentene ikke hadde god nok kunnskap om cyberangrep til å svare på spørsmålene.

4.2.1 Utvalg

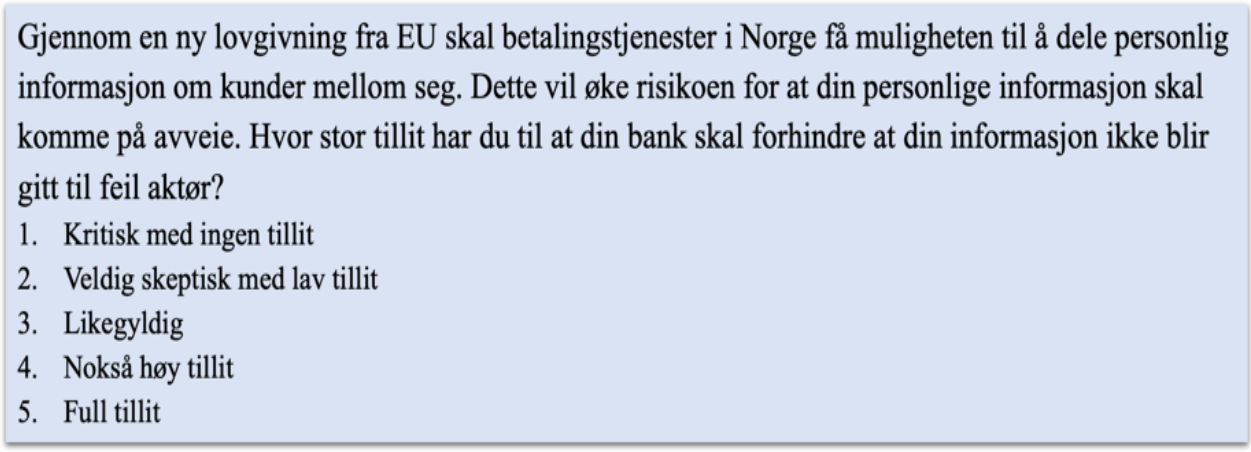
Det er ikke blitt valgt ut et utvalg for denne spørreundersøkelsen. Formålet med spørreundersøkelsen er analytisk og da var målet å få flest mulig respondenter for å kunne analysere svarene i håp om å generalisere informasjonen. Ved de fleste undersøkelser basert på min valgte metode er målet å gjøre svarene representative. Dette betyr at resultatet av undersøkelsen ville vært det samme dersom man hadde undersøkt hele populasjonen (Halvorsen, 2014, s. 155). I samråd med min veileder, i utgangspunktet satt jeg et mål at størrelsen på antall respondenter bør være større enn 100 besvarelse for å skape validitet fra en statistisk tilnærming. Ettersom at jeg ikke hadde noen klare bestemmelser på utvalg av respondenter så ble respondentene kun kategorisert i kjønn og alder. Dette gjør at egenskapene ikke er spesielle og bidrar heller ikke til å gjøre det vanskeligere eller mer komplisert å samle inn svar. Ved å inkludere respondenter uten et bestemt utvalg, så bidro dette til å gjøre resultatene mer representative enn dersom jeg kun hadde hatt en spesifikk aldersgruppe eller et geografisk område (ibid., s. 156). Det skal dog nevnes at antallet respondenter har overskredet mine forventninger, og derfor ble datainnsamlingen fremstilt på en kvantitativ måte ved hjelp av figurer.

4.2.2 Spørreundersøkelsens oppbygning

Survio.com er en nettside som tilbyr en online survey service. Denne nettsiden ble valgt på grunn av dens enkle tilnærming til spørreundersøkelser. Først og fremst var det enkelt for meg som forsker å konstruere en spørreundersøkelse da nettsiden legger til rette for enkle spørreundersøkelser. For det andre så bidro nettsiden sin enkle tilnærming av spørreundersøkelsen til å gjøre at den ble enkel å svare på for respondenter pga. dens tilgjengelighet. Spørreundersøkelsen var også anonym hvor det var ikke mulig for meg som forsker å finne ut hvem som besvarte spørreundersøkelsen. Jeg hadde kun mulighet til å skille respondentene inn i grupper basert på kjønn og alder i kategoriene; “under 18 år”, “18-28 år”, “29-39 år”, “40-60 år” og “over 60 år”. Det ideelle ved en spørreundersøkelse er å selv overlevere hver enkelt undersøkelse og distribuere dem på egenhånd (Halvorsen, 2014, s. 147). Dette er tidkrevende og krever høy kapasitet, noe som ikke var tilfellet ved denne studien. På grunn av tidspress ble derfor spørreundersøkelsen distribuert via Facebook for å få raske respondenter. Dette vil både ha styrker og svakheter, noe som blir redegjort for i

delkapittelet om reliabilitet og validitet.

Spørreundersøkelsens oppbygning var basert på åtte spørsmål med fokus på ulike teoretiske grunnlag. Det var strategiske spørsmål som skulle åpne opp for muligheten til å besvare det teoretiske grunnlaget for denne oppgaven. Oppbygningen med åtte spørsmål bidro til å gjøre spørreundersøkelsen kort, og tiden som brukes for å besvare spørreundersøkelsen var kort. Dette bidro trolig til at flere ønsket å ta undersøkelsen. Dette var en vurdering basert på egen erfaring da jeg selv har erfart at korte spørreundersøkelser krever mindre og er enklere å gjennomføre. Oppsettet på spørreundersøkelsen var strukturert systematisk med lukkede spørsmål hvor svaralternativene var gitt på forhånd (Halvorsen, 2014, s. 141). Årsaken til valgt metode for spørreundersøkelsen var for å gjøre at respondenten skulle ha muligheten til å gjenkjenne fenomener og ytre sin mening om dette fenomenet (ibid., s. 141). Spørreundersøkelsen var også «enqueter» som betyr at den var selvadministrert. Respondenten leste selv spørsmålet og svarte på spørsmålene i samme spørreskjema (ibid., s. 141). Svaralternativene skilte seg fra at respondentene kunne velge et svaralternativ på en skala fra 1-5 og 1-3, eller velge flere svaralternativer. Ved å bruke lukkede spørsmål så ble spørsmålene klarere presisert da det allerede forelå strategiske svaralternativer. Svarene fra spørsmålene bidro til at jeg som forsker kunne kode svarene og bruke resultatene til å sammenlikne svar. Dette åpnet opp for muligheten til å videre forsøke å generalisere resultatet. Når respondentene ga mer enn én forklaring så ble alle svarene inkludert i undersøkelsen, dette gjaldt spørsmålene med flere svaralternativer. Figur 11 viser til et eksempel på et spørsmål som ble stilt i spørreundersøkelsen, og viser til at her var det mulighet til å velge et planlagt svaralternativ.


Gjennom en ny lovgivning fra EU skal betalingstjenester i Norge få muligheten til å dele personlig informasjon om kunder mellom seg. Dette vil øke risikoen for at din personlige informasjon skal komme på avveie. Hvor stor tillit har du til at din bank skal forhindre at din informasjon ikke blir gitt til feil aktør?

1. Kritisk med ingen tillit
2. Veldig skeptisk med lav tillit
3. Likegyldig
4. Nokså høy tillit
5. Full tillit

Figur 11: Eksempel på spørsmål i spørreundersøkelsen

Vedlegg A viser spørsmålene med følgende svaralternativer som ble brukt i spørreundersøkelsen.

4.2.3 Gjennomførelse av spørreundersøkelsen

Spørreundersøkelsen ble publisert søndag kveld 14.april. Det var ikke noe planlagt tidspunkt hvor denne skulle ble publisert, men den ble publisert så snart undersøkelsen var klar og ferdig. Spørreundersøkelsen lå tilgjengelig på nett i fem dager, og ble avsluttet formiddagen torsdag 18.april. Det var totalt 303 respondenter med en klar variasjon av kjønn og alder. Ved å sammenlikne resultater og evaluere resultatene i forhold til alder og kjønn har Excel blitt brukt aktivt, ettersom hele datasettet var tilgjengelig med en oversikt over alle individuelle besvarelser. Resultatene fra spørreundersøkelsen blir presentert i kapittel 5 ved bruk av figurer og tekst. Årsaken til at det blir brukt figurer var for å gjøre det mer oversiktlig og enklere for leseren å forstå resultatet. Figurene er hentet ut fra programmet Survio hvor all innsamlet data fra denne spørreundersøkelsen var tilgjengelig.

4.3 Dokumentanalyse

Sekundærdata er data som har blitt utarbeidet av noen andre enn forskeren selv, som for eksempel rapporter og tidligere forskning (ibid., s. 114).

Tabell 3: Dokumentanalyse

Dokumenter	Fokusområder	Relevans til oppgaven
World Economic Forum: *The Global Risks Report 2019*	Rapporten er på 107 sider. Informasjonen som ble brukt i denne oppgaven var hovedsakelig knyttet til figuren av «The Global Risks Landscape» og «Preface» skrevet av Børge Brende.	Denne rapporten styrker bakgrunnsinformasjonen til oppgavens tema ved å erklære at cyberangrep er en stor trussel mot dagens samfunn.
Basel Committee of Banking Supervision: *Cyberresilience: Range of practises. Bank of International Settlements.*	Rapporten er på 45 sider. Den delen som fikk største fokus i denne oppgaven var kapittelet om «Cyber Governance».	Denne rapporten bidrar som et empirisk dokument som en del av datainnsamlingen presentert i kapittel 5. Rapporten vektlegger viktigheten av å fokusere på resiliens knyttet til cybersikkerhet.
Nasjonal Sikkerhetsmyndighet, Etterretningstjenesten & Politiets Sikkerhetstjeneste: *Koordineringsgruppen for IKT-risikobildet: Cybersikkerhet.*	Rapporten er på 24 sider. Den innledende delen og delen om «Nye Sikkerhetsbehov» ble gjeldende for denne oppgaven.	Denne rapporten bidrar til å styrke bakgrunnsinformasjonen til oppgavens tema, og viser til store internasjonale aktører som vektlegger fokus på cybersikkerhet.
Nasjonal Sikkerhetsmyndighet: *Et sikkert digitalt Norge – IKT-risikobilde 2018.*	Rapporten er på 22 sider. Fokuset var på delkapittel 1 «Digitale verdier og digitale trusler».	Denne rapporten bidrar til å styrke bakgrunnskunnskapen knyttet til Norge som et digitalisert land, og hvilke utfordringer dette bringer med seg.

Denne typen datainnsamling har ikke fått stor plass i min oppgave da det ikke var nødvendig for å besvare problemstillingen og de følgende forskningsspørsmålene. Sekundærdata har kun blitt brukt i denne oppgaven til å underbygge tematiseringen og vise til trusselbildet som er i stadig endring. Rapportene fra Basel, WEF, NOU, NSM, E-tjenesten og PST har bidratt til å gi et bilde av virkeligheten og brukes til å belyse oppgavens relevans til dagens trusselbilde. Tabell 3 viser til en dokumentanalyse av rapporter som har hatt betydning for oppgavens oppbygning, bakgrunn og empirisk funn.

4.4 Intervju

Den kvalitative datainnsamlingen knyttet til intervju foregår som en casestudie hvor det er en bedrift som står som undersøkelsesenhet. Dette skjer på bakgrunn av et analytisk formål, hvor poenget ikke er å generalisere, men å gå i dybden. Jeg ønsket å forsøke å finne særtrekk ved de analyseenhetene som kan brukes til å forklare det utfallet jeg studerer i denne studien (Ringdal, 2013, s. 171). Dybdeintervju skal bidra til at man får en dypere forståelse (Halvorsen, 2014, s. 138). Det er et uformelt intervju, som i utgangspunktet skal være ustrukturert og følger samtalens gang. Et ustrukturert intervju er en samtale mellom en forsker og en informant hvor spørsmålene og registreringen av svarene skjer på en systematisk måte. Bruk av denne metoden bidro til at jeg som forsker fikk muligheten til å sammenlikne resultatene (ibid., s. 142). Ved å ta i bruk en metode som baseres på dybdeintervju og ustrukturert intervju så valgte jeg å følge en intervjuguide med åpne svarmuligheter. Dette ga rom for oppfølgingsspørsmål som et resultat av den pågående samtalen. Likevel var det også nyttig med en intervjuguide for å ha en struktur å forholde seg til underveis i intervjuet. Jeg la rette for improvisering gjennom alle intervjuene, samtidig som jeg brukte intervjuguiden som en plan som jeg kunne falle tilbake på for å sikre meg at jeg fikk hentet inn den informasjonen som var nødvendig knyttet til denne studien (Ringdal, 2013, s. 244).

4.4.1 Utvalg og utforming av intervjuguide

Utvalget i denne studien var analytisk hvor jeg var opptatt av å samle inn informasjon, og ikke ha fokus på at utvalget skulle være representativt (Halvorsen, 2014, s. 155). Utvalget var et strategisk utvalg hvor jeg hadde formål om å få høyest mulig kvalitativt innhold i informasjonen (ibid., s. 164). Utvalget var også basert på en teoretisk utvelging da alle respondentene skulle kunne bidra med mest mulig korrekt informasjon om saken. Ettersom

jeg var opptatt av å gå i dybden så var det primært at utvalget var akkurat stort nok til at jeg fikk muligheten til å bruke nok tid med hver enkelt informant (ibid., s. 165). Ettersom at datainnsamlingen gjennom intervjuer var basert på denne metoden, så var jeg på bakgrunn av tidspress og kapasitet kun kapabel til å gjennomføre 12 dybdeintervjuer. Da hensikten med datainnsamlingen var å få tak i informasjon om hvordan sikkerhet fungerer i SpareBank 1 SR-Bank så var det i utgangspunktet nok med én informant. Dette kunne likevel oppleves som svakt, og derfor valgte jeg å intervjue flere informanter for å få økt og eventuelt mer utfyllende eller inngående informasjon, for å eventuelt undersøke om det var enighet om fenomenet fra de ulike informantene (Ringdal, 2013, s. 243). Utvalget av ansatte og ledere har vært i samråd med min kontakt i SpareBank SR-Bank.

Utvalg til intervjuer	Stilling	Fokusområde
Intervju med ansatte i SpareBank 1 SR-Bank	Prosjektleder Systemeier Markedskonsulent Senior HR-rådgiver Fagleder IT-arkitektur Teamleder Kundesenter Chief Data Officer (CDO)	Spørsmål knyttet til sikkerhetskultur
Intervju med ledere i SpareBank 1 SR-Bank, gruppe 1	Konserndirektør kommunikasjon og bærekraft Personvernombudet Senior Fagrådgiver i sikkerhetsavdelingen	Spørsmål knyttet til sikkerhetskultur, i tillegg til spørsmål knyttet til spørreundersøkelsen
Intervju med ledere i SpareBank 1 SR-Bank, gruppe 2	Sikkerhetssjef Konsernbanksjef IT-drift	Spørsmål knyttet til resilience engineering

Figur 12: Utvalg intervju

Figur 12 viser til utvalget i den kvalitative datainnsamling presentert i tre grupper av informanter basert på stilling og fokusområde. I utbredelsen av intervjuguiden valgte jeg å lage tre forskjellige intervjuguider for å ha spesifiserte spørsmål til de ulike gruppene. Årsaken til dette var for å hente ut mest mulig informasjon knyttet til de ulike fokusområdene. Intervjuguiden ble gjennomgått med både veileder og med min kontakt i SpareBank 1 SR-Bank. Dette var for å forsikre meg om at spørsmålene var konkrete og relevante, samtidig slik at min kontakt i banken kunne bidra med utvelging av informanter i forhold til hvilken intervjuguide som skulle brukes.

Både intervju av ansatte og intervju av ledere gruppe 1 har spørsmål knyttet til sikkerhetskultur. Dette var på grunn av at jeg ønsket å vurdere sikkerhetskulturen i

organisasjonen, og å sammenlikne informasjonen fra de ansatte og lederne i organisasjonen. Jeg valgte også å stille spørsmål til ledere i gruppe 1 om spørreundersøkelsen som ble gjennomført i den kvantitative datainnsamlingen. Årsaken til dette var for å vurdere om det var samsvar i bankkunder sine interesser og behov i henhold til strategier for risikokommunikasjon og beskyttelse i forhold til cyberangrep i SpareBank 1 SR-Bank. Den siste intervjuguiden var knyttet til RE, og utvalget var strategisk i den forbindelsen om at jeg ønsket å finne de informantene med mest kunnskap på det nevnte fokusområdet. Figuren 13 viser eksempler på ulike spørsmål som ble stilt til de ulike informantene basert på hvilket fokusområde som var aktuelt i de ulike intervjuguidene.

	Intervju av ansatte	**Intervju av ledere, gruppe 1**	**Intervju av ledere, gruppe 2**
Eksempel på spørsmål:	Hva anser du å være en god sikkerhetskultur? Bidrar ledelsen i SR-bank til å skape en sikkerhetskultur?	Bruker banken en bestemt metode for å informere kundene deres om cyberangrep og konsekvenser for kunden? Anser du at det er oppmuntring til å rapportere feil? Er dette noe dere vektlegger i organisasjonen?	Hvor lang tid regnes med å bruke på å komme tilbake til normaltilstand etter cyberangrep? På hvilken måte overvåker SR-bank dagens utfordringer knyttet til cyberangrep?

Figur 13: Eksempel på spørsmål i intervju

Den første gruppen var intervju av tilfeldig ansatte i organisasjonen. For å kunne måle sikkerhetskultur i en organisasjon er det viktig å ikke bare prate med lederne, men også de som er på lavere nivå i organisasjonen. I den sammenheng ønsket jeg derfor å intervjue mellom 5 og 10 ansatte i Sparebank 1 SR-Bank. Antallet ble 7 respondenter på bakgrunn av kapasitet og behov. Spørsmålene som ble stilt i dette intervjuet var hovedsakelig knyttet til teorien om sikkerhetskultur av James Reason (Vedlegg C). Utvalget var tilfeldig, men likevel strategisk for å ha informanter med ulike stillinger og ulike arbeidsområder, på bakgrunn av ønsket om å vurdere helheten i organisasjonen.

Den andre intervjugruppen var ledere med spesialkompetanse på det fokusområdet som ble vektlagt. De følgende spørsmålene var knyttet til den kvantitative spørreundersøkelsen som var blitt gjennomført og analysert i forkant av intervjuene. Disse spørsmålene ble stilt for å

vurdere om det var samsvar i bankforholdet mellom bank og kunde. I del to av dette intervjuet var spørsmålene knyttet til sikkerhetskultur fra et lederperspektiv (Vedlegg D). Resultatet fra denne delen settes opp mot intervjuene om sikkerhetskultur av ansatte i SpareBank SR-Bank.

Den siste gruppen var også intervju av ledere, hvor deres spesialkompetanse var relevant til spørsmål knyttet til RE. Spørsmålene i intervjuguiden knyttet til dette fokusområdet var planlagt i henhold teorien om RE av Erik Hollnagel. Resultatene fra de to intervjuene ved bruk av denne intervjuguiden ble brukt til å evaluere om SpareBank 1 SR-Bank sin tilnærming til evnen til å respondere, evnen til å lære, evnen til å overvåke og evnen til å forutse var tilstede. Spørsmålene ble delt inn i fire kategorier hvor hver enkelt kategori var de nevnte evnene som var grunnleggende videre i analysedelen i oppgaven. Vedlegg E viser til hele intervjuguiden som ble brukt under disse intervjuene.

4.4.2 Gjennomførelse av intervjuer

Før hvert intervju startet, presenterte jeg et samtykkeskjema for informanten (Vedlegg B). Dette skjemaet tok for seg en kort presentasjon av forskningsstudien og tilhørende problemstilling, og deretter tre spørsmål som informanten måtte godkjenne. Disse spørsmålene var: «Jeg samtykker i å delta i forskningsprosjektet», «Jeg samtykker i at dette intervjuet kan tas opp på bånd» og «Jeg samtykker i at navnet mitt brukes i forskningsprosjektet». På bakgrunn av at enkelte informanter ikke ønsket at navnet deres skulle komme på trykk, så var det gjennomgående i presentasjon av resultater fra datainnsamlingen knyttet til intervjuer, kun brukt stillingstittel på informantene og ikke navn. Dette vil ikke ha noen negativ effekt da det er stillingen som har størst betydning for datainnsamlingen. Alle informantene godkjente at intervjuene kunne tas opp på bånd, hvor jeg senere brukte båndopptaket til å transkribere hvert enkelt intervju. Alle båndopptakene ble slettet etter fullført transkribering.

Alle intervjuene startet med å innhente bakgrunnsinformasjon. Dette var for å få et bilde av de ulike informantene og forsikre meg om at jeg har korrekt informasjon om hver enkelt informant og sikre at hver enkelt informant har spesialkunnskap på dette området. Videre startet jeg på intervjuguiden som var forberedt på forhånd. De tre ulike gruppene har ulike intervjuguider i forhold til hvilken fagkunnskap informanten er spesialist på. Alle intervjuene ble avsluttet med et siste spørsmål hvor informanten fikk mulighet til å gi ytterligere informasjon som vil være nyttig for studien i tillegg til å selv stille spørsmål.

Figur 14 viser til når de ulike intervjuene ble gjennomført og hvor lang tid jeg brukte på hvert intervju. De fleste intervjuene ble gjennomført på hovedkontoret til SpareBank SR-Bank som er i Bjergsted, Stavanger. Tre av intervjuene ble imidlertid gjennomført via telefon. Dette var intervjuene med Senior HR-rådgiver, Fagleder IT-arkitektur og Teamleder Kundesenter, da de ikke hadde mulighet til å møte opp på kontorene i Bjergsted.

	Torsdag 2.mai 2019	**Fredag 3.mai 2019**	**Mandag 6.mai 2019**
Informant etter rekkefølge, og tidsbruk *Over telefon	• Sikkerhetssjef (26minutter) • Chief Data Officer (10minutter) • Prosjektleder (12minutter) • Senior Fagrådgiver sikkerhetsavdelingen (36minutter) • Konserndirektør kommunikasjon og bærekraft (34minutter) • Systemeier (8minutter) • Markedskonsulent (10minutter) • Senior HR-rådgiver* (8minutter) • Fagleder IT-arkitektur* (10minutter)	• Konsernbanksjef IT-drift (35minutter)	• Teamleder Kundesenter* (10minutter) • Personvernombudet (30minutter)

Figur 14: Tidspunkt og tidsbruk på intervjuer

Resultatene fra intervjuene blir presentert i kapittel 5 i oppgaven, strukturert ut ifra hvilken intervjuguide som ble brukt. I presentasjonen av resultater fra intervjuer med ansatte knyttet til sikkerhetskultur, så ble det brukt en ordsky. Ved å bruke en ordsky klarer jeg å få frem mer av særegenhetene til informantene, enn hva jeg ville gjort ved å se på statistikk og prosentandeler. Ordskyen representerer de ansattes tanker i stor grad, og derfor vil denne være fordelaktig å inkludere. Gjennomgående i den resterende presentasjonen brukes tekst og sitater fra de ulike informantene, og det er i hovedsak den viktigste informasjonen fra intervjuene som har blitt presentert.

I etterkant av produksjon av presentasjon av resultater fra intervjuene så ble dokumentet sendt tilbake til min kontakt i SpareBank SR-Bank. Årsaken til dette var at han ønsket å forsikre seg om at det ikke har blitt inkludert informasjon som er i utgangspunktet skulle vært hemmelig eller sikkerhets beskyttet.

4.5 Reliabilitet og validitet

Reliabilitet og validitet er måleverdier for styrker og svakheter innenfor forskningsarbeid. Reliabilitet beskriver påliteligheten ved målingene man foretar seg, da om samme måleinstrument gir samme resultat ved gjentatte målinger (Ringdal, 2013, s. 96). Validitet omhandler gyldighet og reliabilitet omhandler spørsmål knyttet til måleinstrumentets og resultatenes evne til re-testing (Tjora, 2012, s. 203-207). Validitet kan skilles ved indre og ytre validitet. Ytre validitet peker på at resultatene i et eksperiment kan generaliseres og dermed være representativt om et fenomen i den virkelige verden (Ringdal, 2013, s. 144). Den indre validiteten kan forstås som gyldighet, og dette handler om at forskeren faktisk får mulighet til å måle det man ønsker å måle (ibid., s. 96).

4.5.1 Reliabilitet og pålitelighet

Reliabilitet i datainnsamling handler om hvilken data som brukes, måten dataen samles inn på og hvordan informasjonen bearbeides i oppgaven. I den kvantitative datainnsamlingen hvor spørreundersøkelsen var metoden for datainnsamling, så handlet den om å kunne måle virkeligheten. For å kunne måle virkeligheten er det en forutsetning at den er målbar, noe som var tilfellet i denne oppgaven. Reliabiliteten for spørreundersøkelsen er derfor styrket ettersom at resultatene var konkrete, samtidig som at spørsmålene var etablert i henhold til teoretisk sammenheng. Den vil også være styrket hvor en detaljert beskrivelse av forskningsmetoden ble redegjort for i oppgaven, samtidig som at spørsmålene som ble stilt i undersøkelsen er vedlagt som et vedlegg. Dette kan bidra til å utføre en re-testing av spørreundersøkelsen, noe som kan styrke påliteligheten til resultatene fra undersøkelsen.
De kravene som stilles i forhold til å vurdere reliabilitet er lite hensiktsmessig innenfor kvalitativ forskning, hvor det ikke foreligger strukturerte datainnsamlingsteknikker, slik det gjorde i den kvantitative datainnsamlingen. Likevel så kan reliabiliteten i forhold til denne typen datainnsamling styrkes ved å presentere en beskrivelse av forskningsprosessen, i tillegg til å legge ved intervjuguide, noe som er gjeldende i denne oppgaven. En stor del av datainnsamlingen i denne studien er basert på informanter, noe som i stor grad påvirker reliabiliteten til informasjonen som ble hentet inn. Datainnsamlingen knyttet til intervjuene er i stor grad avhengig av åpenhet og i hvilken grad mine informanter har vært villig til å fortelle sannheten. Det er vanskelig for meg som forsker å evaluere om noen forteller sannheten, og

derfor så er denne type datainnsamlingen basert på at jeg gjorde det som var mulig for å hente inn pålitelig informasjon, til tross for risikoen for at informantene kunne lyve under intervjuene og ikke fortelle sannheten. Dette kan påvirke resultatet, men det har vært utenfor min evne til å vurdere.

4.5.2 Validitet og troverdighet

I henhold til den ytre validiteten så jeg tidlig en svakhet ved å publisere spørreundersøkelsen på Facebook. Ved å publisere en spørreundersøkelse på sosiale medier risikerer man å utelukke en del av befolkningen da ikke alle har en Facebook-konto. Jeg valgte likevel å bruke Facebook som kommunikasjonsmedium på grunn av kapasitet. Et annet aspekt som påvirket den ytre validiteten ved denne spørreundersøkelsen var tid og hvor lenge spørreundersøkelsen var tilgjengelig på sosiale medier. Jeg valgte å la den ligge ute på nett i tre døgn da dette var nødvendig på grunn av tidspress. En siste faktor som har påvirket den ytre validiteten var at en stor del av målgruppen som så denne publiseringen var på aldersgruppen mellom 18-28. Dette var likevel noe jeg straks klarte å observere og fikk hjelp av familie og bekjente til å publisere den videre for å prøve å nå så varierte demografiske deler av befolkningen som mulig.

Når det gjelder den indre validiteten i forhold til spørreundersøkelsen så vil den kunne diskuteres å være påvirket da mistolkinger av spørsmålene kunne oppstå. Dette gjelder både generell mistolking av spørsmål og en eventuell manglende forståelse over hva et hackerangrep er i banksammenheng. Dette er et fenomen som bør legges til grunn da etter egen erfaring så viser det seg at ikke alle har full forståelse for hva som ble spurt om i spørsmålene. Likevel så vil dette ikke ha stor påvirkning da jeg også brukte flere eksempler i spørsmålene for å legge fokus på økt forståelse og prøve å forhindre mistolkninger. Den indre validiteten i spørreundersøkelsen blir også påvirket i forhold til å sammenlikne alder og kjønn, hvor det var ujevnt med antall respondenter i det ulike gruppene. Det var langt flere kvinner som svarte på spørreundersøkelsen, og det var ujevn fordeling i forhold til alder. Validiteten ville vært styrket dersom jeg hadde hatt like mange respondenter i hver enkelt kategori.

I forhold til den kvalitative datainnsamlingen så var ikke målet med datainnsamlingen å prøve å generalisere et fenomen. Dette gjør at fokus på den ytre validiteten ikke vil være så relevant i denne forbindelse. Likevel kan det sies å være en sterk ytre validitet i forhold til at

intervjuene gir et genuint bilde av virkeligheten ettersom antallet informanter kan sies å være representativt. Den indre validiteten derimot kan vurderes som sterk i den kvalitative datainnsamlingen. Dette begrunnes med at ved å lage en intervjuguide med spørsmål knyttet til teori, så vil informasjonen som hentes ut av intervjuene være høyst relevant for oppgaven.

4.6 Fordeler og ulemper med valgt metode

Fordelen med å ha en kvantitativ spørreundersøkelse var først og fremst at det krevde lite av meg som forsker under selve datainnsamlingen. Den nettsiden og online survey servicen jeg brukte var til god hjelp når det gjaldt både innsamling og det å samle inn alle resultatene i ulike diagrammer og tabeller. Dette gjorde at jeg unngikk å bruke tid på å lage egne diagrammer og tabeller da disse ble laget gjennom nettsiden. Ulempen med denne spørreundersøkelsen var noe jeg fryktet fra starten av, og det var å bruke sosiale medier som kommunikasjonsmedium. Grunnen til at jeg fryktet dette var på grunn av risikoen for å unnlate eventuelle respondenter på bakgrunn av at de ikke har Facebook. For å forhindre dette forsøkte jeg å ta kontakt med min kontakt i SpareBank SR-Bank for å få kontaktliste og få muligheten til å sende ut spørreundersøkelsen til kunder. Dette var ikke mulig, da banken er under streng taushetsplikt vedrørende informasjon om hvem som er deres kunder. På bakgrunn av dette besluttet jeg å kun bruke sosiale medier som kommunikasjonsmedium, da dette var mest gunstig i forhold til tidskapasitet. Dette bidro til at jeg fikk manglende respondenter på aldersgruppen over 60 år. Jeg vil også vurdere at å spre spørreundersøkelse som en selvadministrert undersøkelse var en ulempe i bruk av denne metoden. Dette kan begrunnes med at tilbakemeldinger fra enkelte respondenter viser at alle respondentene ikke forstod alle spørsmålene, noe som kan bidra til å påvirke resultatet i datainnsamlingen.

Fordelen med å bruke dokumentanalyse som sekundærdata er for å gi dybde i datainnsamlingen. Informasjonen som ble hentet ut fra de ulike rapportene som var inkludert i oppgaven, har bidratt til å gi bakgrunnsinformasjon til temaet om cybersikkerhet i studien. Ved å vise til store aktører som bl.a. Basel og deres rapport om cyberresilience, så underbygger det viktigheten av temaet som var gjeldende i denne studien.

Fordelen med å ha kvalitative intervjuer gjorde at jeg fikk muligheten til å gå i dybden og virkelig forsøke å finne svar på spørsmål som var knyttet til problemstillingen og de følgende

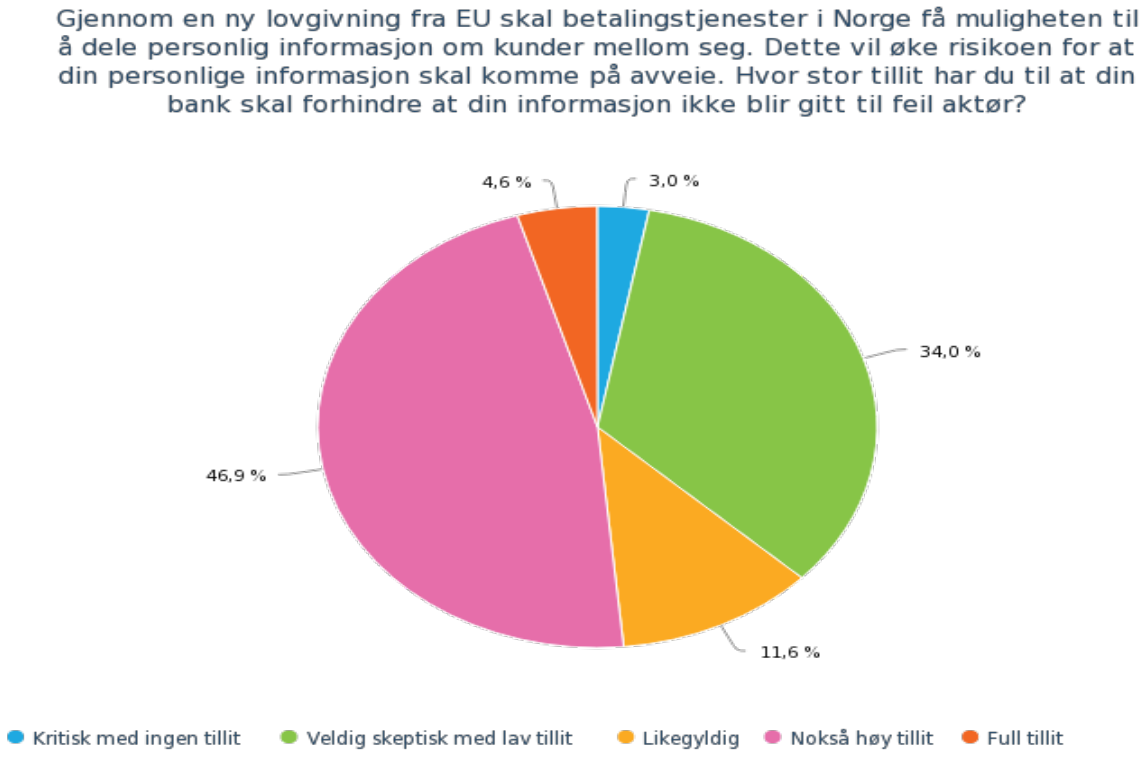
forskningsspørsmålene som er gjeldende for denne oppgaven. Ved å ha et utvalg som er strategisk valgt så har dette gjort at jeg får muligheten til å få informanter med spesialkunnskap på området, noe som styrker oppgaven. Ulempen ved å bruke en slik datainnsamlingsmetode, og antall intervjuer, er at det har krevd mye tid og kapasitet av meg som forsker.

5. Empirisk funn

I dette kapittelet så vil primærdata bli presentert. Dette vil gjøres i tre omganger, hvor de tre ulike delene baseres på den type metode som ble brukt for å samle inn informasjonen. Først ut er resultater fra den kvantitative datainnsamlingen i form av spørreundersøkelsen. Det andre delen er resultater av sekundærdata som brukes i oppgaven og som er relevant for videre diskusjon. Den siste delen av dette kapittelet er presentasjon av resultater fra den kvalitative datainnsamlingen i form av intervjuer. Resultatene vil bli presentert ut ifra hvilken intervjuguide som ble brukt under intervjuene.

5.1 Resultater fra spørreundersøkelse

Det første spørsmålet spørreundersøkelsen tok for seg var alder. Svaralternativene ble delt inn i kategoriene «under 18 år», «18-28 år», «29-39 år», «40-60 år» og «over 60 år». Av de totalt 303 respondentene var 152 mellom 18 og 28 år. Dette har trolig mye å gjøre med at en stor andel av mine venner på Facebook er innenfor denne aldersgruppen. Det var også en stor andel i aldersgruppen mellom 40 og 60 år hvor antallet respondenter var 87 (28,7 %). Dette kan trolig forklares ved at mine foreldre har bidratt til å spre undersøkelsen via deres venner og bekjente. På aldersgruppen 29-39 år var det 50 respondenter, og på aldersgruppen over 60år var det 11 respondenter. Den kategorien med minst respondenter var på under 18år, noe som trolig ikke vil ha stor betydning i denne undersøkelsen hvor barn under 18 år gjerne ikke har stor kontakt med sin bank enda. Det andre spørsmålet i spørreundersøkelsen var kategorisering av kjønn. Svaralternativene var «Mann», «Kvinne» og «Ønsker ikke å oppgi». Resultatene viste at en fordeling på 66,7 % kvinner, med 202 respondenter, og 33,3 % menn, med 101 respondenter. De to første spørsmålene er med i spørreundersøkelsen for å videre kunne vise indikasjoner på om det er forskjell på alder og kjønn korrelert med svarene de oppgir gjennom spørreundersøkelsen. De neste seks spørsmålene handler om forholdet mellom bank og kunde, og resultatene skal videre brukes i analysen.

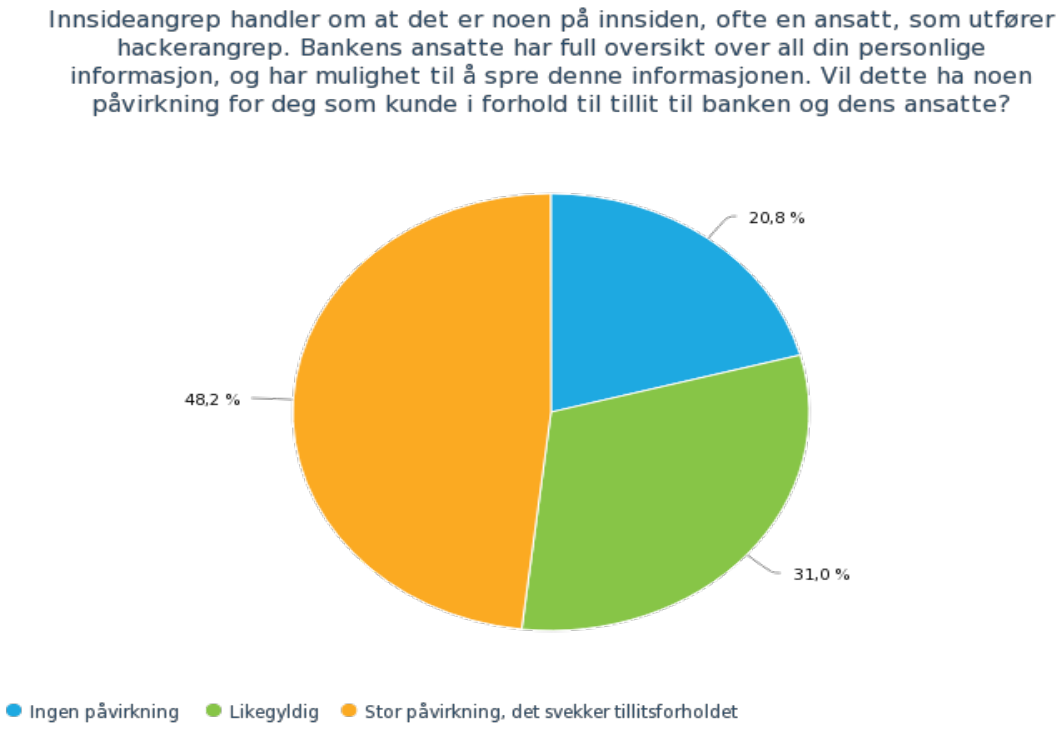


Figur 15: Personlig informasjon og tillit

Det første spørsmålet knyttet til oppgavens problemstilling og forskningsspørsmål i spørreundersøkelsen handlet om nye lovgivninger i forhold til personlig informasjon og deling av denne informasjonen. Spørsmålet tok for seg en kort introduksjon av fakta hvor hensikten var å gi respondenten mulighet til å vurdere tillitsforholdet til sin bank. Dette skulle respondenten gjøre på bakgrunn av at nye lovgivninger åpner opp muligheten til å dele informasjon. Spørsmålet tok for seg om frykt for at deres personlige informasjon skal bli gitt til feil aktør, vil påvirke tillitsforholdet mellom kunde og bank. Figur 14 ovenfor viser kategoriseringen av svaralternativene som var på en skala fra 1 til 5, fra ingen tillit til full tillit. 3 % av respondentene svarer at de ikke har noen tillit til banken. De resterende 97 % svarer at de har tillit til banken, men at tilliten varierer mellom å være skeptisk til å ha full tillit. Den største andelen av respondentene, på 46,9 %, svarte at de har nokså høy tillit til banken når det gjelder deling av informasjon med andre betalingstjenester.

For å vurdere om det er trender i forhold til alder og tillit valgte jeg å se på aldersgruppene «18-28 år» og «40-60 år», og kalkulere ved å se på hvilke av disse to aldersgruppene som har høyest prosentandel på de ulike svaralternativene. Jeg valgte å bruke svaralternativene «Nokså høy tillit» og «Full tillit», og resultatene viste at det var 60,9 % av respondentene i aldersgruppen «40-60 år» som valgte disse to svaralternativene. Ettersom det var 49,3 % som

valgte disse svaralternativene i aldersgruppen «18-28 år», så kan det antas å være en trend at alder påvirker tillitsforholdet til banken når det gjelder personlig informasjon.

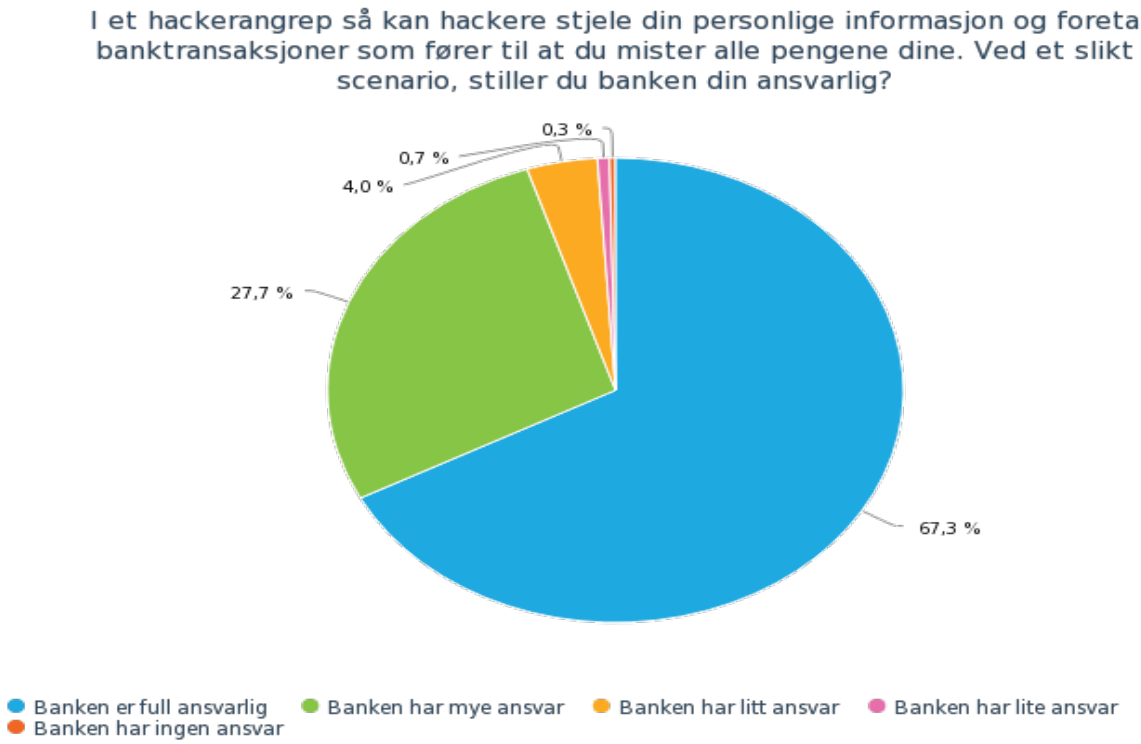


Figur 16: Innsideangrep og tillit

Spørsmål nummer fire i spørreundersøkelsen handlet om innsideangrep og tillit. I dette spørsmålet la jeg frem en forklaring på innsideangrep, som er noe som kan oppstå innad i banken. Dette betyr at det er en ansatt som foretar hackerangrepet. I den forbindelse la jeg frem et spørsmål som spurte om i hvilken grad dette ville ha påvirkning til tilliten til banken og dens ansatte. Der 48,2 % svarte at å vite at ansatte har muligheten til å gjøre angrep fra innsiden vil påvirke deres tillit og 20,8 % sier at det ikke har noen påvirkning. Det er 31 % som sier at de er likegyldig til innsideangrep og tillit til de ansatte i banken er uavhengig av denne informasjonen.

I dette spørsmålet viser resultatene at desto eldre man blir, desto flere valgte svaralternativet «Stor påvirkning, det svekker tillitsforholdet». Av alle respondentene i gruppen «over 60 år» var det 64 % som valgte dette alternativet, og i gruppen «40-60 år» var det 50,6 % som valgte det alternativet. Dette kan tyde på at alder har en effekt på tillitsforholdet man har til banken ved å vite at innsideangrep kan oppstå. Det var også interessant å se på respondentene som valgte at de var likegyldige til spørsmålet som ble stilt. 37,5 % i aldersgruppen «18-28 år» og 38 % i aldersgruppen «29-39 år» valgte det alternativet. Det som viste seg å være merkverdig

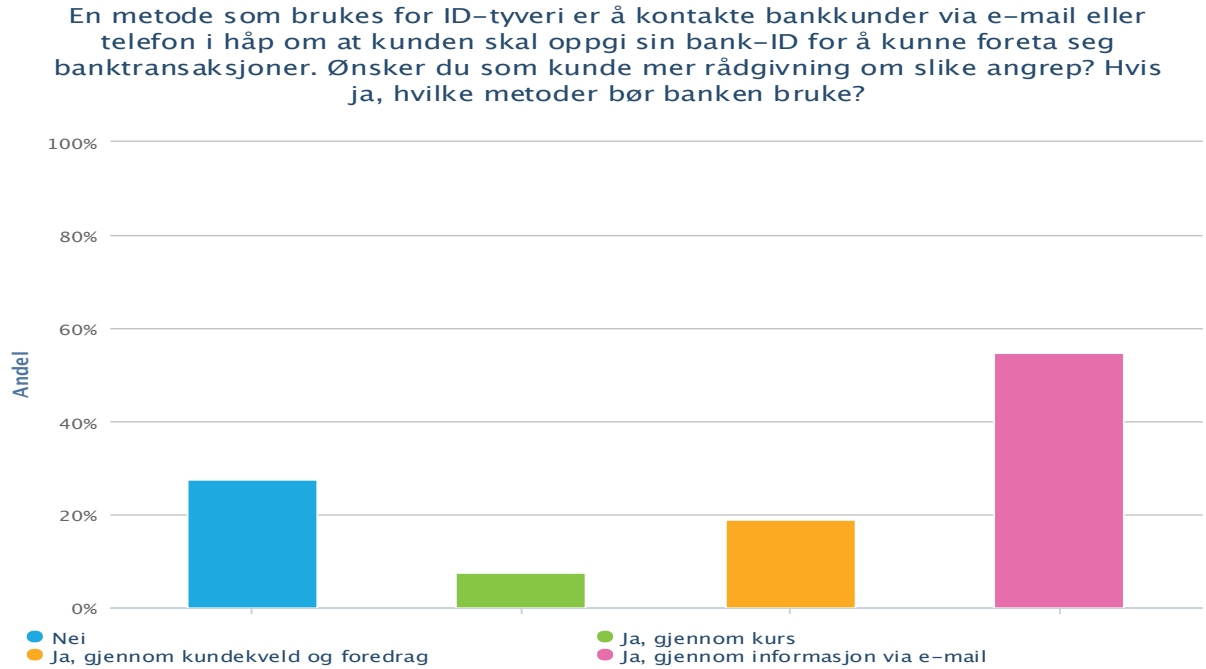
ved resultatet var å se på skillet mellom menn og kvinner og deres tillitsforhold ved bank og innsideangrep. Kvinner er klart mer skeptiske til banken når det gjelder innsideangrep, hvor 52 % av alle kvinnene som responderte valgte svaralternativet «Stor påvirkning, det svekker tillitsforholdet». Det var bare 38 % av alle mennene som responderte som valgte dette svaralternativet, noe som betyr at 62 % mente de var enten likegyldige til at banken kan ha innsideangrep eller det ikke har noen påvirkning.



Figur 17: Hackerangrep og ansvar

Det neste spørsmålet i spørreundersøkelsen tar for seg hackerangrep og ansvar. Hvem er ansvarlig når et hackerangrep oppstår, banken eller kunden? I dette spørsmålet la jeg frem et scenario for å gi respondenten grunnlag til å ta en vurdering om hvem som er ansvarlig dersom et hackerangrep oppstår. Jeg valgte å bruke et scenario for å forklare at dette gjelder kun dersom din personlige informasjon blir brukt til å foreta banktransaksjoner. Et hackerangrep i denne forstand brukes kun som et begrep for å gjøre respondenten oppmerksom på hva som blir diskutert, uten å definere dette videre. Spørsmålet tar høyde for at dette angrepet gjelder både når det er personlige angrep som bedrager og svindelangrep, i tillegg til angrep mot banken i seg selv. Det spørsmålet som stilles er hvorvidt respondenten syntes banken er ansvarlig for tilbakebetaling av penger dersom dette ville vært et resultat av et hackerangrep. 99,7 % av respondentene svarte at banken er ansvarlig, men det varierer i

hvilken grad banken skal stå ansvarlig. Det var 0,3 % av respondentene som svarte at banken ikke er ansvarlig i det hele tatt. Det svaralternativet som ble valgt flest ganger, 67,3 % var at banken var full ansvarlig. Figuren ovenfor viser resultatet av spørsmålet, som tydelig viser at respondentene mener at banken har et stort ansvar når det gjelder tilbakebetaling ved hackerangrep.

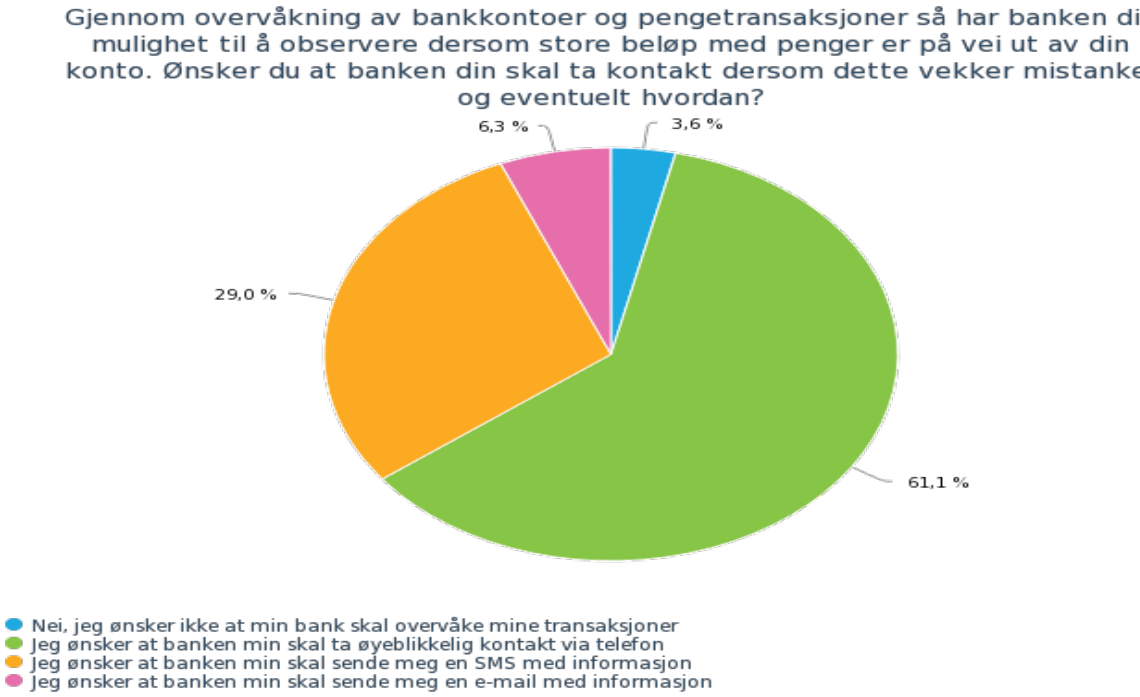


Figur 18: Kommunikasjon mellom bank og kunde

I tabellen ovenfor vises det fire ulike svaralternativer som var svar på om respondenten ønsker mer veiledning. 83 av de 303 respondentene svarte at de ikke ønsket mer veiledning fra banken sin. De resterende 220 respondentene ønsket mer veiledning, hvor flesteparten med 54,8 % ville at banken skulle sende ut mer informasjon om ID-tyveri via e-mail.

For å undersøke videre om resultatene viser noen trender, undersøkte jeg videre de individuelle spørreundersøkelsene for å finne sammenheng mellom alder/kjønn og svar på spørsmålet. Det første svaralternativet jeg tok for meg var «Nei». Av de 83 respondentene som svarte dette alternativet var det 44,57 % menn og 54,21 % kvinner. Ettersom det var flere kvinner som deltok i spørreundersøkelsen så vil ikke dette tallet vise noe særlig. Dersom vi beregner det ut fra den totale mengden kvinner og menn som deltok, så var det en høyere andel menn som valgte dette svaralternativet enn kvinner. Det neste svaralternativet som viste en antydning til en trend var svaralternativene «Ja, gjennom kundekveld og foredrag» og «Ja, gjennom informasjon via e-mail». Å få veiledning gjennom kundekveld og foredrag var

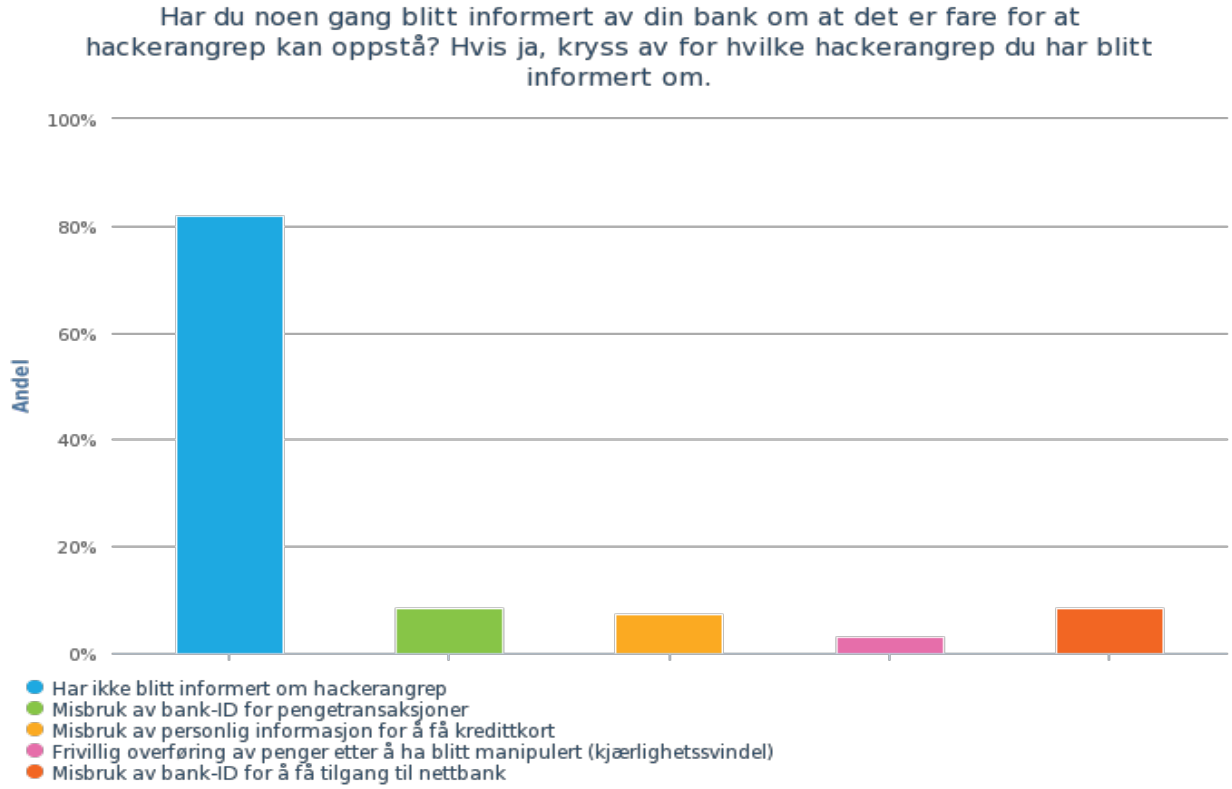
ønsket av 57 respondenter hvor 30 av disse var i aldersgruppen «18-28 år». Med en prosentandel på 52,63 kan det antydes at alder hadde en betydning for de som valgte dette svaralternativet. Det svaralternativet som flest respondenter valgte var å få informasjon fra banken via e-mail, med 166 respondenter. 92 av disse 166 var i aldersgruppen «18-28 år» og 46 var i aldersgruppen «40-60 år». Disse tallene viser til at det var flest unge som valgte dette svaralternativet. Dette kan likevel være misvisende da det var flere i aldersgruppen «18-28 år» som svarte på spørreundersøkelsen. Det var nemlig 46 av 83 respondenter i aldergruppen «40-60 år» som svarte med dette svaralternativet. Med dette kan det antydes at det ikke eksisterer noen trender på alder ved dette svaralternativet.



Figur 19: Overvåkning

Det syvende spørsmålet i spørreundersøkelsen handlet hovedsakelig om hvorvidt og hvordan respondenten ønsker å bli kontaktet dersom uregelmessige aktiviteter blir oppdaget på deres kontoer. I spørsmålsbeskrivelsen valgte jeg å informere om at banker i dag har en egen gruppe som er ansvarlig for å overvåke aktiviteter på banken sine kunder. Deres oppgave er å fange opp aktiviteter som antydes å være utenom det vanlige, som bl.a. store transaksjoner til utenlandske kontoer. Spørsmålet tok også for seg overvåkning og om respondenten ikke ønsker at banken skal overvåke deres aktiviteter. De tre andre svaralternativene var i forhold til hvilken metode respondenten ønsker at banken skal kontakte dem på dersom uregelmessig aktivitet oppdages. Figuren ovenfor viser resultatet fra spørreundersøkelsen, hvor først og fremst 96,4 % ønsker overvåkning, hvor kun 3,6 % sa at de ikke ønsket overvåkning. Av de

96,4 % av respondentene var det størst andel som ønsket å øyeblikkelig bli kontaktet gjennom telefon og nest størst andel ønsket å bli kontaktet via SMS. Det var kun 6,3 % som ønsket å bli kontaktet via e-mail.



Figur 20: Informasjon om hackerangrep

Det siste spørsmålet i spørreundersøkelsen handlet om kommunikasjon mellom bank og kunde i forhold til at det er en fare for at hackerangrep kan oppstå. Spørsmålet inkluderte også fire ulike metoder som brukes for å hacke kunder i banksammenheng. Spørsmålet tok for seg hvorvidt respondenten har blitt informert om hackerangrep av banken sin, og dersom ja hvilke hackerangrep respondenten har blitt informert om. Figuren ovenfor viser et diagram som er delt hovedsakelig inn i to ulike grupper. Ved å se på resultatet så viser dette at 81,8 % av respondentene ikke har blitt informert om hackerangrep fra sin bank. De resterende 18,2 % av respondentene har svart at de har blitt informert av banken sin, hvor det varierer mellom de fire ulike metodene de har blitt informert om.

Hovedfunn fra spørreundersøkelsen

Tabell 4: Spørreundersøkelse om cyberangrep i bank

Hovedfunn fra spørreundersøkelsen
• Spørreundersøkelsen hadde 303 respondenter fordelt på fem ulike aldersgrupper. Det var 202 respondenter som var kvinner og 101 respondenter som var menn. • 97 % av respondentene har tillit til banken, men tilliten er på ulik grad. Den største andelen var på 46,9 % som hadde nokså høy tillit til banken sin. Undersøkelsen viste også at desto høyere alder, desto mer tillit til banken. • 48,8 % av respondentene svarte at innsideangrep i bank kan påvirke tillitsforholdet de har til banken sin. De resterende 51,2 % var mente dette ville ikke ha påvirkning til tillitsforholdet eller at de var likegyldige. Alder og kjønn hadde stor påvirkning på svarene, hvor kvinner var mer skeptiske enn menn, og eldre mente det kunne påvirke tillitsforholdet i større grad enn unge. • 99,7 % av respondentene mener at banken er ansvarlig i alle cyberangrep dersom din personlige informasjon brukes til å foreta banktransaksjoner. Graden av ansvarsfordeling varierer, hvor høyest antall svar var at banken var full ansvarlig. • 27,3 % av respondentene ønsker ikke mer veiledning fra banken sin om cyberangrep. De resterende 72,6 % ønsket mer informasjon, hvor fleste parten ville ha mer informasjon via e-mail. • 96,4 % av respondentene ønsker at banken skal kontakte dem dersom uregelmessig aktivitet foregår på deres kontoer. 61,1 % ønsket å bli kontaktet øyeblikkelig via telefon. • 81,8 % av respondentene i undersøkelsen har ikke blitt informert om hackerangrep av sin bank. De som har blitt informert om hackerangrep varierer på ulike metoder.

5.2 Resultater fra Basel III

I denne delen av datainnsamlingen presenteres den empiriske sekundærdataen som brukes videre i diskusjonsdelen.

Bank for International Settlements (BIS) som er en internasjonal organisasjon som er opprettet for å kunne veilede banker til å kunne opprettholde stabilitet, og bidra til å skape samarbeid i den globaliserte finansnæringen. En del av BIS er baselkomiteen for banktilsyn, Basel Committee on Banking Supervision (BCBS), som ble opprettet på 70-tallet som skulle ha ansvar for internasjonal bankovervåkning. BCBS er en komite bestående av 45 deltakere med representanter fra sentralbanker og tilsynsmyndigheter fra de ulike medlemslandene. Denne komiteen skal opptre som en standard for tilsynsregulering av banker (BIS, 2018).

Det første rammeverket som ble introdusert av BCBS kalles Basel-I og ble introdusert i 1988. Dette rammeverket fokuserte hovedsakelig på kapitaldekning for bank. I 2004 ble en revidert utgave introdusert, kalt Basel-II, hvor rammeverket nå bestod av en videreutvikling av kapitaldekning, tilsyn og markedsdisiplin. Allerede seks år etter ble en ny og revidert utgave

introdusert, Basel-III. Årsaken til dette var finanskrisen i 2007 som stilte spørsmål ved om regelverket var godt nok rustet med hensyn til systemviktighet, egenkapital og likviditetskrav. I denne reviderte utgaven ble det vektlagt fokus på risiko og risikostyring gjennom resiliens. I de rammeverkene BCBS har publisert inneholder krav til banker som komitéen anbefaler at de bør følge (BIS, 2018).

5.2.1 Rapport 2018: Cyberresiliens

I 2017 ble en bekymring ytret av G20 Finances Ministers og Central Bank Governors, hvor deres uttalelse inneholdt blant annet (BCBS, 2018, s. 7):

> *"..the malicious use of information and communication technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability"*

På bakgrunn av denne bekymringen utredet BCBS en rapport som tar for seg en identifisering, beskrivelse og en sammenlikning av banker med fokus på observasjon av bruk av regler og cyberresiliens på tvers av jurisdiksjon (BCBS, 2018, s. 5). BCBS baserer sin rapport på data og informasjon fra en undersøkelse gjennomført av Financial Stability Board (FSB) (ibid., s. 5). Operational Resilience Working Group (ORG) bistod FSB i deres forskning ved å dele informasjon om deres erfaringer, slik at FSB skal kunne hente inn best- og mest mulig konkret informasjon i deres vurdering av trender, prosesser og hull i systemer når det gjelder cyberresiliens i banksektoren (ibid., s. 8). Rapporten er delt inn i ulike deler med fokus på ulike områder hvor delene om "cyber governance". Delen om kultur er mest relevant for denne oppgaven. "Cyber governance" kan forstås som styring av aktiviteter gjennom teknologi og digitalisering ved bruk av internett. Hva som ligger i begrepene "cyberdomenet" og "digitalisering" blir forklart ytterligere i neste kapittel.

Først og fremst er det nødvendig å forstå hva som legges i begrepet "cyberresiliens". I rapporten blir cyberresiliens definert som følger (BCBS, 2018, s. 8):

> *"The ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents"*

I kapitelet om cyber governance presenteres fem underkategorier som fokuserer på styring av risiko som kommer fra cyberdomenet (BCBS, 2018, s. 11). Denne delen av rapporten tar for seg fokusområder som sikkerhetsstrategi, ledelse og ansvar, sikkerhetskultur, arkitektur og

generelt arbeid med cybersikkerhet. De fem nevnte områdene er blitt vurdert av komitéen med fokus på tilsyn og mål om forbedring. Bakgrunnen for denne delen av rapporten er at risikoen fra cyberdomenet er en voksende og raskt utviklende trussel, og dermed skaper unike utfordringer for bankinstitusjoner som krever dedikert oppmerksomhet og ressursbruk (ibid., s. 5).

Til tross for at det ikke stilles krav til en egendefinert strategi for cybersikkerhet, så forventes det at institusjonen har en godkjent strategi for informasjonssikkerhet, med fokus på retningslinjer, prosedyrer og tilsyn av teknologien som brukes. Rapporten klargjør viktigheten med fokus på tiltak som skal minimere cybereksponering ved å øke sikkerheten i systemer gjennom resiliens (BCBS, 2018, s. 11-12). Rapporten beskriver viktigheten av anerkjennelse fra styret og ledelse når det gjelder ansvar og jurisdiksjoner i forhold til risikoen ved cyberdomenet. Flere banker har implementert 3LD-modellen, som er en risikostyringsmodell med tre linjer med forsvar. Hensikten med å bruke 3LD er for å kunne balansere ansvaret mellom styret og ledelsen, ulike aktører for risikostyring og internrevisjon. Modellen forutsetter at ansvaret fordeles likt på de tre linjene, noe som var manglende ifølge forskningen som har blitt foretatt i forhold til bankinstitusjoner (ibid., s. 12-13). Bevissthet om cyberdomenet og risiko som kommer fra bruk av cybernettverket, bør anerkjennes, og gjennom rapporten vises det at en felles sikkerhetskultur er grunnleggende for å kunne opprettholde robusthet. Dette bør opprettholdes i enhver bankorganisasjon med fokus på kontinuerlig læring og økt bevissthet. I rapporten legges det frem forslag om å fortsette å ha fokus på sikkerhetskultur både i økt bevissthet hos alle ansatte, samtidig som at det bør implementeres fokus på cybersikkerhet og sikkerhetskultur ved opplæring i ansettelsesperioden (ibid., s. 14). Rapporten presenterer funn som viser at det ikke foreligger generelle krav til arkitektur og standarder for banker. Det var et lite antall som hadde fokus på kontroll, og få land som hadde vekt på veiledning ved cybersikkerhetsarkitektur (ibid.). Det er stor variasjon i hvordan de ulike bankene prioriterer utvikling av kompetanse i forhold til cybersikkerhet. I de fleste banker foreligger det ikke spesifikke krav til kompetanse og relevante ressurser til cybersikkerhet. Det er likevel ulike praksiser på om krav som stilles til banker i de ulike landene. Enkelte myndigheter stiller krav til styring av personell, noen land har krav om konkrete rammer for kompetanse om cybersikkerhet, mens andre gjennomfører vurdering av kompetanse gjennom tilsyn og opplæringsprosesser (ibid., s. 14-15).

5.3 Resultater fra intervjuer

I denne delen presenteres resultatene fra intervjuene i tre ulike underkapitler for å tydelig vise til de ulike intervjuguidene som har blitt brukt. Hvert av de tre underkapitlene har en tabell med sammendrag av de funnene som anses for å være sentrale for videre diskusjon.

5.3.1 Intervju med ansatte

For å kunne vurdere sikkerhetskulturen i en organisasjon så var det første spørsmålet som ble stilt knyttet til hvilke faktorer som er viktige i en sikkerhetskultur, og hva en god sikkerhetskultur er for informantene. For å vise til hva som er viktig for de ansatte så velger jeg å vise til en ordsky. Ordskyen er generelt fra svarene til informantene i denne studien. Den viser til de presise faktorene som ligger til grunn i en god sikkerhetskultur.

Figur 21: Ordsky

Størrelsen på ordene viser til hvilke faktorer som har blitt nevnt flest ganger av de ansatte, hvor opplæring, kundeopplysninger, informasjon, kunnskap og bevissthet har blitt nevnt flest ganger. Både prosjektlederen, markedskonsulenten, fagleder IT-arkitektur og teamleder på kundesenter la ekstra vekt på at det var viktig å ivareta kunden i alle aktiviteter som ble gjennomført. Prosjektlederen sa: *«Å ha en god sikkerhetskultur anser jeg at du skal ha sikkerhet i tankene og i det du gjør»,* mens systemeieren sa at sikkerhetskultur handler om: *«..å ha god kontroll på datamaskinen din, pulten din og arbeidsverktøyene dine».* For senior HR-rådgiveren så vil det å ha en god sikkerhetskultur være basert på: *«..at ansatte etterkommer de anbefalinger og instrukser som kommer fra sikkerhetsavdelingen».*

I spørsmålet om det var et etablert rammeverk i SR-Bank som skal bidra til å skape en sikkerhetskultur så var det flere uklare svar. CDO mente at det var et rammeverk, men at det kanskje ikke var uttalt og tydelig, men at det absolutt var tilstede. Tilsvarende ble nevnt av senior HR-rådgiveren da han sa: *«Ja, det regner jeg med at det er uten at jeg kjenner til innholdet i den»,* dette var på bakgrunn av hans jevnlige samtaler med sikkerhetsavdelingen. Fagleder IT-arkitektur var en tredje informant som ytret lignende hvor han sa: *«Ja, det er det, men den er kanskje ikke fullt kjent og godt brukt»,* i et videre spørsmål om hvordan han kunne vite at den var etablert svarte han: *«Det er litt sånn, jeg vet at den finnes, men jeg har vel i grunnen ikke fått noen innføring eller gjennomgang av den».* De resterende informantene hadde alle et synspunkt at gjennom prosedyrer og retningslinjer som bl.a. taushetsplikt så v ar det en felles oppfatning om at det foreligger et rammeverk for sikkerhetskultur.

I spørsmålet om ledelsen bidrar til å skape en god sikkerhetskultur så kom det frem ulik informasjon. Når det gjaldt om ledelsen deltar generelt, så var det et repeterende ja fra alle informantene, men det var ulike svar på når de trådte inn og i hvilken grad ledelsen deltok. CDO sa at han opplevde at ledelsen var involvert tidlig nok slik at de ikke bare bidro i beslutningsfasen, men også gjennom hele prosessen. Prosjektlederen hadde et annet synspunkt på dette hvor hun opplevde at ledelsen ofte kom for sent inn i bildet, og skulle ønske de var med tidligere. Senior HR-rådgiveren sa: *«I utgangspunktet tror jeg de gjør det de kan for å bidra til en sikkerhetskultur, og så kan det variere på kompetansenivå naturlignok»,* mens fagleder IT-arkitektur sa de var tilstede på bakgrunn av: *«Det er jo for eksempel ved at de har en sikkerhetsavdeling, og at den har blitt styrket med flere ressurser og ansatte».*

En stor del av sikkerhetskultur handler om rapportering av hendelser som anses som uønskede, og i den forbindelse var det fjerde spørsmålet om de ansatte var klar over hvordan rapportering fungerte i SpareBank 1 SR-Bank. Markedskonsulenten, senior HR-rådgiveren, teamleder kundesenter, CDO og fagleder IT-arkitekt nevnte alle en hendelsesdatabase som ble brukt til å rapportere uønskede hendelser. Systemeieren henviste til flere ulike metoder som brukes for rapportering, mens prosjektlederen opplevde at det var rapportering, men i liten grad til hva hun hadde opplevd i andre organisasjoner.

Det neste spørsmålet var for å samle inn informasjon om hvilke hendelser som blir rapportert og om det er eventuelle konsekvenser for rapportering. Teamleder på kundesenter sa at

rapportering gjelder forskjellige saker: *«Det kan være fra alt i fra forfalskning i form av at folk utgir seg selv for å være noen andre ved bruk av Bank-ID, det kan være hvitvasking eller hendelser som gjør at man kan fatte en form for mistanke».* Basert på egne erfaringer sa senior HR-rådgiveren: *«Jeg har ikke opplevd negative konsekvenser på det jeg har rapportert. Jeg har et par ganger fått et par oppfølgingsspørsmål om hva som hendte fra sikkerhetsavdelingen, men utover det har jeg ikke merket noen ting».* Lignende ble nevnt av CDO ved: *«Jeg opplever at det oppfordres til å rapportere inn, så jeg opplever ikke at det er noen slike negative konsekvenser»* spørsmål om det var konsekvenser for rapportering. Dette utsagnet ble støttet av de andre informantene, hvor det var ingen som la frem klare meninger om at konsekvenser kunne oppstå ved rapportering. Prosjektlederen derimot vektla en bekymring hvor hun opplevde at kulturen ikke lå til rette for rapportering av uønskede hendelser.

Det neste spørsmålet var basert på den ansattes myndighet til å ta avgjørelser i krisesituasjoner. Det var ulike svar fra de ulike informantene om myndighet til å ta avgjørelser. Samlet sett uavhengig av beslutningsmyndighet så ville de fleste ta avgjørelser dersom det var nødvendig på grunn av tidspress. Prosjektleder sa at dersom man har tid og mulighet til å kontakte sikkerhetsavdelingen eller øverste leder så ville hun gjort det, og sa videre: *«Nei, jeg har ikke myndighet, men så er spørsmålet om tidsaspektet og hvor alvorlig ting er i forhold til hvordan du agerer».* For CDO så hadde han frie rammer til å ta avgjørelser, men dersom han skulle knytte banken til noe, så ville han forsikret seg om at det var greit for ledelsen. Systemeieren sa: *«Du har alltid tilgang til egen hjerne for å si det veldig enkelt»* og sa videre at dersom man skulle hjelpe en kunde så hadde hun myndighet til å ta avgjørelser. Senior HR-rådgiver svarte at han hadde myndighet til å ta avgjørelser, men at avgjørelsene skulle være i henhold til beredskapsplanen som foreligger, mens teamleder kundesenter og fagleder IT-arkitektur sa at de begge ikke hadde myndighet i det hele tatt.

Det siste spørsmålet i intervjuene med ansatte handlet om fokus på evaluering av uønskede hendelser. Senior HR-rådgiver var skeptisk til evaluering og sa: *«Hvis vi skal være ærlige, tror jeg at vi kan si vi ikke er gode nok på det på sånn generelt grunnlag. Der er det forbedringspotensialet».* Markedskonsulenten delte også dette synspunktet og sa: *«Nei, vi har nok ikke evaluert mye, men jeg tror heller ikke vi har hatt så mange hendelser»,* og samme gjorde prosjektlederen: *«Jeg har ikke fått en evaluering av en uønsket hendelse uten at jeg har spurt om det selv».* CDO ytret at han kjente ikke noe særlig til hvordan evaluering fungerer,

men basert på egne erfaringer så har han tidligere rapportert inn og deretter ikke fått noen tilbakemelding. Systemeieren på den andre siden sa: *«Den som har meldt inn får tilbakemelding om hva som er gjort i det konkrete tilfellet».* Teamleder på kundesenteret opplevde lignende hvor de snakket mye om uønskede hendelser og det var fokus på dette. At evaluering får fokus i SpareBank 1 SR-Bank blir også nevnt av fagleder IT-arkitektur ved hans utsagn: *«Ja, det mener jeg vi har med den hendelsesdatabasen vi har og hvordan den er bygget opp med å involvere den rette til å finne ut hva som skjedde, hva hendelse betydde, hvordan vi fikser det og hva vi gjør for at det ikke skal skje igjen».*

Hovedfunn intervju med ansatte

Tabell 5: Intervju av ansatte

Hovedfunn intervju med ansatte
• En god sikkerhetskultur betyr å ha fokus på opplærling, kundeopplysning, informasjon, kunnskap og bevissthet. Sikkerhet må være henhold til retningslinjer fra sikkerhetsavdelingen i alt du gjør av aktiviteter, i tillegg til å ha kontroll på arbeidsverktøyene dine. • Det er et rammeverk for sikkerhetskultur i SpareBank 1 SR-Bank, men dette er utydelig og lite brukt. Retningslinjer, prosedyrer og taushetsplikt brukes som eksempel på et eksisterende rammeverk. • Det er deltakelse fra ledelsen når det gjelder sikkerhetskultur, men grad av deltakelse varierer. • Det brukes en hendelsesdatabase til å rapportere uønskede hendelser og avvik i SpareBank 1 SR-Bank. Det varierer hvor ofte rapportering skjer. • Det er stor variasjon i hvilke hendelser som blir rapportert i SpareBank SR-Bank. Det oppleves ikke at det kan oppstå konsekvenser for rapportering, hvor flere opplever en oppmuntring til rapportering. • De ulike informantene har ulik grad av myndighet til å ta avgjørelser. Denne graden varierer på bakgrunn av stilling og kompetansenivå. • Det er evaluering av rapporterte hendelser i SpareBank 1 SR-Bank, men dette varierer i ulik grad på de ulike avdelingene.

5.3.2 Intervju med ledelsen, gruppe 1

Det første spørsmålet som ble stilt i intervjuene med konserndirektør for kommunikasjon, personvernombudet og senior rådgiver for sikkerhet, handlet om at banken brukte en bestemt metode for å informere kundene sine om cyberangrep og følgende konsekvenser. *«Vi gir generell informasjon på våre websider, og tipsene endrer seg litt og litt på hva kunden bør være oppmerksom på»* sa sikkerhetsrådgiveren, men han la også til at det er ikke alltid de gir all informasjon som er tilgjengelig for de ønsker ikke å dele for mye informasjon. Dette kom også frem fra konserndirektøren for kommunikasjon og bærekraft, hvor han vektla at kommunikasjonsmetoden skal brukes på riktig måte slik at man unngår panikk.

Personvernombudet nevnte også at dersom kunder tar kontakt med banken på eget initiativ, så vil de også bli godt ivaretatt med en god dialog. De siste årene har det vært fokus på en strategi om å gi kunden et høyere kompetansenivå rundt cyberangrep, bakgrunnen for dette kom frem i intervjuet med konserndirektøren for kommunikasjon og bærekraft: *«Dette har jo handlet litt om at når ting skjer så ønsker vi at det skal være et visst kompetansenivå hos de aller fleste kundene våre, som gjør at det ikke blir en slik panikk».*

I spørsmålet om det var fokus på å gi informasjon om nye lovgivninger kom det frem ulik informasjon fra informantene. Seniorrådgiver for sikkerhet forklarte at kundene ofte ble informert om GDPR gjennom media om hvilke rettigheter kunden har, og at banken da hadde ansvar for å følge opp disse kravene. Fra personvernombudet kom det en klarere beskjed om hvordan dette har blitt kommunisert ut fra banken: *«I juli når det var nytt så hadde vi et slags banner på nettbanken og nettsiden om nytt personvernlovverk hvor du kunne gå inn og lese mer».* Det kom også frem at i den siste tiden har dette blitt fjernet som banner, men informasjonen ligger fortsatt tilgjengelig på nettsiden. Det er også mulig å ta i bruk bankens sin chat-funksjon «Banki» som vil svare på enkle spørsmål om blant annet GDPR og eventuelt sende kunden videre til personvernerklæringen. I intervjuet med konserndirektør for kommunikasjon og bærekraft vektla han: *«Tillit til bank er utrolig høy, kanskje i noen tilfeller litt for høy»* og fortsatte ved å forklare at når banken sender ut informasjon og samtykkeerklæringer til kunden så opplevde han at de aller fleste ikke leser gjennom informasjonen. På underspørsmålet om det var innført noen tiltak for å beskytte kundene mot at ansatte kan spre informasjonen, ble det fra alle informantene forklart at de brukte et sporingssystem som gjør at overvåkingstemaet kan avdekke om ansatte har brukt informasjon de ikke skal bruke. Dette utdypes av konserndirektøren for kommunikasjon og bærekraft: *«Over tid vil jeg si vi har bygget opp en god kultur gjennom kommunikasjon og holdningskampanjer, som gjør at kulturen hos oss sitter veldig godt som gjør at det er en begrenset risiko for at ansatte deler informasjon om kunder til enten utenforstående eksternt eller utenforstående internt».* Konsekvenser for deling av slik informasjon i SpareBank 1 SR-bank er ganske harde og kan resultere i oppsigelse, noe som alle ansatte er klar over ifølge sikkerhetsrådgiveren. Fra personvernombudet poengteres det at dette er ikke tiltak som har blitt innført etter de nye lovgivningene knyttet til personvern, men at det: *«..ligger i bunn som ryggmargen til banken*».

Hvem som er ansvarlig dersom et cyberangrep oppstår handler mye om hvilken type angrep som legges til grunn. Dette kom klart frem fra alle informantene, og det skilles i ansvarsfordelingen avhengig av angrepet. *«En ting er ansvaret hvis det er hele nettbanken som er rammet og det lekker ut millioner, da er jo kunde uforskyldt, da er det vår infrastruktur som er dårlig. Men en annen ting er hvis kunden selv slipper inn den utenfor og vil ha tak i midlene. Da skiller vi på type uaktsomhet»* sa personvernombudet, og forklarte videre at de så langt ikke har akseptert noen tilfeller av sistnevnte hendelser uten å ta det videre til en rettsavgjørelse. Fra seniorrådgiveren for sikkerhet så blir det forklart at de ikke anser deling av Bank-ID som et cyberangrep og han sier: *«..slipper du noen inn i nettbanken ved å gi de koder, så er vi innenfor at det er kunden sitt ansvar. Da har kunden delt koder og det skal kunden vite at du ikke skal gjøre».* På bakgrunn av dette forklarte han at slike angrep ikke vil være SpareBank 1 SR-Bank sitt ansvar.

Det siste spørsmålet som var knyttet til den kvantitative datainnsamlingen, spørreundersøkelsen, så var spørsmålet om banken har noen tjenester de tilbyr til kunder for å gi økt informasjon og kunnskap om håndtering av angrep. Fra intervjuene med de tre informantene kommer det frem at de ikke tilbyr tjenester som via kurs og veiledning. På en annen side så har banken flere kurs for sine ansatte som skal bidra til å gjøre de ansatte mer robuste i dialog med kundene. Det har også vært diskutert om det skal tilbys bedriftskunder kurs, men med informasjon fra personvernombudet så har ikke dette blitt realisert enda. Fra intervjuet med seniorrådgiver for sikkerhet, så fortalte han at han har hatt foredrag for bedriftskunder hvor de informerer om cybersikkerhet, men for privatkunder ligger det kun informasjon på deres nettsider. Nettsiden og SpareBank 1 SR-Bank sitt nyhetssenter via Facebook blir brukt for å gi informasjon om aktuelle saker, endringer og når man bør være ekstra oppmerksom.

Del to i denne intervjuguiden som ble brukt som et utgangpunkt i intervjuene, handlet om sikkerhetskultur. I intervjuet med seniorrådgiveren for sikkerhet så forklarte han at sikkerhetskultur ble målt av sikkerhetsavdelingen for å se til at opplæring og månedlige kurs bidro til en kultur i banken. Måten de måler sikkerhetskulturen på er gjennom ulike spørsmål som bl.a. om man har sett ansatte gå fra datamaskinen ulåst og testing av passord for å måle kunnskapsnivå. For konserndirektøren for kommunikasjon og bærekraft så beskrev han en god sikkerhetskultur slik: *«En god sikkerhetskultur handler om å sørge for at du er trent, og at du har utviklet en kritisk sans som gjør at du kan vurdere hendelser og henvendelser*

fortløpende på eget initiativ, og faktisk kunne huke av dersom det er noe her som kan virke for godt til å være sant». Han fastslo videre at sikkerhetskultur handler om at de ansatte er åpne for å tilføye seg ny kunnskap og ikke være fastslått i å bruke gamle modeller for hva som er god sikkerhetskultur. Videre må alle ansatte: *«..ha et dynamisk forhold til risikobildet, fordi risikobildet forandrer seg hele tiden».* Personvernombudet vektla retningslinjer i hennes syn på hva god sikkerhetskultur var: «*En skal kjenne til hvilke retningslinjer man skal forholde seg til, og følge disse og fremstå som en god ambassadør og ikke være villig til å fire på kravene for at man skal være mer effektiv»*, mens seniorrådgiveren for sikkerhet vektla rapportering i en god sikkerhetskultur: *«Du har en plass å melde hendelser, at hvis det skjer noe så er det lett å melde fra, og du vet at det blir behandlet, og du kan sette inn tiltak».*

I spørsmål om de nevnte faktorene er gjeldende i SR-bank så sa personvernombudet at hun mente at fokus på retningslinjer absolutt er tilstedeværende og at dette har blitt vektlagt mye de siste årene. Fra konserndirektøren for kommunikasjon og bærekraft sa han: *«Vår sikkerhetsavdeling over tid har gjort mye godt på dette området, fordi vi har beveget oss fra et fysisk risikobilde gjennom håndtering av kontanter på kontorene, til å nå ikke se disse kjeltringene med finlandshette, men at trusselen nå ligger i skyen*». Årsaken til at dette ifølge han hadde fungert bra er på grunn av høy kompetanse og godt samarbeid på tvers i konsernet. Fra seniorrådgiveren for sikkerhet så viser deres målinger at SpareBank 1 SR-bank blir stadig bedre på det han legger i en god sikkerhetskultur.

I spørsmål om det foreligger en bestemt sikkerhetsstrategi som er grunnleggende for sikkerhetskulturen i SpareBank 1 SR-Bank så kan det tolkes ut ifra svarene fra informantene at dette ikke er tilfellet. Seniorrådgiveren for sikkerhet forklarte at det brukes en strategi med fokus på MTO-prinsipp (menneske, teknologi og organisasjon), men han var usikker på om dette brukes i henhold til sikkerhetskultur. Fra konserndirektøren for kommunikasjon og bærekraft så henviste han til at de har en sikkerhetsavdeling og deres statusrapporter. Lignende ble sagt av personvernombudet da hun også henviste til et intranett som er et medium som brukes i banken med oppfordringer til å dele historier knyttet til cyberangrep.

Med ønske om å evaluere ledelsens rolle i en sikkerhetskultur fra et lederperspektiv, så valgte jeg å stille spørsmål om hva de mener ledelsen gjør for å skape en god sikkerhetskultur. Konserndirektøren for kommunikasjon og bærekraft uttrykte at ledelsen var opptatt av sikkerhetskultur og sa: *«Hvis ikke konsernledelsen og administrerende hadde vært opptatt av*

det, så tror jeg heller ikke vi hadde fått en slik god kultur rundt ellers i organisasjonen». Seniorrådgiveren for sikkerhet forklarte at ledelsen ofte er i dialog med sikkerhetsavdelingen for å vise deres støtte til sikkerhetsavdelingens arbeid. Ifølge han vektla ledelsen fokuset på opplæring og de kursene sikkerhetsavdelingen sender, og han sa videre: *«En forutsetning for å få bonus er at du må ha gjennomført disse kursene. Dette viser jo at sikkerhet er mer aktuelt nå enn hva det var tidligere».* For personvernombudet så handlet det om synlighet og at ledelsen viste at de er synlige på deres intranett. Informasjon og opplæring ble vektlagt hos ledelsen og hun ytret viktigheten i at det hele tiden er på den daglige agendaen.

Det siste spørsmålet handler om rapportering av feil, og om det er en oppmuntring fra ledelsen til å rapportere uønskede hendelser knyttet til cyberangrep. Seniorrådgiver for sikkerhet forklarte at SpareBank 1 SR-Bank bruker en hendelsesdatabase hvor det meldes inn uønskede hendelser, i tillegg har de en mailadresse hvor de oppfordrer ansatte til å sende inn informasjon dersom det er usikkerhet. Personvernombudet har en klar rolle når det gjelder rapportering, og fra sitt ståsted sa hun: *«Det blir signalisert at det skal være en lav terskel for å rapportere alle typer feil».* Dette var noe hun fokuserte på i samtaler med de ansatte på bakgrunn av: *«Ofte er jo feil en menneskelig handling, og det viktigste er at man lærer av det og unngår å gjøre det på ny».* Det nevnte utsagnet har fellestrekk til det konserndirektøren for kommunikasjon og bærekraft sa: *«Jeg opplever at systemet i forhold til å avdekke når det oppstår uønskede hendelser, er ikke for å straffe, men det er for å lære».* Han sa videre *«Jeg syntes at vi på dette området har beveget oss konstruktivt i rett retning i forhold til at det ikke er frykten for å feile som styrer. Nå er det akseptabelt å feile og det tror jeg er en felles oppfatning i konsernet, under forutsetning av at vi lærer av det. Hvis vi gjør gjentakende feil i de samme tingene, så skal det ikke være akseptabelt å feile».*

Hovedfunn intervju med ledelsen, gruppe 1

Tabell 6: Intervju av ledelsen, gruppe 1

Hovedfunn intervju med ledelsen, gruppe 1	
Spørsmål knyttet til spørreundersøkelsen	• Informasjon om cyberangrep blir lagt ut på SpareBank 1 SR-Bank sine hjemmesider. De ønsker å gi nok informasjon for å gi kundene kompetanse om cyberangrep, men ikke for mye slik at de skaper panikk. • Ved nye lovgivninger så har det vært fokus på informasjon ved å bruke nettbank og hjemmesiden til SpareBank 1 SR-Bank. Det er høy tillit til banken blant befolkningen, noe som gjør at kunder ofte samtykker til informasjon som banken gir, uten å gå gjennom den. • Brudd på regler som å dele kunder sin informasjon tas alvorlig, og kan i verste fall resultere i oppsigelse. Det oppleves å være en god kultur som gjør at ansatte ikke deler slik informasjon. • Ansvarsfordelingen dersom et cyberangrep oppstår er todelt og blir vurdert ut ifra hvilket angrep som har oppstått, og om kunden selv har vært delaktig i å dele informasjon. • SpareBank 1 SR-Bank tilbyr ikke tjenester som kurs og veiledning for kunder når det gjelder cyberangrep og informasjon om informasjonssikkerhet.
Spørsmål knyttet til sikkerhetskultur	• En god sikkerhetskultur blir målt i SpareBank 1 SR-Bank for å kontrollere at månedlige kurs og opplæring bidrar til en kultur. Faktorer som er viktige for en god sikkerhetskultur er: Ha en kritisk sans, være trent, ha et dynamisk forhold til risikobilde, kjenne til retningslinjer og ha rapportering av uønskede hendelser. • En god sikkerhetskultur er eksisterende gjennom de nevnte faktorene i SpareBank 1 SR-Bank. • Å ha en sikkerhetskultur blir prioritert i SpareBank 1 SR-Bank gjennom å ha en god sikkerhetsavdeling med høy kompetanse. • Statusrapporter og MTO-strategien brukes som en strategi for sikkerhetskultur SpareBank 1 SR-Bank. • SpareBank 1 SR-Bank sin ledelse bidrar til en sikkerhetskultur ved å være synlige og være opptatt av sikkerhet generelt. Informasjon og opplæring viser også at ledelsen vektlegger sikkerheten i banken. • Det brukes en hendelsesdatabase til å rapportere uønskede hendelser i SpareBank 1 SR-Bank. Det er lav terskel for å rapportere, og rapportene brukes for evaluering og videre læring. Det er akseptabelt å feile så lenge man tar lærdom av feilen.

5.3.3 Intervju med ledelsen, gruppe 2

I et forsøk på å evaluere motstandsdyktigheten i SpareBank 1 SR-Bank så ble sikkerhetssjefen og konsernbanksjefen IT-drift intervjuet. Det første spørsmålet er knyttet til om det foreligger beredskapsplaner og retningslinjer som skal inneholde informasjon om hva de ansatte skal gjøre dersom et cyberangrep oppstår. Begge informantene fortalte at SpareBank 1 SR-Bank har beredskapsplaner, slik som sikkerhetssjefen sa: *«Det er generelle beredskapsplaner, og vi har et generelt planverk for krisehåndtering».* Beredskapsplanen er publisert og lett tilgjengelig for de ansatte som har som å rolle å respondere på uønskede hendelser.

Det neste spørsmålet handlet om overvåkning og om banken til enhver tid har ansatte på jobb som kan håndtere et cyberangrep. Konsernbanksjefen IT-drift forklarte at de kontinuerlig har folk som kan håndtere cyberangrep, men at de ikke nødvendigvis sitter på kontorene i SpareBank 1 SR-Bank. Gjennom banksamarbeidet i SpareBank 1 gruppen så har de en overvåkningsfunksjon kalt Incident Respons Team (IRT) som er ansvarlig for alle aktiviteter knyttet til nettverksfunksjon. IRT ble også nevnt av sikkerhetssjefen da han svarte: *«Ja, vi har en 24/7 funksjon for overvåkning».* IT-drift-avdelingen vil også være knyttet til å håndtere cyberangrep, men dette er på dagtid, og de er i kontinuerlig kontakt med IRT dersom de ønsker økt overvåkning.

I evnen for å kunne respondere så handler det om responstid. Dette er bakgrunnen for det neste spørsmålet som ble stilt i intervjuene, om hvor lang tid som regnes med å bruke på å komme tilbake til normaltilstanden. Fra begge informantene så ble det uttrykt at det var vanskelig å kunne gi et eksakt svar på responstid, men at det jobbes så raskt som mulig å komme tilbake til normalstand. *«Det er veldig vanskelig å si hva den faktiske tidsrammen er, det kommer helt an på scenarioet»* sa sikkerhetssjefen, og det samme sa konsernbanksjefen IT-drift: *«Ekstremt vanskelig å svare på for det spørs helt på hva det er som har skjedd».* Han la til at de erfaringsvis bruker mellom 20 sekunder og 2 minutter på å kunne komme tilbake til normaltilstanden ved et DDoS-angrep, men hvis det er et kryptoangrep som har oppstått så kan det brukes opp til én dag for å komme tilbake til normaltilstanden. I spørsmål om når kunden blir kontaktet dersom slike angrep oppstår så svarte sikkerhetssjefen: *«Hvis det er en hendelse som treffer konsernet, så er vi under regulatoriske krav for varsling av kundene, hvor de skal bli kontaktet uten opphold. Da blir kundene kontaktet så fort vi har mulighet, etter vi har gjennomgått hendelsen og omfanget».* Han fortalte videre med at dersom et cyberangrep skjer direkte på kunden, så vil håndteringen være annerledes: *«Hvis vi har*

cyberangrep som treffer kundene i reell tid, så blir de umiddelbart kontaktet». Fra konsernbanksjefen IT-drift så fortalte han at det er kundesenteret til SpareBank 1 SR-Bank som er ansvarlig for kontakten med kundene.

Når det gjelder systemene som brukes i SpareBank 1 SR-Bank så er flere av disse systemene på utkontrakteringsavtaler eller forvaltet gjennom SpareBank 1 gruppen. Dersom systemene er på utkontrakteringsavtaler fortalte sikkerhetssjefen at da er det leverandøren som er ansvarlig for at disse systemene skal være oppdaterte og intakte. Når det gjelder systemene i SpareBank 1 gruppen så er ansvaret todelt, ved at man har en systemeier og en systemansvarlig i både SpareBank 1 gruppen og i SpareBank 1 SR-Bank. I de systemene SpareBank 1 SR-Bank er forvalter selv så er det konsernbanksjefen som er hovedansvarlig, men at dette ansvaret delegeres til en systemeier og en systemansvarlig. I spørsmålet om det er regelmessig testing av systemet så sa sikkerhetssjefen: *«Vi har jo regelmessige driftshendelser som gjør at vi bruker reserveløsninger. Når det gjelder testing, så tester vi alle systemene før produksjonssetting som en sikkerhetstest, men regelmessig testing eller gjør vi ikke systematisk».* Fra konsernbanksjefen IT-drift så kom det frem at systemene gjennom SpareBank 1 gruppen blir testet årlig.

Det neste spørsmålet var om det er fokus på overvåkning i SpareBank 1 SR-Bank. *«Ja, vi har et 24/7 overvåkningsteam som overvåker cyberhendelser. I tillegg til det så har vi interne overvåkningsprosedyrer for å se på systemer som har mye kundeinformasjon»* sa sikkerhetssjefen. I samtalen med konsernbanksjefen IT-drift kom det frem at Sparebank 1 SR-Bank for tiden beveger seg fra en tradisjonell driftsmodell til en dynamisk sikkerhetsmodell. I den sammenheng diskuteres det hvem som skal være ansvarlig for overvåkning i fremtiden, hvor de går fra å overvåke uønsket trafikk til å heller fokusere på hva som er ønsket trafikk. Han avsluttet med å si: *«Så, hele måten å tenke sikkerhet på blir ikke lenger «chinese wall» for å prøve å beskytte det, men mer å ha en oversikt over hva som er normal og unormal drift».*

Det neste spørsmålet som ble stilt var også knyttet til overvåkning, og på hvilken måte SpareBank 1 SR-Bank overvåker dagens utfordringer knyttet til cyberangrep. Her ble det nevnt av konsernbanksjefen IT-drift at dette er en tjeneste som de har på utkontrakteringsavtale gjennom SpareBank 1 gruppen. Denne leverandøren er ansvarlig for å overvåke dersom det oppstår datatrafikk som ikke er å anse som normal. Sikkerhetssjefen la

til at de har flere leverandører de bruker, både internasjonale og lokale. *«De lokale leverandørene er de som filtrerer vekk mye av den informasjonen som ikke treffer bedrifter i Norge, og fokuserer veldig mye på de trussel scenarioene som er relevante her»* sa sikkerhetssjefen videre. I tillegg så la konsernbanksjefen IT-drift frem at de også har interne overvåkningsverktøy gjennom IRT som brukes for å løpende evaluere om det oppstår hendelser som kan være suspekte og hvor det bør innføres tiltak.

Hvor ofte beredskapsplaner og tilhørende retningslinjer blir oppdatert var fokus i det neste spørsmålet i intervjuene. *«Det vi har på beredskapsplanverk er ganske generelt. Det er designet slik at du kan motstå enhver hendelse som kommer opp. Grunnen til at vi har gjort det slik, er at hvis du skal dokumentere enhver type hendelse som eventuelt kan komme opp så produserer du en masse dokumentasjon som aldri blir brukt»* ble sagt av sikkerhetssjefen, hvor det fokuseres på å ha et generelt planverk, men også ha en hendelsesdatabase med hendelser som kan brukes som et oppslagsverk. Fra konsernbanksjefen IT-drift ble det sagt: *«Vi har et sett med policyer, standarder og retningslinjer, og de revideres når det er behov for det».* Videre kom det frem fra sikkerhetssjefen at selv om de ikke oppdaterer beredskapsplanen, så oppdateres det tiltak som å styrke eventuelle svakheter i systemene. Dette gjøres ved å innhente informasjon fra de eksterne leverandørene, og basert på den nye trusselvurderingen så opprettes det tiltak. *«Overvåkningsteamet vil ta den informasjonen og legge det inn i våre systemer, for å legge inn blokkeringer eller deteksjon. Det kommer helt an på trusselen om du ønsker blokkering eller deteksjon»* sa han avslutningsvis.

Det neste spørsmålet var om de ansatte i SpareBank 1 SR-Bank er kontinuerlig opplært i alle typer trusler, knyttet til cyberangrep, som banken står ovenfor. Her sa begge informantene nei, og konsernbanksjefen la til: *«Nei, for det tenker jeg nesten ikke er mulig».* Han sa videre at dette var årsaken til at de ønsker å bruke generelle beredskapsplaner hvor ledelsen ønsker å gjøre de ansatte kompetente i å oppfatte når noe som ikke er ønskelig oppstår og hvordan de skal håndtere det. Han avsluttet med å si: *«Alle skal være opplært i hvordan vi skal agere på noe som enten ikke er bra, eller lurer på om det er bra. Det kan være alt i fra fysiske hendelser til IT-tjenester».* Sikkerhetssjefen la til at de bruker månedlige opplæringskurs som alle ansatte får via e-mail, og at dette skal være et verktøy for å gi de ansatte oppdatert informasjon om ulike trusler de står ovenfor. *«Vi endrer fokus på de forskjellige læringskursene på de tingene som er relevante akkurat i øyeblikket»* ble sagt før han la til at

de i tillegg har en statistikk over hvor mange av de ansatte som faktisk gjennomfører disse kursene.

«Det er både trusselvurdering i SpareBank 1 gruppen og her i SpareBank 1 SR-Bank. Trusselvurderingene blir forelagt styret, og jeg tror trusselvurderingen i SpareBank 1 gruppen er halvårig, mens i SpareBank 1 SR-Bank årlig» svarte konsernbanksjefen IT-drift på spørsmålet om hvor ofte det blir foretatt en trusselvurdering. Sikkerhetssjefen svarte: *«Trusselvurderinger blir gjort kontinuerlig. For det teamet som er ansvarlig for deteksjon vil da se trusselbildet kontinuerlig»,* og han la til at han som sikkerhetssjef daglig sjekker informasjonen de får fra leverandører for å se hva som skjer i miljøet. I SpareBank 1 SR-Bank blir det årlig gjennomført en risiko- og sårbarhetsanalyse basert på trusselvurderingen som blir foretatt. Denne risikoanalysen er basert på en risikomatrise hvor risikoevalueringen er basert på sannsynlighet, konsekvens og frekvens. Sikkerhetssjefen sa videre at risikomatrisen er delt inn i seks ulike dimensjoner: operasjonell risiko, omdømme, økonomi, etterlevelse av det regulatoriske, strategi og forretning, og liv og helse. I samtalen med konsernbanksjefen IT-drift sa han: *«Primært er det tre ting vi vurderer knyttet til et risikostyringssystem: tilgjengelighet, integritet og konfidensialitet. Og da er risikoen i form av at systemet ikke vil være tilgjengelig, hvor krise ville det vært hvis noen fikk tilgang som ikke skulle ha tilgang, og hvor krise det ville vært hvis noen ville manipulert dataen som ligger her».* Fra begge informantene var det enighet om dersom risikoen på noen måte ble vurdert som høy, så vil det implementeres tiltak for å redusere denne.

Det neste spørsmålet handler om rapportering av uønskede hendelser, i hovedsak avvik og hendelser knyttet til cyberangrep. Fra sikkerhetssjefen så ble det sagt at alle hendelser som anses å være uønskede skal rapporteres. *«De hendelsene som blir rapportert her internt er som regel hendelser som kan ha en fremtidig konsekvens»* ble sagt av konsernbanksjefen IT-drift, hvor han senere la til: *«Vi rapporterer nok ikke hendelser som ikke har medført en feil, hvis risikoen tilstede er lav, eller hvis det ikke er noen tiltak som må iverksettes for å hindre at det skjer igjen».* Videre i intervjuet ble det også fortalt at det er to ulike praksiser som brukes i forhold til rapportering, den ene internt i SpareBank 1 SR-Bank og den andre eksternt til finanstilsynet. Den sistnevnte praksisen er lovpålagt hvor banken må rapportere dersom det er avvik knyttet til kunden sine tjenester. Dette må enten skje umiddelbart hvis hendelsen er av en viss størrelse, men regelmessig skjer denne rapporteringen én gang i måneden.

Neste spørsmål hadde fokus på evaluering av rapporterte hendelser, og om dette blir vektlagt i SpareBank 1 SR-Bank. *«Ja, alle hendelser som blir rapportert skal bli behandlet. Rapporteringene går til en gruppe for behandling som er delt inn i forskjellige områder»* sa sikkerhetssjefen. Konsernbanksjefen IT-drift kan sies å være enig hvor han sa: *«Ja, alle hendelser som blir rapportert eies av «Risk and compliance avdelingen», så de følger opp og rapporterer videre til styret. Ikke konkret på hver enkelt sak, men på volum og generell rapportering».* Han la til at dette er noe som har blitt vektlagt de siste årene, da det for en stund tilbake var litt svakere evaluering enn nå.

Det siste spørsmålet i intervjuene med konsernbanksjefen IT-drift og sikkerhetssjefen var om det var fokus på kurs og videre opplæring i forhold til sikkerhet i SpareBank SR-Bank. *«Vi har opplæring med alle ansatte når de begynner. Én times lang opplæring hvor vi går gjennom og ser på hvordan vi jobber med informasjonssikkerhet, hvilke kontroller vi har på plass og hvordan de ansatte skal behandle sensitiv informasjon»* sa sikkerhetssjefen før han la til at utover dette er det fokus på de månedlige kursene som blir sendt ut på e-mail til alle ansatte. Dette ble også nevnt av konsernbanksjef IT-drift hvor han la til at dette gikk ut på kompetanseheving knyttet til sikkerhet, og at de blir sendt ut mellom ti til tolv ganger i løpet av ett år. Ved å bruke disse månedlige kursene så skal alle de ansatte være beredt på hendelser knyttet til informasjonssikkerhet.

Hovedfunn intervju med ledelsen, gruppe 2

Tabell 7: Intervju av ledelsen, gruppe 2

Hovedfunn intervju med ledelsen, gruppe 2	
Evnen til å respondere	• SpareBank 1 SR-Bank bruker en generell beredskapsplan som er publisert og lett tilgjengelig for de som er ansvarlige for respons. • Gjennom IRT så har SpareBank 1 SR-Bank kontinuerlig ansatte på jobb som har kompetanse til å kunne håndtere et eventuelt cyberangrep. I tillegg så har banken på dagtid en IT-drift-avdeling som jobber med denne type håndtering. • SpareBank 1 SR-Bank jobber med å ha så kort responstid som mulig, og har etter erfaringer klart å komme raskt tilbake til normaltilstanden etter både DDoS-angrep og kryptoangrep. • Kundene kontaktes av kundesenteret umiddelbart dersom cyberangrep er knyttet direkte til dem. Kundene blir også kontaktet dersom et angrep skjer på banken, og dette skal skje så snart banken har fått oversikt. • Gjennom utkontrakteringsavtaler så sikres det at systemene SpareBank 1 SR-Bank bruker er kontinuerlig oppdaterte og intakte. Testing av systemene skjer ved produksjonstesting og deretter årlig.
Evnen til å overvåke	• Det er en 24/7 funksjon for overvåkning i SpareBank SR-Bank gjennom IRT. I tillegg er det interne overvåkningsfunksjoner som fokuserer på systemer med kundeinformasjon. • SpareBank 1 SR-Bank er inne i en periode med transformasjon fra en tradisjonell sikkerhetsmodell til en dynamisk sikkerhetsmodell. • Ved å bruke utkontrakteringsavtaler så får SpareBank 1 SR-Bank informasjon om trusler i miljøet knyttet til cyberangrep. • Ved å ha et generelt beredskapsplanverk så er alle de ansatte beredt dersom en uønsket hendelse oppstår. Policyer, standarder og retningslinjer blir endret hvis og når det er behov for det. • De ansatte får jevne drypp av hvilke trusler som banken står ovenfor gjennom å utføre månedlige kurs.
Evnen til å forutse	• Det blir foretatt en trusselvurdering i SpareBank 1 gruppen halvårlig, mens i SpareBank 1 SR-Bank blir den foretatt årlig. • Risiko- og sårbarhetsanalysen blir gjennomført én gang i året ved bruk av en risikomatrise basert på seks dimensjoner. • Tiltak implementeres på aktiviteter hvor risikoen er å anses for å være for høy. • Risikovurderingen blir vurdert ut fra tre faktorer: tilgjengelighet, integritet og konfidensialitet.
Evnen til læring	• Alle hendelser som anses for å være uønskede skal rapporteres i SpareBank SR-Bank. • Rapportering foregår internt i SpareBank 1 SR-Bank, i tillegg til eksternt til finanstilsynet. • Alle hendelser som blir rapportert internt i SpareBank SR-Bank skal bli evaluert av en avdeling som er ansvarlig for dette. • En grundig opplæring knyttet til informasjonssikkerhet blir gjennomført med alle nye ansatte. Opplæring og kurs utover det blir gjennomført via månedlige kurs sendt på e-mail.

6. Analyse

Fokuset i denne delen av oppgaven er å finne svar på oppgavens to forskningsspørsmål via en analyse av empirisk funn sett fra oppgavens teoretiske grunnlag.

6.1 Hva kjennetegner en resilient cybersikkerhetskultur i bank?

Teknologisk og digital utvikling i banknæringen har resultert i et paradigmeskifte når det gjelder fokus på sikkerhet. Dette skiftet har bidratt til å intensivere fokuset på sikkerhet, ikke bare innad i organisasjoner, men også utad til befolkningen. I henhold til denne endringstakten så kommer det frem i intervjuene med flere informanter at sikkerhetskultur blir vektlagt i SpareBank 1 SR-Bank. For å vise til dette så er det hensiktsmessig å vurdere sikkerhetskulturen ut ifra en informert kultur som det ble redegjort for i teorikapittelet i oppgaven. Sikkerhetskultur i henhold til teorien fra James Reason (1997, s. 192) handler om en informert kultur som er basert på en rettferdig kultur, en rapporterende kultur, en fleksibel kultur og en lærende kultur.

Det første som må bli diskutert for å vurdere sikkerhetskulturen i en organisasjon, er å redegjøre for om det foreligger samsvar i hva som betegnes som sikkerhetskultur. Slik som den empiriske datainnsamlingen viste i forhold til intervjuene med de ansatte i SpareBank 1 SR-Bank, så innebærer en sikkerhetskultur at det er fokus på opplæring, informasjon, kunnskap og bevissthet, og at aktiviteter i banken skal være i henhold til organisasjonens retningslinjer. Gjennom intervjuene med informanter fra ledelsen i SpareBank 1 SR-Bank, så er kritisk sans, opplæring, kjennskap til retningslinjer og et dynamisk forhold til risikobildet viktige faktorer i en sikkerhetskultur. Til tross for at de ulike informantene fra de to forskjellige gruppene ikke er helt like, så er det likevel enighet i hva som bør være implementert i en organisasjon for at det skal være en sikkerhetskultur. Samtidig ville det også vært fordelaktig dersom alle i organisasjonen hadde hatt lik oppfatning om hva som er sikkerhetskultur, da dette kunne tydet på at sikkerhetskultur ble vektlagt ytterligere.

En rettferdig kultur

I en sikkerhetskultur med fokus på rettferdighet så handler det om å implementere like retningslinjer for alle ansatte, hva som er akseptabelt og om det brukes straff som virkemiddel for å få frem ønsket atferd (Reason, 1997, s. 202-205). I intervjuene med informanter fra

ledelsen i SpareBank 1 SR-Bank kom det frem at det forelå retningslinjer for hva som var akseptabelt i henhold til deling og bruk av kunders personlige informasjon. Gjennomgående i intervjuene med de ansatte kom det ikke frem hva som var akseptert risiko, men at målet for de ansatte var å yte for at kunden skal få best mulig behandling, veiledning og beskyttelse. Imidlertid så nevnte enkelte informanter at taushetserklæringen alle i organisasjonen signerte, er et av de viktigste virkemidlene SpareBank 1 SR-Bank har. Det kom frem fra samtlige intervju at det hovedsakelig ikke ble brukt noen form for sanksjoner eller konsekvenser dersom uønskede hendelser oppstår. Fra ledelsen ble det gitt signaler om at de ønsket at ansatte skulle få lov til å gjøre feil, så lenge dette produserte videre læring og at hendelsen ikke oppsto igjen. Fra de ansatte sitt perspektiv så var det en felles forståelse for at sanksjoner og konsekvenser ikke var et resultat av uønskede hendelser. Likevel må det nevnes at i samtale med ledelsen så kom det frem at dersom en uønsket hendelse hendte på bakgrunn av at ansatte var involvert, for eksempel i et innsideangrep, så resulterte dette i konsekvenser med en eventuell oppsigelse. For at det ikke skal oppstå mistillit til ledelsen i en organisasjon som har en rettferdig sikkerhetskultur, er det tungtveiende at ledelsen er synlig og arbeider for å skape en atmosfære preget av tillit. Det var fokus på å skape tillit gjennom synlighet av ledelsen ved hjelp av tilgjengelighet og deltakelse. Fra intervjuene med ledere i henhold til spørsmål om aktivitet fra ledelsen kom det markant fram at dette var noe ledelsen prioriterte. Fra de ansatte sitt perspektiv kom det frem at ledelsen var tilstedeværende og synlige, og at de deltok i flere prosesser knyttet til sikkerhet. Samtidig var det også et ønske om at ledelsen skulle være mer synlige i en tidligere fase av en prosess. Dette har i mellomtiden trolig ikke bidratt til å gi noen form for mistillit eller uro vedrørende lederne sin rolle i organisasjonen.

En rapporterende kultur

En rapporterende kultur er elementær for å oppnå en informert kultur. Å ha en rapporterende kultur handler hovedsakelig om å rapportere uønskede hendelser for å forhindre at latente feil som etableres kan resultere i fremtidige uønskede hendelser (Reason, 1997, s. 196). I SpareBank 1 SR-Bank brukes det en database for å rapportere hendelser. Dette kan være alle slags hendelser som er knyttet til en tidligere, nåværende eller fremtidig risiko. For å få en tydelig kultur innenfor rapportering så bør det erkjennes og understrekes av ledelsen at dette er fokus. For de fleste av informantene var det klart at rapportering var viktig, men det ble også nevnt at kulturen vedrørende rapportering kunne forbedres til sammenligning med tidligere arbeidsplasser. I intervjuene med ledelsen var det selvskrevent at det var fokus på å oppmuntre ansatte til å rapportere inn uønskede hendelser. Bakgrunnen var at ledelsen ønsket

å hente inn informasjon som kunne bidra til videre læring. Flere av lederne var delaktige i å oppmuntre ansatte; både ved å forklare og vektlegge hvorfor det var nødvendig med rapportering, og hvordan rapporteringen skulle gjennomføres og registreres. Gjennom denne oppmuntringen så ønsket ledelsen å bidra til å gi ansatte oppdatert informasjon og opplæring i å håndtere den usikkerheten som er knyttet til cybernettverket i SpareBank 1 SR-Bank. Dette ønsket fra ledelsen la spor da flere av de ansatte ytret i intervjuene at de følte ledelsen bidro med oppmuntring til rapportering. Dette kan tyde på at ledelsen fremmer et fokus på sikkerhet gjennom å vise til sine ansatte at rapportering av uønskede hendelser var avgjørende for videre sikkerhet innad i organisasjonen. Ved at det er flere typer hendelser som ble rapportert og at alle de ansatte anerkjente det systemet som brukes, så kan det se ut som at det er en forståelse om at det er nødvendig å gjennomføre rapportering, både på bakgrunn av normer i kulturen og retningslinjer i organisasjonen.

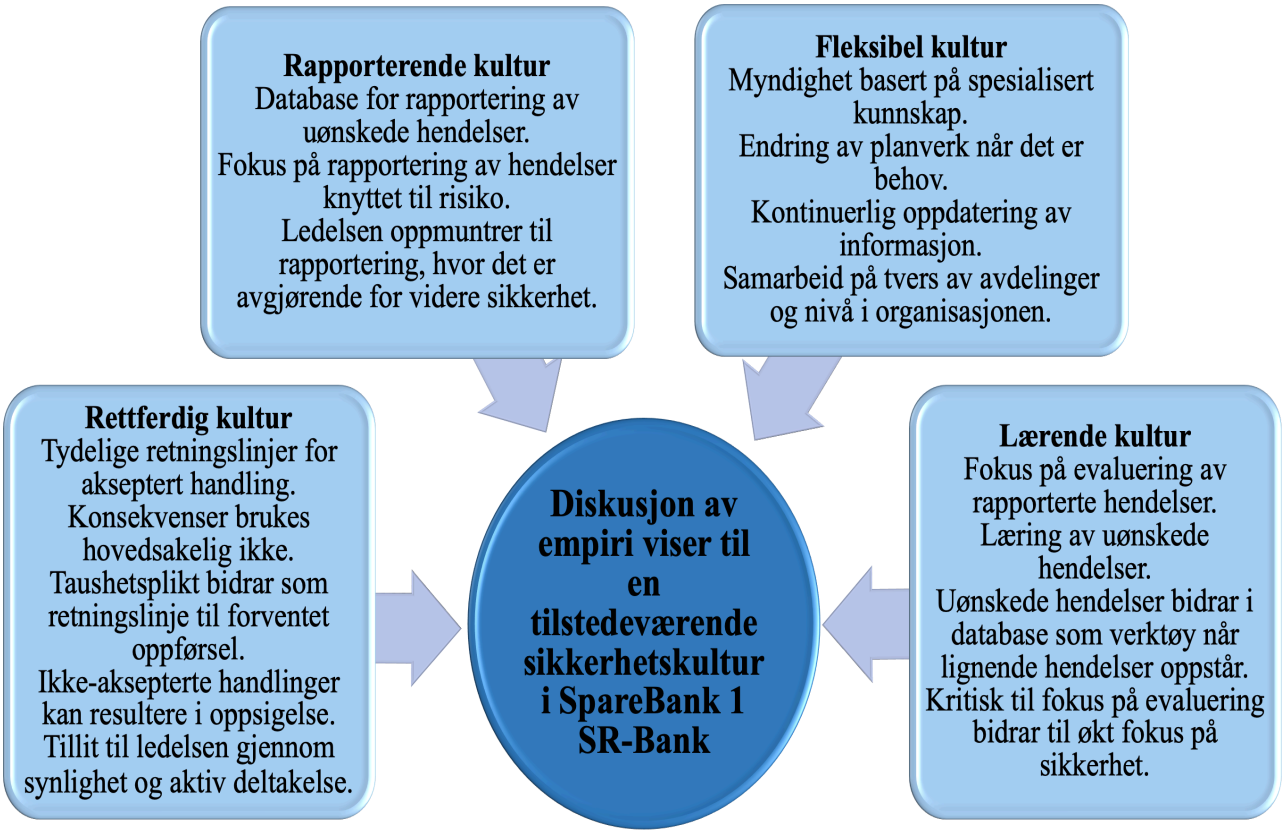
En fleksibel kultur

Å ha fleksibilitet i en organisasjon med fokus på en informert kultur, handler om håndtering av informasjon, forandringer, og autoritet og formaliteter rundt rang og roller (Reason, 1997, s. 213-217). Først og fremst har SpareBank 1 SR-Bank en klar hierarkisk struktur. Dette påvirker videre myndighet da øverste leder som regel har ansvaret for aktiviteter, hvis ikke annen delegering har blitt gjort. Innad kan det tyde på at de ønsket å ha en slik rollefordeling slik at de får spesialkunnskap på de områdene som trenger det, og de som har ansvarsmyndighet har kunnskap relatert til dette. Ved å ha spesialisering langsmed ulike avdelinger og roller så kunne alle ansatte jobbe med det de har kunnskap om. Dette kom frem i ulike intervjuer hvor myndighetsansvaret ble diskutert. Det var ulike svar fra de ansatte vedrørende om de hadde myndighet til å ta beslutninger, noe som kan forklares ut ifra informanten sin stilling og rolle i organisasjonen. Det kan dog anses å være noe negativt, da ikke alle ansatte var trygge nok i sin rolle til å ta beslutninger i krisesituasjoner. Til tross for dette så vil det ha lite betydning da hovedessensen i en fleksibel kultur er at den personen med mest kunnskap på området skal være den som tar beslutningen, hvor det da er fordelaktig at sikkerhetsavdelingen tar beslutninger knyttet til sikkerhet, noe som er standard i SpareBank 1 SR-Bank. Fleksibilitet angående endringer og forandringer skal skje fortløpende dersom organisasjonen fokuserer på en informert kultur (ibid.). I forbindelse med å ha intervjuer med ledelsen kom det frem at vurdering av beredskapsplaner, retningslinjer og analyser av risiko ble gjennomført regelmessig, noe som kan tyde på fokus på oppdatering av informasjon. Innhenting av informasjon hendte daglig, hvor bruk av eksterne leverandører var en velbrukt

ressurs og bidragsyter. En regelmessig innhenting av informasjon åpnet opp for muligheten til å aktivere forandringer ved behov, noe som var nødvendig når det gjaldt sikkerhet knyttet til cybernettverket. Ved hjelp av intervjuene kan det også vurderes at det var en kollegial autoritet hvor samarbeid på tvers av avdelinger og fagområder ble vektlagt. Denne samarbeidsviljen kan gi uttrykk for at banken er opptatt av fleksibilitet, og hvor samarbeid vil bidra positivt i henhold til bankens sikkerhetsstrategi.

En lærende kultur

I en informert kultur så er det også iboende å etablere en lærende kultur. En del av å ha en lærende kultur er evaluering av hendelser som har oppstått og videre læring (Reason, 1997, s. 218-220). Ifølge informantene varierte det i hvilken grad evaluering av hendelser ble gjennomført. Dette var et område hvor det forelå et klart forbedringspotensial, hvor enkelte ansatte ønsket at dette området skulle bli vektlagt ytterligere. Dette synspunktet ble ikke delt av lederne som ble intervjuet knyttet til sikkerhetskultur. Fra intervjuene ble det fortalt at alle hendelser som ble rapportert skal bli evaluert. Ifølge ledelsen så forelå det et åpenbart fokus på at man skal lære av de hendelsene som har oppstått. Dette kan være tegn på at det er lav kommunikasjon mellom ledelsen og de ansatte når det gjelder evaluering av hendelser, og at lærdommen ikke kommer tydelig nok frem. På grunn av at enkelte ansatte omtalte at det forelå rom for forbedring, så kan det tyde på at det eksisterer en åpenhet i banken hvor det er lov å være kritisk til hvordan ting gjøres i organisasjonen. Dette kan betraktes til å være av stor betydning for å kunne forbedre den eksisterende praksisen og videre utvikling. For at det skal foreligge en lærende kultur er det også primært at det er en fremtredende kompetent informasjonshåndtering etablert i organisasjonen (ibid.). Gjennom grundig opplæring av alle ansatte ved ansettelse og deretter månedlige opplæringskurs, så bidro dette til å forbedre informasjonshåndteringen i banken. Rapportering gjennom den nevnte databasen ~~er~~ var også et supplement til økt informasjonshåndtering da det åpnet opp for analyser og tolkning gjennom refleksjon. Som nevnt tidligere var det akseptabelt i SpareBank 1 SR-Bank å gjøre feil, så lenge det bidro til at ansatte, ledelsen og de involverte fikk en form for læringsutbytte og kompetanseheving.



Figur 22: Oppsummering av diskusjon av sikkerhetskultur

Vedrørende diskusjonen om sikkerhetskultur og SpareBank 1 SR-Bank, så kan det konkluderes med at cybersikkerhetskulturen er tydelig tilstedeværende i forhold til en informert kultur basert på teorien til Reason. På bakgrunn av å evaluere empiriske funn opp mot det teoretiske grunnlaget for sikkerhetskultur, så kan det vurderes at sikkerhetskultur er noe som blir vektlagt i banken på flere områder. Til tross for dette, så eksisterer det et forbedringsområde, noe som er tenkelig da en perfekt sikkerhetskultur kan hevdes å være uoppnåelig. For å kunne oppnå en resilient cybersikkerhetskultur må det foreligge rammer for henhold til de evnen til å lære, forutse, overvåke og respondere. Dette ble fremstilt i figur 9, og denne figuren skal bli brukt videre i drøftingen for å vise hvordan SpareBank 1 SR-Bank er i forhold til sikkerhetskultur og RE.

Ved å ha en etablert cybersikkerhetskultur, noe som viste seg å være allestedsnærværende i SpareBank 1 SR-Bank, så kan det konkluderes med at rammene er tilstedeværende da empiriske funn fra flere nivåer i organisasjonen kan sies å være valide. En del av datainnsamlingen inneholdt en dokumentanalyse av rapporten til BCBS om cyberresilience. I denne rapporten kom aktualiteten ved å implementere en strategi for sikkerhetsstyring i henhold til sårbarheten knyttet til cyberangrep tydelig frem. Gjennomgående i rapporten blir

det presentert vurderinger som bør være anerkjent i banker for å gjøre det mulig for dem å være motstandsdyktige mot dagens trusselnivå. De faktorene som blir nevnt i rapporten er knyttet til strategi, ledelse og ansvar, kultur og arkitektur. Majoriteten av disse faktorene er gjeldende i teorien om RE til Erik Hollnagel (2015; 2011), og på bakgrunn av dette så vil faktorene bli diskutert i sammenheng med drøftingen av SpareBank 1 SR-Bank sin evne til motstandsdyktighet. Cybersikkerhetskultur ble diskutert ovenfor hvor drøftingen bidro til muligheten ved å konkludere med at SpareBank 1 SR-Bank har en tilstedeværende sikkerhetskultur. Denne konklusjonen tilsier at banken følger anbefalingene til BCBS men hensyn til etableringen av en fremtredende sikkerhetskultur.

Et fremtredende aspekt innenfor teori om sikkerhet og sikkerhetsstyring i forhold til angrep gjennom cybernettverket, handler om at uønskede hendelser ikke er uunngåelige, og at en nullvisjon kan sies å være urealistisk. Det er ikke mulig å fjerne all risiko når cybernettverket brukes, hvor teknologien ikke legger til rette for det. Teknologien og digitaliseringen har ført til høy kompleksitet, og dagens trusler kan ikke lenger stoppes av barrierer. For å kunne være motstandsdyktig ved bruk av cybernettverket er det derfor essensielt å skape et relevant og etablert kunnskapsgrunnlag (Hollnagel, 2016). På bakgrunn av dette er det viktigere å ha en forståelse om at uønskede hendelser vil oppstå, og at de som er ansvarlige for sikkerheten bør implementere pålitelige rutiner for hvordan man skal minimere sårbarheten og strebe for å redusere responstiden når en uønsket hendelse oppstår. Gjennom en observasjon tatt ut ifra de intervjuene som har blitt gjennomført i SpareBank 1 SR-Bank, kan det forstås at banken arbeider for dette. Banken har egne avdelinger som overvåker aktiviteter for å oppdage uønskede hendelser så tidlig som mulig, samtidig som de har ansatte med kunnskap om hvordan de skal håndtere uønskede hendelser. En utfordring som kan oppstå i organisasjoner som blir utfordret av trusler gjennom cybernettverket, er mangel på kunnskap og informasjon. For å kunne håndtere, forutse eller forhindre en uønsket hendelse så må en organisasjon ha kunnskap om hendelsen, noe som ofte kan være vanskelig for hendelser gjennom cybernettverket. Årsaken til dette er at det er kontinuerlig forandring i metoder som brukes, noe som innebærer at organisasjonen stadig må endre sine forsvarsbarrierer.

Ved at SpareBank 1 SR-Bank bruker eksterne leverandører gjennom utkontrakteringsavtaler så brukes det spesialkunnskap for å observere miljøet og hente inn relevant kunnskap som blir levert til ledelsen i sikkerhetsavdelingen. Den innhentede informasjonen kan bidra til at banken får mulighet til å oppdatere sine brannmurer og deteksjonssystemer, som kan hjelpe

med å forhindre cyberangrep. Da det er raske endringer i metodebruk, så vurderes det som avgjørende at sikkerhetssjefen i SpareBank 1 SR-Bank sjekker ny informasjon de får fra leverandører daglig. Dette er primært hvor det ikke bare viser ledelsen sitt fokus på området, men også at det bidrar til å sikre bankens informasjon og systemer. Den daglige sikkerhetskulturen og synet på sikkerhetsstyring som er eksisterende i SpareBank 1 SR-Bank, blir stadig utfordret av den digitaliserte epoken vi nå er inne i. Den tradisjonelle måten å vurdere risiko og sårbarheter på er under utvikling, hvor fokuset ikke lenger kun handler om å se på hva som er uønsket drift. Et nytt og moderne perspektiv på risiko er nødvendig, og kravet om et mer dynamisk syn på risiko er høyst nødvendig. Årsaken til dette er at tradisjonelle metoder for sikkerhetsstyring ikke lenger er like effektive hvor kompleksiteten har økt og nye sårbarheter har oppstått. Dette er grunnlaget for teorien til Hollnagel da han etablerte et skifte på syn på risiko fra safety-I til safety-II. Hans teori om RE oppmuntrer til en mer sikker håndtering av uønskede hendelser med mer dynamisk kontroll. Denne teorien er høyst tilpasningsdyktig til denne studien da SpareBank 1 SR-Bank har høy kompleksitet gjennom deres bruk av cybernettverket.

Evnen til å respondere

Den første egenskapen Hollnagel presenterer er evnen til å respondere. Denne egenskapen handler om å vite hva man skal gjøre og ha kapasitet til å gjøre det (Hollnagel, 2011, s. 284-286). For å vurdere om SpareBank 1 SR-Bank har denne egenskapen så handlet intervjuguiden til «Intervju av ledere, gruppe 2» om RE. Gjennom intervjuene kom det fram at banken var rask til å respondere på uønskede hendelser ved bruk av overvåkningsteam, kundesenter, avdeling for IT-drift og avdeling for sikkerhet. Ved gjensidig kontakt, samarbeid og kontinuerlig dialog mellom de ulike avdelingene så ble responstiden redusert. Det konstateres at SpareBank 1 SR-Bank jobbet for at responstiden skal være så kort som mulig, og de vektla fokus på å komme tilbake til normaltilstand så fort som mulig når uønskede hendelser oppstod. På bakgrunn av innsamlet empiri så kan det virke som at SpareBank 1 SR-Bank har betraktelig resiliens i øyeblikket. For å kunne ha evnen til respons er å vite om organisasjonens systemer er intakte. Slik som redegjort for tidligere så brukte SpareBank 1 SR-Bank eksterne leverandører til flere tjenester, som for eksempel systemleverandører. Testing av systemene skjer årlig og når nye systemer ble implementert. Systemene ble også testet ved reelle hendelser, noe som kan bidra til å gi banken mer informasjon om angrep, men det kan også være for sent hvor det ikke er full sikkerhet om systemet fungerer til enhver tid. I utgangspunktet vil antallet testing som SpareBank 1 SR-Bank har være nok, men ettersom

hackere stadig skifter metode for angrep og at det er gjentatte forandringer, så kan det hevdes at testingen bør skje oftere. På en annen side så er det vanskelig å teste et system for et angrep hvor man ikke har kunnskap om hvilken metode som skal brukes. På bakgrunn av dette så kan det indikere at SpareBank 1 SR-Bank har hensiktsmessige rutiner for hvordan de skal håndtere cyberangrep, da de har generelle planverk samt en hendelsesdatabase over angrep som har skjedd tidligere. Til tross for at testingen av systemene kan hevdes å være manglende, så hadde banken kontinuerlige trusselvurderinger for å få informasjon om de truslene banken står ovenfor og hvordan metoder for cyberangrep endrer utseende.

Evnen til overvåking

Den andre egenskapen som må være gjeldende i en organisasjon for å være resilient, er evnen til overvåkning (Hollnagel, 2011, s. 286). Som en del av SpareBank 1 Gruppen så har SpareBank 1 SR-Bank en egen 24/7funksjon for overvåkning gjennom IRT. I tillegg har SpareBank 1 SR-Bank andre leverandører som gir banken informasjon om trusselnivå og miljøet for sikkerhet, noe som øker og samtidig styrker banken sitt kunnskapsnivå. Denne informasjonsdelingen er-noe som gjør at SpareBank 1 SR-Bank har daglig og kontinuerlig oppdatert informasjon, vedlagt til at de har en felles delingsfunksjon med andre banker som bidrar til at banken får mulighet til å forberede seg dersom angrep skjer i andre banker. Den informasjonen som blir hentet inn evalueres og gjør det mulig at SpareBank 1 SR-Bank kan legge inn nye barrierer som deteksjoner eller brannmurer i sine overvåkningssystemer. Den informasjonen som samles inn er i hovedsak om hendelser som går galt, og ut ifra intervjuene kan det tyde på at banken fokuserte lite på hendelser hvor alt gikk bra. Dette var også toneangivende ved evaluering av egne hendelser internt i organisasjonen. Manglende fokus på hendelser som går bra kan bidra til å svekke evnen til overvåkning, da kunnskap om hendelser med positive resultater kan brukes som en pekepinn på riktig handling. På den andre siden så er evnen til overvåkning gjeldende i henhold til kunnskap. Det repeterende samarbeidet i organisasjonen på tvers av avdelinger øker fleksibiliteten, hvor sikkerhetsavdelingen får mulighet til å dele sin kunnskap om sikkerhet og håndtering av sikkerhet til andre avdelinger. Evnen til overvåkning av basisfunksjoner internt i organisasjonen har også fått økt fokus de siste årene. Gjennom intern overvåkning får sikkerhetsavdelingen muligheten til å kontrollere at informasjon ikke blir spredt eller delt, noe som ifølge flere av informantene til denne studien er svært viktig for å oppbevare tilliten til sine kunder.

Evnen til å forutse

Den tredje egenskapen som må foreligge i en organisasjon for å oppnå motstandsdyktighet i henhold til Hollnagel sin teori, er evnen til å forutse (2011, s. 286). En stor del av SpareBank 1 SR-Bank sin strategi for å oppdage mønster og aktiviteter i miljøet er gjennom samarbeid med andre banker og deres leverandørtjenester. Dette gjør det enklere for banken å etablere beredskap dersom uønskede hendelser er truende og dette gir mer tid forberedelse. Metoden for innhenting av informasjon har blitt diskutert tidligere, og denne metoden bidrar til at banken får en økt evne til å gjenkjenne endringer da de har kontinuerlig oppdatert informasjon. Kunnskapen om trusselnivået og aktiviteter knyttet til risiko åpner opp for muligheten til å forstå hva som kan skje dersom endringer i aktiviteten oppstår. Kunnskapsnivået bidrar også til å legge grunnlag for å ta øyeblikkelige avgjørelser, noe som antydes å være viktig i forhold til responstid i SpareBank 1 SR-Bank. Gjennomgående i denne drøftingsdelen så har de seks evnene i mønsteret til David Woods (2011, s. 121-125) blitt diskutert, hvor blant annet testing av systemer ble konkludert med var tilstede, men at hyppigheten var mangelfull. Videre så er det klare signaler på at SpareBank 1 SR-Bank prioriterer sikkerhet. En evne som må være tilstede for å kunne oppnå motstandsdyktighet gjennom evnen til å forutse, for å ha en evne til å identifisere risiko og følgende konsekvenser, noe som er gjeldende i SpareBank 1 SR-Bank ved årlige ROS-analyser og bruk av risikomatrise. Det må også foreligge en viss evne til å erkjenne at systemene organisasjonen bruker og de følgende metodene for sikkerhet ikke alltid er perfekte; noe som kan anses å være nødvendig for å kunne opprettholde høyt fokus på sikkerhet. Ut ifra intervjuene med informanter med kunnskap om RE i SpareBank 1 SR-Bank så kan det være tegn på at dette er utbredt da begge informantene i ulike bisetninger nevnte at det var rom for forbedring. Dette tyder på at det er et uavbrutt jag etter å gjøre sikkerheten i organisasjonen så resilient som mulig.

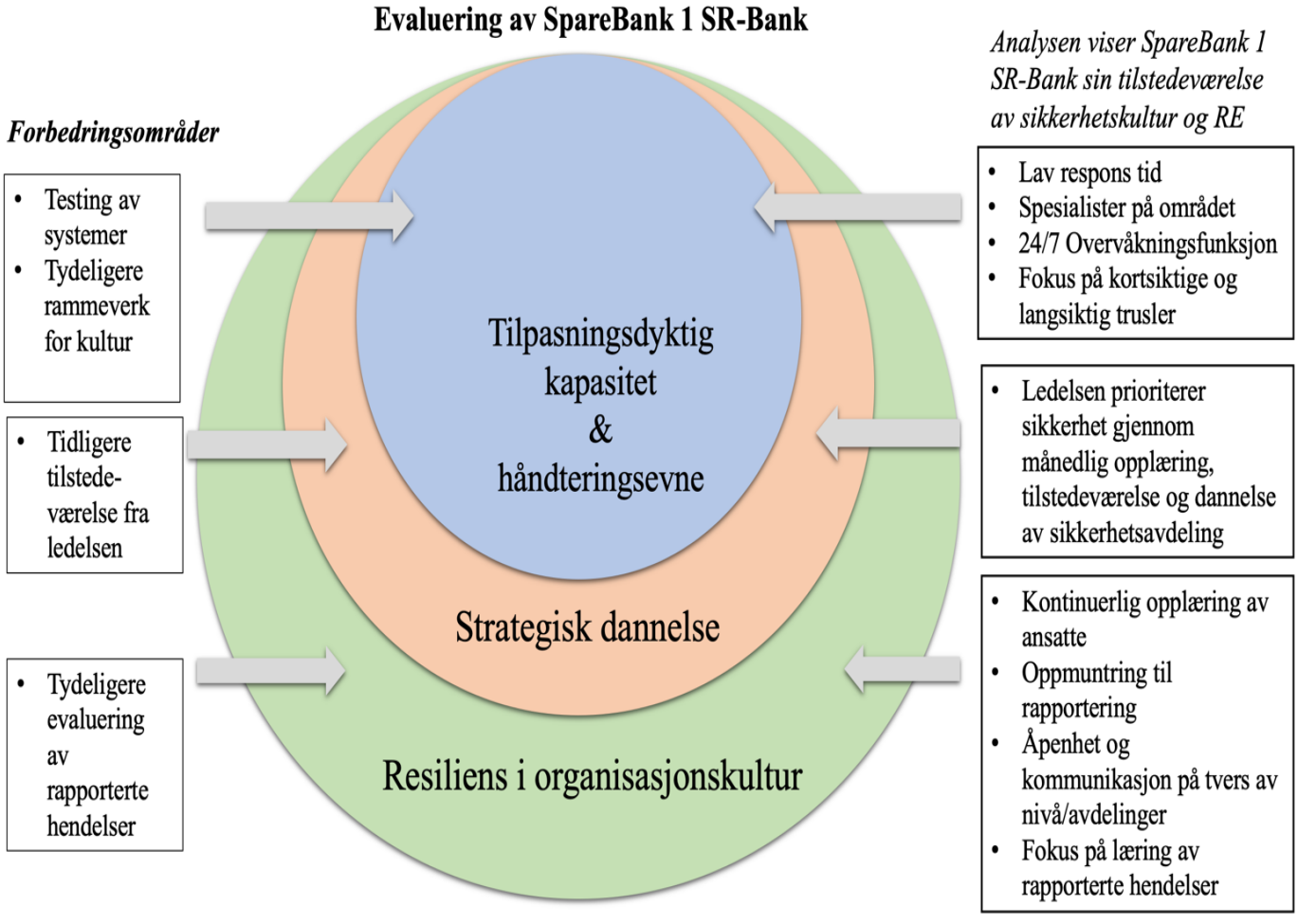
Evnen til læring

Den siste egenskapen som er grunnleggende for en resilient organisasjon er evnen til læring. Det handler om å ha kunnskap om hva som har oppstått og det som faktisk har skjedd (Hollnagel, 2011, s. 287). Først og fremst er SpareBank 1 SR-Bank en aktiv organisasjon med høy aktivitet, noe som åpner opp for at rammene for læring er tilstede. Ved at SpareBank 1 SR-Bank har implementert en database for rapportering av hendelser, så har dette bidratt til at sikkerhetsavdelingen får mulighet til å evaluere hendelser som har en betydning for risikoen og sikkerheten i banken. Gjennomgående i flere av intervjuene, og ikke bare de to intervjuene

som var relevante for denne delen av studien, så ble det vektlagt at det var fokus på rapportering og at denne rapporteringen var et verktøy for videre læring. I forbindelse med økt kunnskap så kan det tyde på at organisasjonen har evnen til å tilpasse seg endringer, hvor utvidelsen av sikkerhetsavdelingen og økt fokus på sikkerhet er klart fremtredende. Denne tilpasningen kan også hevdes å være tilstede på bakgrunn av at banken hadde etablert gode rutiner for sikkerhet og kommunikasjon når det gjaldt nye lovgivninger og retningslinjer. Videre var også fokus på læring via økt kunnskap og opplæring vektlagt i SpareBank 1 SR-Bank gjennom deres månedlige opplæringskurs. Disse kursene fokuserer på saker som er dagsaktuelle og det handler om den aktiviteten som skjer i miljøet som de ansatte arbeider i.

Konklusjon forskningsspørsmål 1

RE er en måte å drive sikkerhetsstyring på, men i motsetning til andre styringsstrategier så er ikke RE noe man har, det er noe man kontinuerlig streber etter (Hollnagel, 2016). Ved å evaluere empiriske data samlet inn fra intervjuer med informanter med antatt spesialkunnskap på området, har det blitt mulig å vurdere SpareBank 1 SR-Bank sin tilnærming til RE.



Figur 23: Evaluering av sikkerhetskultur og RE

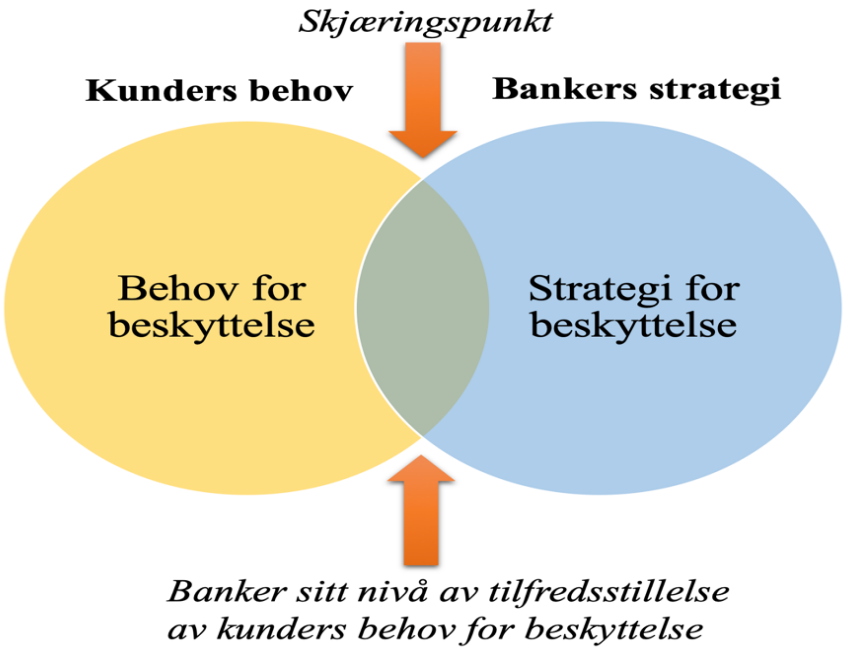
Gjennomgående i drøftingen av informasjonen fra intervjuene knyttet opp mot de fire ulike egenskapene til Hollnagel, så kan det indikere at banken på flere ulike måter jobber for å få så sterk motstandsdyktighet som mulig. Til tross for enkelte mangler eller svakheter, så kan det likevel konkluderes med at banken som helhet har en sikkerhetsstrategi som på flere områder er i henhold til Hollnagel sin teori om RE. Som tidligere nevnt så foreligger det en sikkerhetskultur i SpareBank 1 SR-Bank, noe som legger grunnlag for rammer for å oppnå RE. Figur 23 viser til hvordan RE og sikkerhetskultur blir evaluert i henhold til teori om at sikkerhetskultur skal skape rammer for motstandsdyktighet (Steen, 2019).

Ved at banken har både en sikkerhetskultur og en RE så kan det hevdes at det er fokus på sikkerhet. SpareBank 1 SR-Bank tilfredsstiller også anbefalingene til det som blir presentert i rapporten til BCBS for hvordan man skal etablere cyberresilience i banknæringen. Hovedkravet som presenteres i rapporten handlet om å implementere en strategi for sikkerhet, noe som kan knyttes til datainnsamlingen og videre drøfting kan argumenteres for at er eksisterende i SpareBank 1 SR-Bank.

Den teknologiske utviklingen og digitaliseringen som er i stadig forandring utfordrer både strategier for sikkerhet og sikkerhetskultur i organisasjoner. For å kunne ha en resilient cybersikkerhetskultur i en organisasjon er det derfor flere elementer som ble nevnt gjennomgående i drøftingen som må være tilstede (Leveson, 2016). Disse elementene er hovedsakelig å ha en cybersikkerhetskultur som danner rammer for å jobbe for å etablere en motstandsdyktighet i organisasjonen, noe SpareBank 1 SR-Bank har gjennom en analyse av teori og empiri vist seg å være et eksempel på, slik figur 22 viser. Nye hendelser oppstår ved bruk av nye metoder, som gjør at de tradisjonelle metodene for sikkerhet ikke lenger er kapable til å håndtere dagens risikonivå (ibid.). For å kunne opprettholde sikker drift så blir det derfor viktig å etablere nye rutiner for å håndtere den forandringen organisasjonen står ovenfor (Hollnagel, 2015, s. 1). I SpareBank 1 SR-Bank foregår det en etablering av en ny driftsmodell med et nytt dynamisk syn på risiko. Banken ønsker å skifte fokus som er i tråd med safety-II perspektivet (Hollnagel, 2016), hvor de ønsker å se på hva som er normal drift og ikke bare hva som er uønsket drift. Dette paradigmeskiftet oppmuntrer til en mer sikker håndtering av kompleksiteten i systemene som banken bruker, hvor mer moderne og utviklede barrierer vil bidra til å redusere sårbarheten i organisasjonen.

6.2 På hvilken måte kan banker arbeide for å imøtekomme kundenes interesser i forhold til behov for beskyttelse?

Det er vanskelig å legge skjul på at norske banker er noen av de virksomhetene i Norge som har betydelige trusler mot seg knyttet til cyberangrep. Anerkjente internasjonale og nasjonale aktører som WEF, Basel, NSM og Finanstilsynet uttrykker viktigheten av å skape gode sikkerhetsrutiner for cybersikkerhet i banknæringen. Årsaken til dette er trolig den stadige utviklingen av digitale tjenester som skal videreutvikle banktjenester for å gjøre dem enklere og mer effektive for bankene sine kunder. Den digitaliserte utviklingen resulterer i økt sårbarhet, noe som har blitt nevnt tidligere i denne oppgaven, da kompleksitet og bruk av cybernettverk krever regelmessig oppfølging og håndtering. Tradisjonelt sett så har norske banker høy tillit fra befolkningen, noe som trolig kan være på grunn av norske banker sin håndtering av finanskrisen, i tillegg til et tilfredsstillende omdømme i medier. Det kan også antagelig være på grunn av lave tall på cyberangrep hvor kunder mister penger, eller lav forekomst av uønskede hendelser som gjør at kunden mister tilliten til sin bank. Til tross for at det er risikabelt at kunder deler all sin personlige informasjon til en bank, så kan det gis uttrykk for at denne risikoen anses å være akseptert. Denne risikokompensasjonen kan hevdes å være begrunnet av høy tillit og gjerne litt naivitet. Flere norske banker er avhengig av sine kunder, og dersom kunder er misfornøyde så kan dette føre til at banken mister kunder. I den sammenheng er det interessant å vurdere hva den norske befolkningen faktisk ønsker og hvilke behov de har i forhold til sin bank knyttet til cyberangrep. Gjennom å drøfte to ulike deler av den empiriske datainnsamlingen, så skal det være mulig å vurdere om SpareBank 1 SR-Bank dekker de behovene som respondentene i spørreundersøkelsen har for beskyttelse med tanke på cyberangrep. Resultatet av analysen vil bli vurdert i forhold til figur 24 som vises nedenfor. Denne figuren tar for seg skjæringspunktet mellom bankkunder sine behov for beskyttelse og SpareBank 1 SR-Bank som norsk bank sin strategi. Samsvaret mellom behov og strategi vil vurderes ved å drøfte datainnsamlingen fra spørreundersøkelsen og intervjuene i SpareBank 1 SR-Bank.



Figur 24: Bankers nivå av tilfredsstillelse av kunders behov

Tillit og kommunikasjon

Gode tillitsforhold mellom bank og kunde er grunnleggende for å kunne lykkes ved bruk av ny teknologi. For at en bank skal kunne få utbytte av ny teknologi, så er det viktig at kundene har tillit til at banken implementerer nye forandringer hvor dette er i kundenes beste interesse. En strategi som SpareBank 1 SR-Bank følger er at deres kunder i utgangspunktet ikke har nok kompetanse eller kapasitet til å være oppdatert på den raske endringen som foregår når det gjelder den teknologiske utviklingen og digitaliseringen. Derfor så har SpareBank 1 SR-Bank implementert strengere krav til sine ansatte knyttet til økt informasjon om cyberangrep og retningslinjer om personvern, noe som skal bidra til å opprettholde tillitsforholdet som allerede foreligger mellom bank og kunde. Gjennom spørreundersøkelsen så kan tilliten til bank vurderes ut fra to spørsmål hvor det ene er knyttet til nye lovgivninger og det andre er knyttet til innsideangrep. En antakelse i denne spørreundersøkelsen var å se på om alder og kjønn hadde noen innflytelse på nivå av tillit i henhold til nevnte risikoer. Resultatene viser at alder har påvirkning der høy alder viser til større tillit og at tillitsforholdet blir mer påvirket dersom banken de bruker misbruker denne tilliten. Dette kan trolig være knyttet til erfaring, hvor eldre kunder ofte har vært kunder i samme bank over tid uten at det har oppstått noe som kan være tillitsvekkende. At yngre respondenter er mer kritiske til bank kan hevdes å påvirkes av media, og på grunn av deres hyppige endrede kundeforhold knyttet til deres ønske om å ha åpne muligheter. I tillegg til at alder påvirker tillitsforholdet, viste resultatene også at de kvinnelige respondentene var mer skeptiske enn menn når det gjaldt tillit til banken sin.

Videre i henhold til spørreundersøkelsen ble det undersøkt om respondentene sitt tillitsforhold til banken ble påvirket på bakgrunn av at risikoen knyttet til personvern hadde økt, og da gjennom nye implementerte europeiske lovgivninger. Resultatene viste på tross av den nevnte risikoen at halvparten av respondentene likevel hadde nokså høy eller høy tillit til banken. Det var også kun 3 % som ikke hadde noe tillit i det hele tatt, og 34 % hadde tillit, men disse respondentene var blitt mer skeptiske i henhold til nye lovgivninger og mulighet for feilaktig deling av informasjon.

SpareBank 1 SR-Bank sine gode rutiner for intern overvåkning, kan indikere at banken er opptatt av at informasjon ikke skal komme på avveie. I tillegg kom det frem i flere av intervjuene med ulike informanter at kundenes beste var hovedfokuset, og at det ble alvorlige konsekvenser for ansatte dersom brudd på regler knyttet til kunden sitt personvern ble brutt. Det kan dermed hevdes at SpareBank 1 SR-Bank arbeider for å tilfredsstille bankkunder sine behov for beskyttelse når det gjelder kunden sin personlige informasjon knyttet til nye lovgivninger. Det samme kan også sies når det gjelder resultatene fra spørreundersøkelsen knyttet til tillit ved innsideangrep. På spørsmålet om respondentene blir påvirket av risikoen knyttet til at banken sine ansatte kan utføre innsideangrep, var det 48,2 % som svarte at dette ville få stor påvirkning i tillitsforholdet til deres bank. Gjennom den empiriske innsamlingen fra intervjuer med ledere i SpareBank 1 SR-Bank, så kom det fram at innsideangrep er noe som ble tatt alvorlig, og av den grunn hadde banken overvåkning av aktiviteten til sine ansatte. Det var også strenge retningslinjer for hvem som skulle ha tilgang til kundenes personlige informasjon, i tillegg til at det ble registrert med et ID-nummer hver gang noen sjekket kunder sin personlige informasjon. På denne måten arbeider banken for både å redusere sårbarheten for innsideangrep, samtidig som det gir dem mulighet til å forsikre seg om at personlig informasjon ikke blir misbrukt. Ved begge disse to spørsmålene som har blitt drøftet, så er det også grunnleggende med en sikkerhetskultur i banken for å kunne opprettholde tillitsforholdet. Cybersikkerhetskulturen som viste seg å være tilstede i SpareBank 1 SR-Bank kan brukes som et av de viktigste argumentene for at organisasjonen prioriterer kundene og deres interesser. Kulturen i banken åpner ikke opp for at det er sosialt akseptert eller lovlig å bryte de retningslinjene og prosedyrene som foreligger for personvern, både når det gjelder intern og ekstern deling. Ved at SpareBank 1 SR-Bank har en tilstedeværende cybersikkerhetskultur og intern overvåkning, så kan det virke som om at banken prioriterer sine kunder og deres interesser i forhold til behov for beskyttelse i henhold til deling av informasjon og innsideangrep.

Cyberangrep og ansvarsfordeling

En vanskelig utfordring norske banker står overfor i dag når det gjelder cyberangrep, er ansvarsfordelingen ved eventuelle angrep og tilhørende konsekvenser for kunden. I spørreundersøkelsen som ble gjennomført svarte 99,7 % av alle respondentene at banken har ansvar dersom kunden sin personlige informasjon og penger blir misbrukt eller stjålet. Den største andelen (67,3 %) svarte også at banken var fullt ansvarlig. Spørsmålet var basert på alle angrep som ville resultere i de nevnte konsekvensene, da det ikke ble nevnt om kunden var involvert i angrepet eller ikke. Det faktum at et så høyt antall av respondentene svarte at banken var ansvarlig var forventet da det kan hevdes at banken skal beskytte kunden sin informasjon og penger. Gjennom intervjuene med informantene fra SpareBank 1 SR-Bank så viste det seg at denne ansvarsfordelingen ikke er like enkel som respondentene skulle ønsket. Banken sitt ansvar ved cyberangrep er basert på bakgrunn av hvilken type angrep som har oppstått, samtidig som at kunden sin involvering vil være avgjørende. På tross at det ikke forelå et opplagt samsvar mellom respondentene i spørreundersøkelsen og den informasjonen som kom frem gjennom intervjuene, så er det ikke dette nødvendigvis negativt. Det kan virke som om at det ikke er tilstrekkelig kommunikasjon mellom bank og kunde angående kunden sitt ansvar når det gjelder deres bankID og personlige passord. Det at kunden ikke har nok informasjon om dette kan forbedres, slik at kunden er klar over at de er ansvarlige for eventuelle tap dersom de er involvert i misbruk av sin bankID. I henhold til den informasjonen informantene fra SpareBank 1 SR-Bank delte så burde ikke dette være nødvendig da det er åpenbart at man ikke bør dele personlige passord. Denne tilnærmingen kan hevdes å være litt streng da det bør legges til grunn at kunder ikke nødvendigvis har den kunnskapen og kapasiteten som er grunnleggende for å forstå hvordan slike hackerangrep foregår. Ett tiltak som imidlertid skal implementeres er en ny lov som skal klargjøre dette skillet mellom hvem som er ansvarlig for gjenopprettelse etter eventuelle cyberangrep. Dette vil trolig bidra til å øke fokuset slik at kundene er bevisste sitt personlige ansvar.

Kommunikasjon om hackerangrep

For å etablere et godt tillitsforhold så er kommunikasjon et viktig verktøy. For å vurdere om Sparebank 1 SR-Bank tilfredsstiller bankkunder sine behov for kommunikasjon, så ble det stilt et spørsmål i spørreundersøkelsen som var knyttet til kommunikasjon vedrørende informasjon om cyberangrep. Resultatet fra spørreundersøkelsen viste at det var en jevn fordeling på respondentene om de ønsket mer informasjon fra sin bank om hackerangrep og da spesielt om misbruk av bankID. Majoriteten av respondentene ønsket mer informasjon enn

det de har fått i dag, og i hovedsak skulle denne informasjonen blitt kommunisert gjennom e-mail. Dette behovet samsvarer ikke med metoder som SpareBank 1 SR-Bank bruker for kommunikasjon ut til sine kunder. De bruker hovedsakelig sin nettside og sosiale medier som kommunikasjonsmedium. Det vil derfor kunne hevdes å være motstridende til det som var behovet for respondentene i spørreundersøkelsen, noe som gjør at det vil foreligge et forbedringspotensial til SpareBank 1 SR-Bank på dette området. På en annen side så kom det frem gjennom intervjuene at bankens ansatte stadig fikk opplæring i hvordan de skal håndtere sine kunders behov for informasjon vedrørende cyberangrep, og da hovedsakelig dersom kunden selv tar kontakt med banken. Denne opplæringen gjør det mulig for de ansatte å gi informasjon om cyberangrep til sine kunder, så lenge kunden selv ønsker det. I og med at resultatene ikke viste at 100 % av respondentene både ønsket mer informasjon og at det ikke var samstemmighet i hvilken metode som skulle brukes, så kan dette bety at selv om bankkunder ikke får informasjon gjennom kurs og e-mail, så foreligger det likevel en plan for kommunikasjon om informasjon vedrørende cyberangrep. Denne planen inneholder også retningslinjer for hvordan banken skal kommunisere med sine kunder dersom et cyberangrep pågår eller har oppstått.

I intervjuene med informantene i SpareBank 1 SR-Bank så kom det frem at det forelå en utviklet strategi for hvordan banken skal kontakte sine kunder dersom et cyberangrep har oppstått og dette har medført konsekvenser for kunden, i tillegg til hvordan kunden skal bli kontaktet dersom banken har overvåket at det pågår aktiviteter som vurderes å være mistenksomme eller unormale. I spørreundersøkelsen ble det stilt et spørsmål vedrørende om respondenten ønsket å bli kontaktet, og eventuelt hvilken metode banken skulle bruke til å kontakte dem dersom det blir observert unormal aktivitet. Resultatene som ble presentert i kapittelet om empirisk datainnsamling viste at 61,1 % av respondentene ønsket å bli kontaktet av banken sin umiddelbart og at kontakten skulle være via telefon. Dette samsvarer med hvordan SpareBank 1 SR-Bank håndterer slike situasjoner, noe som gjør at banken oppfyller store deler av sine respondenter sitt behov knyttet til denne type kommunikasjon.

Informasjon om hackerangrep

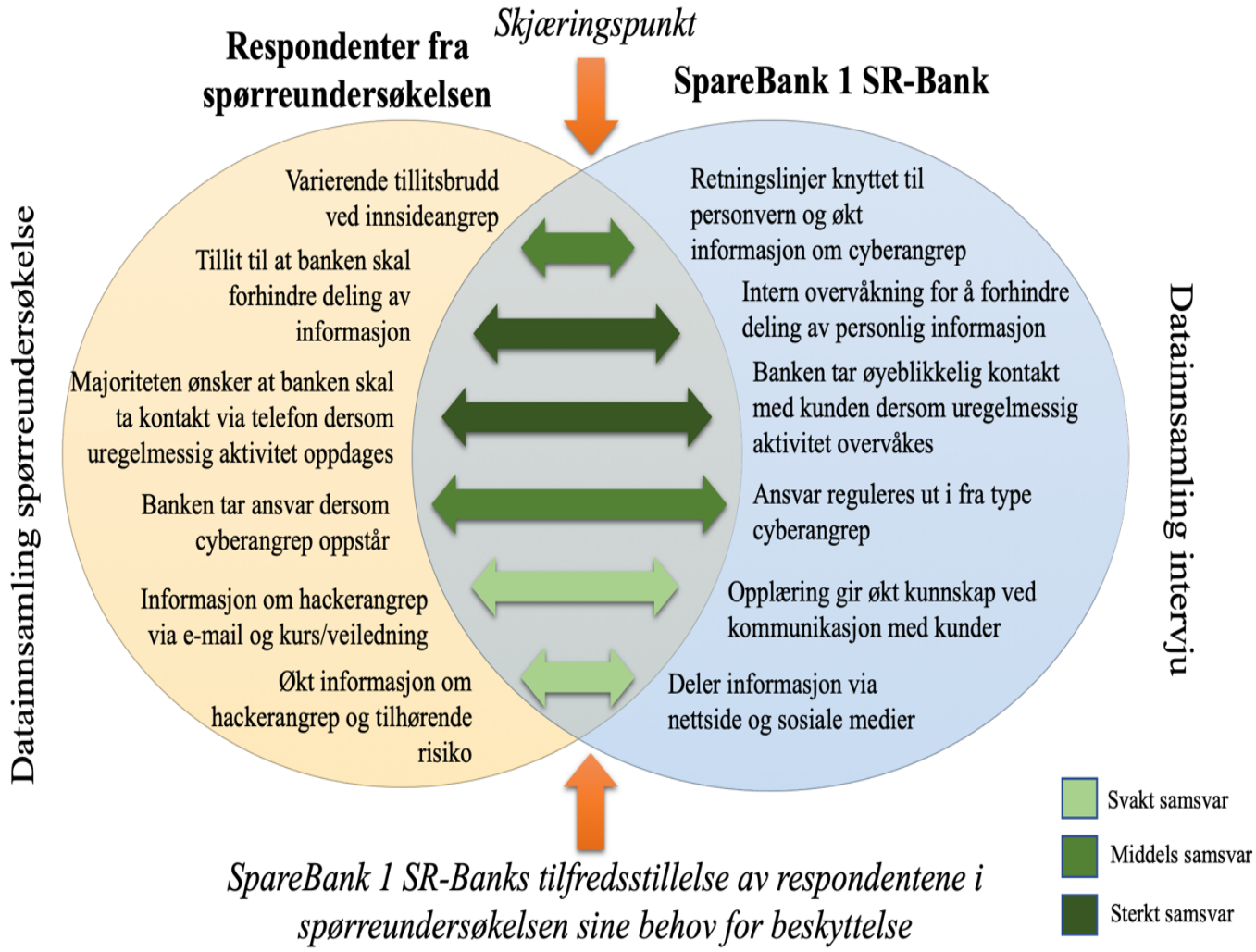
Det siste spørsmålet som ble stilt i spørreundersøkelsen var om hvorvidt respondenten har blitt informert om risikoen for å bli hacket, og eventuelt hvilke metoder av hackerangrep som ble nevnt av banken. Resultatene fra spørreundersøkelsen viste at 81,8 % av respondentene har blitt informert om denne risikoen fra sin bank. Dette resultatet kan være tegn på at det er

en henholdsvis svak risikokommunikasjon fra norske banker, da tallet på respondenter som ikke var blitt informert om slike angrep var nokså høyt. I intervjuene med informantene fra SpareBank 1 SR-Bank så kom det frem at de brukte sin nettside som kommunikasjonskanal og at det eventuelt ble lagt inn informasjon ved innlogging til mobilbank og nettbank. Ettersom resultatene fra spørreundersøkelsen viste at et såpass høyt antall av respondentene ikke hadde blitt informert om faren for hackerangrep, så kan det indikeres at SpareBank 1 SR-Bank sin strategi for kommunikasjon når det gjelder hackerangrep er for svak og har et forbedringspotensial. På en annen side så kom det frem gjennom intervjuene med informantene at banken ikke ønsker å gi ut for mye informasjon om cyberangrep da dette kan skape panikk. Samtidig bør det også gis ut nok informasjon slik at kundene kan være obs på hva de skal gjøre dersom de blir kontaktet av noen som ønsker deres bankID.

Ansatte i SpareBank 1 SR-Bank fikk opplæring og stadig påfyll av informasjon knyttet til cyberangrep, og hvordan de skulle bidra til å gi kunden økt informasjon dersom de tok kontakt gjennom kundesenter. Det bør samtidig ikke være nødvendig at kunden selv må oppsøke banken for å få informasjon om risikoen ved hackerangrep. SpareBank 1 SR-Bank bruker også media som et verktøy da de sprer informasjon om dagsaktuelle trusler, men det kan se ut som dette er noe banken i ytterligere grad bør vektlegge og informere om selv. Hva som er årsaken til at et så høyt antall av respondentene i spørreundersøkelsen ikke har fått informasjon om hackerangrep fra sin bank kan skyldes flere faktorer; som blant annet at kunden selv ikke har vært oppmerksom dersom de har fått informasjon eller ikke har observert dette på banken sin nettside, samtidig som det også kan være på bakgrunn av informasjonen ikke har vært lett tilgjengelig eller at informasjonen er mangelfull. Likevel så kan det manglende samsvaret mellom resultatene fra spørreundersøkelsen og den empiriske datainnsamlingen tyde på at SpareBank 1 SR-Bank har et forbedringspotensial når det gjelder å dekke kunder sine behov om informasjon om hackerangrep.

Konklusjon forskningsspørsmål 2

SpareBank 1 SR-Bank har en tilstedeværende cybersikkerhetskultur som legger rammer for det kontinuerlige arbeidet for å skape høy motstandsdyktighet når det gjelder cyberangrep. Gjennom å etablere rutiner for sikkerhet og sikkerhetsstyring så gjør dette at banken på flere områder klarer å tilfredsstille de behovene dagens bankkunder har når det gjelder beskyttelse i henhold til cyberangrep.



Figur 25: Analyse av SpareBank 1 SR-Banks samsvar av kunders behov

Slik som drøftet gjennomgående i denne delen av oppgaven så viser resultatet i figur 25 at SpareBank 1 SR-Bank på flere områder har oppnådd en form for behovstilfredsstillelse, på bakgrunn av spørreundersøkelsen med 303 respondenter som ble gjennomført. Ettersom spørreundersøkelsen var basert på respondenter med tilknytning til ulike banker, så kan det bare være antydninger til at SpareBank 1 SR-Bank klarer å tilfredsstille flere behov med ulik tilknytning til cyberangrep. Samtidig legges det også til rette for at det eksisterer forbedringspotensial, slik som figuren viser, men svakhetene vil likevel ikke påvirke negativt i den grad at kunder mister tillit til banken. Det kan vurderes at banken gjør mye viktig arbeid i en riktig retning for å beskytte sine kunder, da gjennom deres cybersikkerhetskultur og resiliens.

7. Avslutning

7.1 Svar på problemstilling

Trusselen for cyberangrep har økt, og gjennomgående i oppgaven blir det klart at cyberangrep kan ikke unngås. Oppgaven illustrerer at trusselen er uunngåelig og noe bankene må ta hensyn til gjennom deres strategi for sikkerhet. Bakgrunnsinformasjonen viser derfor at banker må etablere tilstrekkelig beskyttelse omkring sine løsninger. Cyberangrep vil være en vedvarende trussel grunnet stadige forandringer i hvordan cyberangrep utføres og på hvilke måter hackeren velger å angripe. Denne endringstakten øker sårbarheten for spredning av bankkunders personlige informasjon, noe som danner grunnlag for studiens problemstilling:

«Hvordan kan en bank som en organisasjon beskytte sine kunder mot cyberangrep?»

På bakgrunn av endringstakten i dagens trusselbilde er det viktig for norske banker å etablere velutviklede rutiner som skal øke motstandsdyktigheten og gjøre responstiden er så lav som mulig. Dette vil kunne resultere i at hackere får tak i mindre informasjon og at banken fort kan gjenopprette normaltilstanden. Studiens analyse viser at sikkerhetsrutiner gjennom sikkerhetskultur og RE er effektive for å øke bankens beskyttelse for deres kunder. En sikkerhetskultur med fokus på rapportering, fleksibilitet, rettferdighet og læring skaper rammene for en organisasjons mulighet til å strebe etter resiliens. Læring kan vurderes som den viktigste egenskapen en bank må ha for å kunne håndtere den stadige forandringen av cyberangrep. Gjennom opplæringsrutiner, kontinuerlig informasjonshenting, stadig evaluering av rapporterte hendelser og kommunikasjonen på tvers av banker så øker muligheten til å gi beskyttelse til bankens kunder. For å opprettholde tillitsforholdet mellom bank og kunder må kommunikasjon ut fra banker økes og forbedres, for å forbedre den tilliten kunder har til at banken prioriterer deres sikkerhet. Samtidig bør gjeldende lovgivninger og retningslinjer fra både nasjonale og internasjonale aktører revideres i takt med trusselbildet og tilhørende risiko.

De rammene for sikkerhet som har vært etablert i over lenger tid er ikke lenger kapable til å motstå de truslene banker står ovenfor i dag. For å kunne øke kapasiteten bør derfor flere banker og organisasjoner som håndterer angrep fra cybernettverket etablere en mer dynamisk sikkerhetsmodell. En dynamisk sikkerhetsmodell vil kunne øke motstandsdyktigheten dersom organisasjonen prioriterer sikkerhet gjennom etablering av sikkerhetsstrategier som sikkerhetskultur og RE.

7.2 Veien videre

Det temaet som har blitt diskutert gjennomgående i denne oppgaven er høyt dagsaktuelt, og forskning på dette temaet er i kontinuerlig forandring. For å følge den stadige utviklingen er det flere områder som krever videre forskning. Først og fremst vil det være interessant å vurdere SpareBank 1 SR-Bank sin prosess når de skal implementere en ny strategi for sikkerhet, og videre vurdere om den nye tilnærmingen vil øke sikkerheten og redusere den sårbarheten deres kunder står ovenfor. Det vil også være nyttig med en videre studie på norske banker for å vurdere deres tilnærming til RE og sikkerhetskultur, for å videre kunne evaluere om det eksisterer flere tiltak som bør implementeres for å øke sikkerheten i banknæringen. Når det gjelder lovgivninger knyttet til norske banker så ville det vært nyttig med videre forskning basert på forholdet mellom GDPR og PSD2 for å vurdere om de to lovgivningene bidrar til økt personvern til tross for delingsmulighetene. Sist, men ikke minst, så ville det vært hensiktsmessig med en videre studie knyttet til kunders rolle når det gjelder hackerangrep, og studere mulighetene for å etablere tiltak som kan virke reduserende i forhold til hackerangrep og tilhørende sårbarhet.

Referanseliste

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering and System Safety* 92(6), 745-754.

Aven, T. (2015) (2.utg.). *Risikostyring.* Oslo: Universitetsforlaget.

Aven, T. (2016). Usikkerhet. Store Norske Leksikon. Hentet fra: https://snl.no/usikkerhet

Aven, T. (2018). The Call for a Shift from Risk to Resilience: What does it Mean? *Society for Risk Analysis.*

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

Aven, T. & Renn, O. (2010). *Risk Management and Governance. Concept, Guidelines and Applications*. US: Springer.

Aven, T. & Renn, O. & Rosa, E.A. (2011). The ontological status of the concept of risk. *Safety Science 49.*

Bank of International Settlements (BIS) (2018). History of the Basel Committee. Hentet (05.04.19) fra: https://www.bis.org/bcbs/history.htm

Basel Committee of Banking Supervision (BCBS) (2018). *Cyber-resilience: Range of practises. Bank of International Settlements.* Hentet fra: https://www.bis.org/bcbs/publ/d454.pdf

Bjerknes, C. (2018). DNB-sjefen frykter at hacking kan utløse den neste finanskrisen. Dagens Næringsliv. Hentet (20.02.19) fra: https://www.dn.no/marked/rune-bjerke/dnb/finanskrisen/dnb-sjefen-frykter-at-hacking-kan-utlose-den-neste-finanskrisen/2-1-419662

Bond, D. (2018). Seven UK banks targeted by co-ordinated cyber-attack. *Financial times*.

Hentet (20.02.19) fra: https://www.ft.com/content/2e582594-48ab-11e8-8ee8cae73aab7ccb

Clarke, R. & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it.* US: Harper Collins.

Datatilsynet (u.å.). ID-tyveri. Hentet (20.02.19) fra: https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/id-tyveri/

Dugan, K. (2018). Hackers target thousands of bank emails in cyber-attack. *New York Post*. Hentet (20.02.19) fra: https://nypost.com/2018/08/16/hackers-target-thousands-of-bank-emails-in-cyber-attack/

Dvergsdal, Henrik (2019). Digitalisering. Store Norske Leksikon. Hentet (12.02.19) fra: https://snl.no/digitalisering

Endringslov til finansforetaksloven mv. (2018). Lov om endringer i finansforetaksloven mv. (andre betalingstjenestedirektiv) (LOV-2018-11-23-87). Hentet fra: https://lovdata.no/dokument/NL/lov/2018-11-23e-87?q=betalingstjenestedirektivet

Engen, O. A., Kruke, B. I., Lindøe, P., Olsen, K. H., Olsen, O. E. & Pettersen, K. A. (2016). *Perspektiver på samfunnssikkerhet.* Oslo: Cappelen Damm akademisk.

Finans Norge (2017). *Finansnæringens arbeid mot kriminalitet – Trusler og sårbarheter.* Hentet fra: https://www.finansnorge.no/contentassets/be85a67b49ec4d408d05b1305ef3d54f/finansnaringens-arbeid-mot-kriminalitet---trusler-og-sarbarheter.pdf

Finans Norge (u.å.). PSD2 eller betalingstjenestedirektivet. Hentet fra: https://www.finansnorge.no/tema/bank/psd2-eller-betalingstjenestedirektivet/

Finanstilsynet (2017). Finanstilsyn og regelverk i EØS. Hentet fra: https://www.finanstilsynet.no/tema/finanstilsyn-og-regelverk-i-eos/

Forskrift om IKT-systemer i banker mv. (2003) Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) (FOR-2003-05-21-630). Hentet (04.06.2019) fra: https://lovdata.no/dokument/SF/forskrift/2003-05-21-630

Forskrift om risikostyring og internkontroll (2009) Forskrift om risikostyring og internkontroll (FOR-2008-09-22 1080). Hentet fra: https://lovdata.no/dokument/SF/forskrift/2008-09-22-1080

GDPR (2016). General Data Protection Regulation ((EU) 2016/679). Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

Grunnloven (1814). Kongeriket Norges Grunnlov (LOV-1814-05-17). Hentet fra: https://lovdata.no/dokument/NL/lov/1814-05-17

Gundersen, D. (2018). Latent. Store Norske Leksikon. Hentet (03.03.19) fra: https://snl.no/latent

Halvorsen, Knut. (2008). *Å forske på samfunnet: en innføring i samfunnsvitenskapelig metode* (5.utg.). Oslo: Cappelen akademisk forlag.

Hammer, J. (2018). The billion-dollar bank job. *The New York Times Magazine.* Hentet (20.02.19) fra: https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html

Hollnagel, E. (2011) Epilouge: RAG – The Resilience Analysis Grid by Erik Hollnagel i Pariès, J., Wreathall, J. Woods, D. D. & Hollnagel, E. (Red.) (2011). *Resilience Engineering in Practice: A guidebook.* UK: Ashgate

Hollnagel, E. (2014). *Safety-I and Safety-II. The Past and Future of Safety Management*. UK: Ashgate.

Hollnagel, E. (2015). Introduction to the Resilience Analysis Grid (RAG). Hentet fra: http://erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf

Hollnagel, E. (2016). Resilience Engineering: A New Understanding of Safety. Journal of the Ergonomics Society of Korea.

Hollnagel, E. (2017). Safety-*II in Practice: Developing the Resilience Potentials.* UK: Routledge.

Hollnagel, E. & Woods, D.D. (2006). Prologue: Resilience Engineering Concepts. I Hollnagel, E., Woods, D. D. & Leveson, N.C. (Red.) (2006). *Resilience engineering: Concepts and Precepts.* UK: Ashgate.

Hovland, K. M. (2017). Her er de verste dataangrepene. E24. Hentet (04.04.19) fra: https://e24.no/digital/datakriminalitet/her-er-de-verste-dataangrepene/23997690

Hvitvaskingsloven - hvvl (2018). Lov om tiltak mot hvitvasking og terrorfinansiering (LOV-2018-06-01-23). Hentet fra: https://lovdata.no/dokument/NL/lov/2018-06-01-23#KAPITTEL_3

Johnson, B. R., Onwuegbuzie, J. A. & Turner, L. A. (2007). Toward a Definition of Mixed Methods Reserach. *Educational researcher,* 33(7), 14-26.

Justis- og politidepartementet (1994). «Langtidsplan for det sivile beredskap 1995-1998». *Stortingsmelding nr.48 (1993-1994),* Justis- og politidepartementet, Oslo.

Justis- og beredskapsdepartementet (2018). *Nasjonal risikovurdering. Hvitvasking og terrorfinansiering i Norge 2018.* Hentet fra: https://www.regjeringen.no/contentassets/58f96ea9756d4457be3095609624d96d/nasjonal-riskikovurdering.pdf

Kaufman, G. & Kaufman, A. (2015). *Psykologi i organisasjon og ledelse* (5.utg. ed.). Bergen: Fagbokforlaget

Knuth, D., Kehl, D., Hulse, L. & Schmidt, S. (2014). Risk Perception, Experience, and Objective Risk: A Cross-National Study with European Emergency Survivors. *Risk Analysis, 34*(7), 1286-1298. doi:10.1111/risa.12157

Leveson, N. (CREDC) (2016). *The Need for a Paradigm Shift in Safety and Cyber Security*. Hentet (05.06.2019) fra: https://www.youtube.com/watch?v=WBktiCyPLo4&t=3395s

Lindøe, P.H., Kringen, J. & Braut, G.S. (2012). *Risiko og tilsyn. Risikostyring og rettslig regulering.* Oslo: Universitetsforlaget.

Malt, U. (2018). Fleksibilitet. Store Norske Leksikon. Hentet (05.06.2019) fra: https://snl.no/fleksibilitet_-_psykologi

Mee, P. & Schuermann, T. (2018). How a Cyber Attack Could Cause the Next Financial Crisis. *Harvard Business Review.* Hentet (20.03.19) fra: https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis

Monaghan, A. (2018). Bank of England stages day of war games to combat cyber-attacks. The Guardian. Hentet (02.02.19) fra: https://www.theguardian.com/business/2018/nov/09/bank-of-england-stages-war-games-combat-cyber-attacks-data-breaches

Nasjonal Sikkerhetsmyndighet (2014). Sikkerhetskultur. Hentet (31.05.19) fra: https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/

Nasjonal sikkerhetsmyndighet (2015a). *Sikkerhetsfaglig råd.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/nsm-sikkerhetsfaglig_raad_2015_web.pdf

Nasjonal sikkerhetsmyndighet (2015b). *Veileder i sikkerhetsstyring.* Hentet fra: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf

Nasjonal sikkerhetsmyndighet (2018). *Et sikkert digitalt Norge – IKT-risikobilde 2018.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf

Nasjonal sikkerhetsmyndighet, Etterretningstjenesten & Politiets sikkerhetstjeneste (2010).

Koordineringsgruppen for IKT-risikobildet: Cybersikkerhet. Statsministerens kontor. Hentet fra: https://www.regjeringen.no/contentassets/252f869fdfac46648e41e6ca5fb0600a/cybersikkerhet_svar-med-merknader_nsm-pst-etterretningstjenesten.pdf

NOU 2015:13 (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Justis- og beredskapsdepartementet. Hentet fra: https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/sec2

NRK (2017). IKT-hendelser kan ramme hardt i verdens mest digitaliserte land. *Norsk rikskringkasting.* Hentet (02.02.19) fra: https://www.nrk.no/sorlandet/ikt-hendelser-kan-ramme-hardt-i-verdens-mest-digitaliserte-land-1.13710102

Personopplysningsloven (2018). Lov om behandling av personopplysninger. (LOV-2018-06-05-38). Hentet fra: https://lovdata.no/dokument/NL/lov/2018-06-15-38/*#*

Politiet (u.å.) ID-tyveri. Hentet fra: https://www.politiet.no/rad/tyveri-og-vinningskriminalitet/id-tyveri/

PSD2 (2015). Payment Service Directive 2. Hentet fra: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

Reason, J. (1997). *Managing Risks of Organisational Accidents*. UK: Ashgate.

Reason, J. (2000). Human error: Models and management. *British Medical Journal*, 320, 768-770. Hentet fra: http://www.ncbi.nlm.nih.gov/pmc/articles/pmc1117770/

Renn, O. (2008). *Risk Governance.* UK: Earthscan

Ringdal, K. (2013). *Enhet og mangfold: samfunnsvitenskapelig forskning og kvantitativ metode* (3. utg.). Bergen: Fagbokforlaget.

Rousseau, D.M., Sitkin, S., Camerer, C. F. & Burt, R. (1998) Not so different after all. A cross-discipline view of trust, *Academy of Management Review 23 (3)*.

Sagdahl, M. (2016). Rettferdighet. Store Norske Leksikon. Hentet (05.05.2019) fra: https://snl.no/rettferdighet

Samson, A. & Egan, M. & Booton, J. (2012). Bank of America Hit by Cyber Attack. *Fox Business*. Hentet (20.02.19) fra: https://www.foxbusiness.com/features/bank-of-america-hit-by-cyber-attack

Sjöberg, L., Rundmo, T. & Moen, B-E. (2004). E*xplaining risk perception: an evaluation of the psychometric paradigm in risk perception research* (Vol. no. 84, 2004) Trondheim: Rotunde.

Skulberg, H. (2017) Om sammenheng mellom utdanning og tillit (Temanotat 7, 2017). Hentet fra: https://www.utdanningsforbundet.no/var-politikk/kunnskapsgrunnlag/publikasjoner/2017/om-sammenhengen-mellom-utdanning-og-tillit/

SpareBank 1 SR-Bank (u.å.). (1) Om konsernet. Hentet fra: https://www.sparebank1.no/nb/sr-bank/om-oss/om-banken.html

SpareBank 1 SR-Bank (u.å.) (2) Slik ivaretar vi ditt personvern og vår taushetsplikt. Hentet fra: https://www.sparebank1.no/nb/sr-bank/om-oss/personvern.html

SpareBank 1 SR-Bank (u.å.). (3) Slik sikrer vi personopplysninger. Hentet fra: https://www.sparebank1.no/nb/sr-bank/om-oss/personvern/slik-sikrer-vi-personopplysninger.html#par_title

SpareBank 1 SR-Bank (u.å.). (4) Visjon og verdier. Hentet fra: https://www.sparebank1.no/nb/sr-bank/om-oss/om-banken/visjon-og-verdier.html

SpareBank 1 SR-Bank (u.å.). (5) Vår historie. Hentet fra: https://www.sparebank1.no/nb/sr-bank/om-oss/om-banken/var-historie.html

Steen, R. (2019). On the Application of the Safety-II Concept in a Security Context. *European Journal for Security Research* https://doi.org/10.1007/s41125-019-00041-0.

Stubbs, J. (2018). Hackers stole $6 million from Russian bank via SWIFT system: central bank. Reuters. Hentet (20.02.19) fra: https://www.reuters.com/article/us-russia-cyber-swift/hackers-stole-6-million-from-russian-bank-via-swift-system-central-bank-idUSKCN1G00DV

Tjora, A. H. (2012). *Kvalitative forskningsmetoder i praksis* (2. utg. utg.). Oslo: Gyldendal akademisk.

Tylor, E. B. (1871). *Primitive Culture. Research into the Development of Mythology, Philosophy, Religion, Art and Custom.* Cambridge Library Collection.

Vatnelid, I. L. (2018). *Risiko – en innføring i god praksis*. Oslo: Gyldendal.

Wall, M. (2018). A cyber-attack could stop the country. BBC News. Hentet (20.02.19) fra: https://www.bbc.com/news/business-45952693

Walker, W.E., P. Harremoës, J. Rotmans, J.P. van der Sluijs, M.B.A. van Asselt, P. Janssen, M.P. Krayer von Krauss (2003). Defining Uncertainty: A Conceptual Basis for Uncertainty Management in Model-Based Decision Support. *Integrated Assessment*, Vol. 4, No. 1, pp. 5-17.

Walker, W. E, Lempert, R. J. & Kwakkel, J. H. (2016). Deep Uncertainty. Hentet fra:https://pdfs.semanticscholar.org/8e6b/c8cd6c880e54c68e6c1c71a9f9a5a5781283.pdf

Wilde, G. J. S. (1998). Risk homeostasis theory: an overview. *Injury Prevention, 4*(2), 89 91.doi:10.1136/ip.4.2.89

World Economic Forum (2019). *The Global Risks Report 2019* (14th edition). Hentet fra: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Oversikt over vedlegg

- Vedlegg A: Spørreundersøkelse: Cyberangrep i bank
- Vedlegg B: Samtykkeskjema til informanter
- Vedlegg C: Intervjuguide: ustrukturert intervju med ansatte i SR-bank
- Vedlegg D: Intervjuguide: ustrukturert intervju med ledere, gruppe 1
- Vedlegg E: Intervjuguide: ustrukturert intervju med ledere, gruppe 2

Vedlegg A:

Spørreundersøkelse: Cyberangrep i bank

Spørsmål 1:

Alder

- Under 18år
- 18-28 år
- 29-39år
- 40-60år
- Over 60år

Spørsmål 2:

Kjønn

- Mann
- Kvinne
- Ønsker ikke å oppgi

Spørsmål 3:

Gjennom en ny lovgivning fra EU skal betalingstjenester i Norge få muligheten til å dele personlig informasjon om kunder mellom seg. Dette vil øke risikoen for at din personlige informasjon skal komme på avveie. Hvor stor tillit har du til at din bank skal forhindre at din informasjon ikke blir gitt til feil aktør?

1. Kritisk med ingen tillit
2. Veldig skeptisk med lav tillit
3. Likegyldig
4. Nokså høy tillit
5. Full tillit

Spørsmål 4:

Innsideangrep handler om at det er noen på innsiden, ofte en ansatt, som utfører hackerangrep. Bankens ansatte har full oversikt over all din personlige informasjon, og har mulighet til å

spre denne informasjonen. Vil dette ha noen påvirkning for deg som kunde i forhold til tillit til banken og dens ansatte?

- Ingen påvirkning
- Likegyldig
- Stor påvirkning, det svekker tillitsforholdet

Spørsmål 5:

I et hackerangrep så kan hackere stjele din personlige informasjon og foreta banktransaksjoner som fører til at du mister alle pengene dine. Ved et slikt scenario, stiller du banken din ansvarlig?

1. Banken er full ansvarlig
2. Banken har mye ansvar
3. Banken har litt ansvar
4. Banken har lite ansvar
5. Banken har ingen ansvar

Spørsmål 6:

En metode som brukes for ID-tyveri er å kontakte bankkunder via e-mail eller telefon i håp om at kunden skal oppgi sin bank-ID for å kunne foreta seg banktransaksjoner. Ønsker du som kunde mer rådgivning om slike angrep? Hvis ja, hvilke metoder bør banken bruke?

- Nei
- Ja, gjennom kurs
- Ja, gjennom kundekveld med foredrag
- Ja, gjennom informasjon via e-mail

Spørsmål 7:

Gjennom overvåkning av bankkontoer og pengetransaksjoner så har banken din mulighet til å observere dersom store beløp med penger er på vei ut av din konto. Ønsker du at banken din skal ta kontakt dersom dette vekker mistanke, og eventuelt hvordan?

- Nei, jeg ønsker ikke at min bank skal overvåke mine transaksjoner
- Jeg ønsker at banken min skal ta øyeblikkelig kontakt via telefon
- Jeg ønsker at banken min skal sende meg en SMS med informasjon

- Jeg ønsker at banken min skal sende meg en e-mail med informasjon

Spørsmål 8:

Har du noen gang blitt informert av din bank om at det er fare for at hackerangrep kan oppstå? Hvis ja, kryss av for hvilke hackerangrep du har blitt informert om.

- Har ikke blitt informert om hackerangrep
- Misbruk av bank-ID for pengetransaksjoner
- Misbruk av personlig informasjon for å få kredittkort
- Frivillig overføring av penger etter å ha blitt manipulert (kjærlighetssvindel)
- Misbruk av bank-ID for å få tilgang til nettbank

Vedlegg B:

Samtykkeskjema til informanter

Heihei,

Jeg, Jeannett Hansen, skriver masteroppgave i samfunnssikkerhet på Universitetet i Stavanger, og vil i den sammenheng gjennomføre intervjuer som en del av mitt forskningsprosjekt.

Foreløpig problemstilling er som følger:

Hvordan kan en bank som organisasjon beskytte kundene deres mot cyberangrep?

Jeg samtykker til å delta i forskningsprosjektet ☐

Jeg samtykker i at dette intervjuet kan tas opp på bånd ☐

Jeg samtykker i at navnet mitt brukes i forskningsprosjektet ☐

Signatur informant:

Sted:

Dato:

Vedlegg C:

Intervjuguide: ustrukturert intervju med ansatte i SR-bank

Del 1: Uformell prat

1. Presentasjon av studien og følgende problemstilling.

2. Presentasjon av informant.

Del 2: Intervju

1. Hva anser du å være en god sikkerhetskultur?

2. Er det et rammeverk som skal bidra til sikkerhetskultur i SR-bank, og på hvilken måte?

3. Bidrar ledelsen i SR-bank til å skape en sikkerhetskultur?

4. Hvordan foregår rapportering av feil i SR-bank?

5. Hvilke hendelser blir rapportert til ledelsen i SR-bank, og hva blir konsekvensene?

6. Har du som ansatt myndighet til å ta avgjørelser i krisesituasjoner, eventuelt i hvilken grad?

7. Er det fokus på evaluering av uønskede hendelser i SR-bank?

Del 3: Avslutning

– Har du noen spørsmål, eller noe du ønsker å legge til som vil være nyttig for studien?

Vedlegg D:

Intervjuguide: ustrukturert intervju med ledere, gruppe 1

Del 1: Uformell prat

3. Presentasjon av studien og følgende problemstilling.

4. Presentasjon av informant.

Del 2: Intervju del 1

1. Bruker banken en bestemt metode for å informere kundene deres om cyberangrep og konsekvenser for kunden?

2. Blir kundene deres informert om nye lovgivninger og hvordan dette vil påvirke kunden?
    a. Blir det implementert tiltak for å forhindre at ansatte kan spre personlig informasjon?

3. Hvem er ansvarlig dersom et cyberangrep oppstår?

4. Tilbyr dere som bank noen tjenester for å gi kunden økt informasjon og kunnskap om hvordan man skal håndtere cyberangrep, i form av kurs og veiledning?

Del 3: Intervju del 2

1. Hva anser du å være god sikkerhetskultur?

2. De elementene du nevnte i spørsmålet ovenfor, er dette eksisterende i SR-bank?

3. Bruker SR-bank en sikkerhetsstrategi som grunnleggende for sikkerhetskulturen i organisasjonen?

4. Hva gjør ledelsen for å skape en god sikkerhetskultur?

5. Anser du at det er oppmuntring til å rapportere feil? Er dette noe dere vektlegger i organisasjonen?

Del 4: Avslutning

– Har du noen spørsmål, eller noe du ønsker å legge til som vil være nyttig for studien?

Vedlegg E:

Intervjuguide: ustrukturert intervju med ledere, gruppe 2

Del 1: Uformell prat

1. Presentasjon av studien og følgende problemstilling.

2. Presentasjon av informant.

Del 2: Intervju

1. Foreligger det beredskapsplaner og retningslinjer for hva de ansatte skal gjøre dersom cyberangrep oppstår?

2. Har banken til enhver tid ansatte på jobb som kan håndtere cyberangrep?

3. Hvor lang tid regnes med å bruke på å komme tilbake til normaltilstand etter cyberangrep?

4. Hvem er ansvarlig for at alle systemene skal være intakt og oppdaterte?

5. Er det fokus på overvåkning i SR-bank?

6. På hvilken måte overvåker SR-bank dagens utfordringer knyttet til cyberangrep?

7. Hvor ofte blir beredskapsplaner og retningslinjer oppdatert ved saker som er relatert til sikkerhet?

8. Er det ansatte kontinuerlig opplært i alle typer trusler banken står ovenfor?

9. Hvor ofte blir det foretatt en trusselvurdering?

10. Foreligger det retningslinjer for akseptabel risiko?

11. Hvilke hendelser blir rapportert i SR-bank?

12. Er det fokus på evaluering av hendelser som ble rapportert?

13. Er det fokus på kurs og videre opplæring i forhold til sikkerhet i SR-bank?

Del 3: Avslutning

– Har du noen spørsmål, eller noe du ønsker å legge til som vil være nyttig for studien?