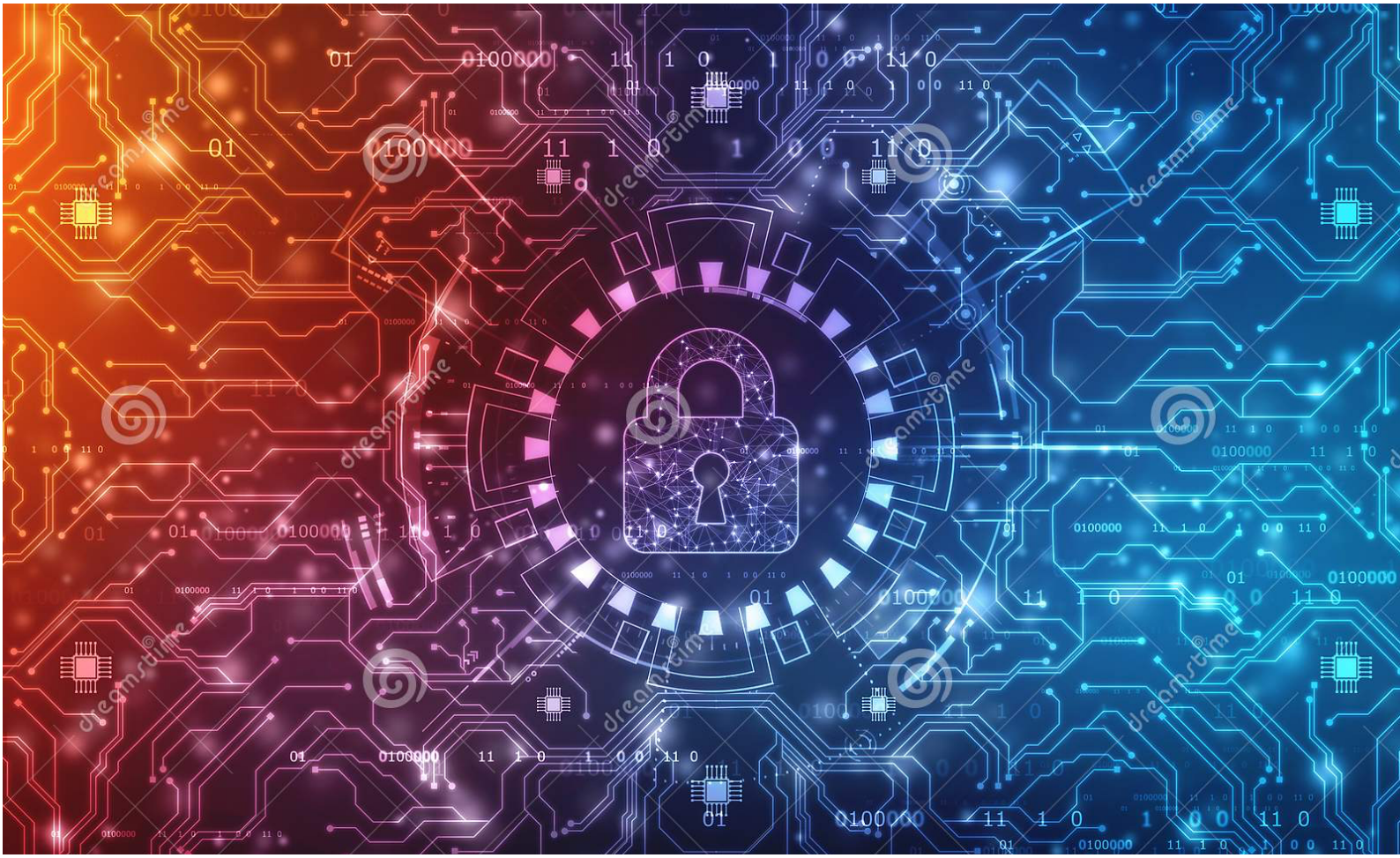
En studie av en digital sikkerhetskultur i en organisasjon



«Man skjønner ikke at man ikke skjønner cyberspace og datamaskiner. Det er egentlig forklaringen på alt».

Master i samfunnssikkerhet

Vår 2022

IRENE HELLA

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET
MASTEROPPGAVE

Studieprogram/spesialisering:

Master i Samfunnssikkerhet

Vårsemesteret, 2022

Åpen / Konfidensiell

Forfatter: **Irene Hella**

.....Irene Hella.....
(signatur forfatter)

Fagansvarlig: Odd Einar Falnes Olsen

Veileder(e): Odd Einar Falnes Olsen

Tittel på masteroppgaven:
En studie av en digital sikkerhetskultur i en organisasjon

Engelsk tittel: **A study of a digital safety culture in an organization**

Studiepoeng: 30

Emneord: Sårbarhet, digital sikkerhet, sikkerhet, robusthet, funksjonalitet, resiliens, barrierer, digital kompetanse, informasjonssikkerhet, IKT-sikkerhet, kompleksitet, modusforvirring, sikkerhetskultur, informasjonssystemer, kultur, datakriminialitet, digitale hendelser, cyberspace, cybersikkerhet

Sidetall: 72

+ vedlegg/annet: 2

Stavanger, 14/6 - 22

Forord

Denne oppgaven markerer at min tid som masterstudent i samfunnssikkerhet ved Universitetet i Stavanger går mot slutten. Disse to årene har vært fylt med spennende forelesninger, interessante diskusjoner og personlig vekst for meg som person, samt gjort meg bedre rustet i møte med arbeidslivet om kort tid.

Gjennom denne oppgaven har jeg benyttet muligheten til å knytte samfunnssikkerhet opp mot et svært aktuelt og viktig tema, nemlig digital sikkerhet. Kunnskapen jeg har tilegnet meg gjennom dette studiet, gjør meg godt rustet for å møte en fremtid med nye og dynamiske sikkerhetsutfordringer innenfor det digitale domenet.

Jeg ønsker å rette en stor takk til min veileder, professor Odd Einar Falnes Olsen, for et godt samarbeid. Han har bidratt med verdifulle innspill, konstruktiv kritikk og entusiasme for temaet.

Jeg ønsker også å gi en ekstra oppmerksomhet til en ildsjel når det kommer til digital sikkerhet, Jørgen Dyrhaug fra Nasjonal Sikkerhetsmyndighet. Takk for ditt engasjement for oppgaven, samt din kompetanse rundt temaet som har gitt meg en unik innsikt i tematikken. Takker også for at jeg fikk tillatelse til å bruke ditt fulle navn i oppgaven, for å skape dybde og troverdighet til uttalelsene dine.

Videre ønsker jeg å rette en takk til mine informanter, som har gjort denne oppgaven gjennomførbar. Jeg kunne ikke forestilt meg å bli møtt med et så stort engasjement og viktige bidrag.

Irene Hella, 14. juni. 2022

Sammendrag

Denne masteroppgaven handler om digital sikkerhet innenfor bank – og forsikringsbransjen. Problemstillingen handler om å belyse de viktigste utfordringene når det kommer til digital sikkerhetskultur i en organisasjon. Gjennom relevante dokumenter og åtte kvalitative intervjuer har jeg forsøkt å se nærmere på hvordan medarbeidere og ledere forholder seg til digital sikkerhet i det daglige.

For å besvare denne problemstillingen ser jeg nærmere på 1) hva ledere gjør for å bygge opp en digital sikkerhetskultur, 2) hvilke rutiner som er etablert for å vedlikeholde digital sikkerhet og 3) hvordan de ansatte forstår trusler og farer ved bruk av teknologi. I denne sammenhengen diskuterer jeg åtte dimensjoner som skal sikre digital sikkerhet i en organisasjon; fellesskap, styring og kontroll, tillit, risikoforståelse, vilje til digitalisering, kompetanse, interesse og atferdsmønstre. Disse bidrar på hver sin måte til å belyse problemstillingen.

Det kommer frem at det ofte er usikkerhet rundt hvem som faktisk har ansvaret for sikkerhet, og at de aller fleste automatisk har tillit til at «de som jobber med sikkerhet» tar seg av arbeidet rundt dette. Digitaliseringen er både avhengig av, og sårbar for tillit, og det kan virke som tillit er sentralt når det kommer til informantenes forståelse av digitale sikkerhet. Sammenhengen mellom tillit og ansvarsfraskrivelse blir diskutert og en delkonklusjon er at den digitale sikkerheten er *alles* ansvar, også de som ikke jobber med sikkerhet i det daglige.

Videre kommer det frem at menneskene i organisasjonen ofte er den sårbarheten som trusselaktørene velger å utnytte. I denne diskusjonen kommer det frem at kompetanse innenfor teknologi og digital sikkerhet, gjerne via kursing og andre godt etablerte rutiner, bidrar til økt digital sikkerhet fordi menneskene i organisasjonen får mer kompetanse. Den enkelte medarbeiders risikoforståelse og tankegang rundt sikkerhet kan derfor bidra til å unngå eventuelle hendelser. I denne sammenhengen blir fellesskap og en kultur som setter sikkerhet høyt på agendaen viktig.

Nøkkelutfordringen knyttet til digital sikkerhetskultur handler om at teknologien og cyberspace er mer komplisert og farligere enn vi noen gang kan forstå.

God lesing!

Innholdsfortegnelse

Figuroversikt

Tabelloversikt

Vedlegg

1. Introduksjon

På bakgrunn av dagens risikobilde i det norske samfunnet har digitalisering og teknologisk utvikling resultert i en økende sårbarhet for alle organisasjoner i samfunnet. «Hovedtrendene er de samme som tidligere år. Den digitale risikoen øker» (NSM, 2019, s. 6). Dette skriver Nasjonal Sikkerhetsmyndighet (NSM) i en rapport fra 2019 som beskriver et helhetlig digitalt risikobilde i Norge. I tillegg ser man i kjølvannet av pandemien Covid-19 at hastighet og tilgjengelighet ved hjelp av digitale løsninger ofte vinner på bekostning av sikkerhet;
"The combination of remote work and data proliferation trend has led to an alarming increase in cybercrimes" (Charpenter, 2022).

En fersk undersøkelse fra NHO viser at 1 av 5 bedrifter har opplevd dataangrep i 2021 (NHO, 2022). Derfor oppfordrer de alle organisasjoner til å sikre at man har god digital beredskap og ikke tar lett på trusselen (NHO, 2022). Et tema som straks fanget oppmerksomheten min er digital sikkerhetskultur i organisasjoner og hvordan vi mennesker er sårbare i det teknologiske risikobildet vi ser i dag. Det kommer frem av en rapport utgitt av NorSIS «Nordmenn og digital sikkerhetskultur 2021» at flere hundre tusen norske arbeidstakere mener de selv ikke kan skru på totrinnsbekreftelse eller vurdere om det er trygt å åpne en e-post (Lystad, 2022).

Faren for at digitale trusler skal inntreffe norske organisasjoner danner derfor det tematiske grunnlaget for denne studien. Datakriminalitet eller utilsiktede digitale uhell rammer selskaper hver dag. De som rammes påføres også direkte kostnader, og som oftest betydelig ressursbruk for å sikre de digitale verdiene som er i spill når det skjer (NSM, 2019). Derfor er det av relevans å se nærmere på hvordan organisasjoner legger til rette for risikoforståelse og en felles digital sikkerhetskultur (NSM, 2021). Å gå i dybden av selskapets eget risikobilde kan gjøre at virksomheter kan identifisere personellsikkerhetsmessige tiltak som begrenser trusselaktørenes mulighetsrom og som øker virksomhetens egen sikkerhetsmessige robusthet (NSM, 2021).

En sikkerhetskultur kan defineres som: «et sett med verdier som deles av medarbeidere i en virksomhet, og som er med på å påvirke deres tanker og forventinger til sikkerhet» (NSM, 2021). Ved å motivere medarbeiderne til å handle på en måte som ivaretar sikkerheten, kan virksomheten skape en god sikkerhetskultur internt og på denne måten skaffe seg barrierer mot datakriminalitet.

1.1 Bakgrunn for valg av tema

Temaet for denne masteroppgaven vil være å se nærmere på den digitale sikkerhetskulturen i en organisasjon. Temaet er aktuelt i dag fordi alle organisasjoner tvinges til å møte teknologiske krav i omgivelsene rundt oss, men ikke alle forstår den risiko og de farer som teknologien også kan føre med seg. Ved å studere digital sikkerhetskultur nærmere, belyser jeg viktigheten av sikkerhetsarbeid i en organisasjon, samt hvilke komponenter som er drivere for å få både ledere og medarbeidere motivert til en mer sikkerhetsorientert tankegang.

Fokuset i masteroppgaven vil være på menneskene i organisasjonen. Fra et HR-perspektiv vil jeg undersøke nærmere hvordan lederes vilje til digitalisering og økt risikoforståelse kan bidra til en sterkere sikkerhetskultur i organisasjonen. Et sentralt spørsmål i denne sammenhengen er om vi faktisk forstår hvilken teknologi og farer som vi står overfor.

Det er samfunnsnyttig å studere dette temaet fordi kompetanse om hvordan man kan skape en mer robust sikkerhetskultur i en organisasjon vil være nødvendig for mange ledere, og ikke minst virksomheter i fremtiden. Denne oppgaven vil bidra til mer innsikt og forståelse om hvordan kultur, risiko og sikkerhet henger sammen og hvorfor det er viktig for ledere å se verdien av å investere i sikkerhet i fremtiden. Oppgaven vil også belyse teknologiske farer vi står overfor og bidra til økt kunnskap om bruk av datamaskiner og annen teknologi i det daglige. Dette er et viktig tema å belyse i dagens sårbare teknologiske samfunn.

1.2 Problemstilling og forskningsspørsmål

Med utgangspunkt i oppgavens avgrensning og tema har jeg utarbeidet følgende problemstilling:

Hva er de viktigste utfordringene innenfor bank – og forsikringsbransjen for å utvikle en digital sikkerhetskultur?

Med utfordringer menes her eventuelle problemstillinger eller situasjoner en organisasjon i denne bransjen kan møte på som gjør det vanskelig å utvikle en digital sikkerhetskultur internt.

I undersøkelsen av denne problemstillingen er det formulert tre forskningsspørsmål som på hver sin måte bidrar til å belyse problemstillingen. For å forstå hva ledere prioriterer i arbeidet med

digital sikkerhet og hvordan de forstår risiko er det første forskningsspørsmålet formulert på følgende måte:

F1) Hva gjør ledere for å bygge opp en digital sikkerhetskultur?

Hva som faktisk gjøres i arbeidet med digital sikkerhet vil også bidra til å gi innsikt i deres generelle risikoforståelse. Videre er det relevant å se nærmere på hvilke rutiner organisasjonen har for digital sikkerhet og hvilke barrierer som er satt opp for å unngå uventede hendelser. Det neste forskningsspørsmålet handler derfor om rutiner og er egnet for å besvare problemstillingen fordi det vil gi en god pekepinn på hvor pålitelig organisasjonens digitale sikkerhetskultur er. Det andre forskningsspørsmålet er derfor formulert på denne måten:

F2) Hvilke rutiner er etablert for å vedlikeholde digital sikkerhet i organisasjonen?

Her vil en kunne se nærmere på når rutinene er innført og om det er på bakgrunn av et forebyggende sikkerhetsarbeid eller om det er et resultat av tidligere hendelser. Endringer i rutiner og systemer for digital sikkerhet vil kunne gi en pekepinn på hvilket fokus en organisasjon har på dette området, og om de faktisk ønsker å gjøre organisasjonen mer robust til eventuelle nye hendelser.

Helt sentralt er det å kartlegge de ansattes perspektiv på digital sikkerhet, da det i stor grad kan reflektere hva ledere gjør for å ha fokus på digital sikkerhet og hvor utfordringene ligger på daglig basis. Det siste forskningsspørsmålet er derfor formulert på følgende måte:

F3) Hvordan forstår de ansatte trusler og farer ved bruk av ny eller eksisterende teknologi?

Ved å undersøke dette vil man få en indikator på om de ansatte er klar over hvilke eventuelle trusler eller farer som finnes ved bruk av teknologi i det daglige arbeidet. Videre vil forskningsspørsmålet også indirekte få frem om de ansatte har kunnskap om eller forstår omfanget av de angrepene organisasjonen kan stå overfor som følge av digitale løsninger.

1.3 Tidligere forskning og rapporter

Innledningsvis er det relevant å se nærmere på noen internasjonale trender innenfor fremveksten av teknologi og digitale enheter for å få et inntrykk av hvilken veksttakt teknologien har hatt gjennom tidene. Den russiske økonomen Nikolai Kondratieff utviklet i 1925 en teori om kulturelle "bølger" for å beskrive langsiktige sykluser av økonomisk aktivitet som hadde betydelig innvirkning på økonomisk aktivitet, produksjonsmidler og utveksling (Levender, 2010, s.127). I etterkant beskriver flere moderne teoretikere den digitale tidsalderen som en slik bølge (Lavender, 2010, s. 127).

Teknologien har utviklet seg i rekordfart internasjonalt de siste 30 årene, og Norge er i dag blitt blant de fremste landene i verden til å ta i bruk ny teknologi (NOU: 2017). På bakgrunn av at vi i dag flytter store deler av verdiene våre over på nettet, øker også den digitale kriminaliteten i en takt vi har vanskelig for å forstå (NSM 2019, s. 12). En undersøkelse viser at 6 av 10 nordmenn hevder at de klarer å bedømme hva som er trygt å gjøre på internett og ikke med tanke på datakriminalitet (NorSIS 2016, s. 8). Likevel klikker vi fortsatt på lenker i e-poster, putter minnepenner i datamaskiner og velger dårlige, gjenbrukte passord (NSM 2019, s. 18).

I 2016 publiserte Norsk Senter for informasjonssikring rapporten The Norwegian Cybersecurity Culture (NorSIS, 2016), hvor konseptet digital sikkerhetskultur for første gang ble beskrevet og kartlagt i Norge. Rapporten ble utarbeidet på oppdrag fra justis – og beredskapsdepartementet, og mange sentrale aktører innen digital sikkerhet deltok i arbeidet. En virksomhets digitale sikkerhetskultur kan ifølge NorSIS (2016) beskrives ved hjelp av åtte spesifikke dimensjoner. Disse dimensjonene blir brukt gjennomgående i oppgaven for å skape en helhetlig forståelse av en digital sikkerhetskultur og hva den består av. Denne rapporten la føringer for den første stortingsmeldingen utelukkende om digital sikkerhet i Norge; Meld. St. 38 (2016-2017) «IKT-sikkerhet: et felles ansvar». Stortingsmeldingen fikk dette navnet fordi det kom frem i lyset at vi har alle en felles interesse av, og et ansvar for, å sikre våre verdier i møte med ny teknologi. Ifølge Meld. St. 38 er det i dag høye forventninger knyttet til at digitale tjenester skal være robuste, motstå trusler, forsøk på misbruk, feil i utstyr og menneskelig svikt (Meld. St. 38 (2016-2017), s. 14).

Norges offentlige utredninger (NOU) har i 2018 utarbeidet en rapport for IKT-sikkerhet i alle ledd (NOU:2018). Rapporten er utarbeidet av departementenes sikkerhets – og

serviceorganisasjon avgitt til Justis – og beredskapsdepartementet. Rapporten omhandler organisering og regulering av nasjonal IKT-sikkerhet, og har et særlig fokus på lover og forskrifter som stiller krav om IKT-sikkerhet. Utvalgets tiltak og anbefalinger i del 4 av rapporten benyttes i denne oppgaven som en veiledning for hvordan virksomheter kan sikre sine informasjonssystemer på en bedre måte enn i dag.

Nasjonal strategi for digital sikkerhet (2019) er en rapport fra Departementet som tar for seg en helhetlig tilnærming til digitaliseringen i det norske samfunn. Denne beskriver at Norges første nasjonale strategi for digital sikkerhet ble lansert allerede i 2003. I takt med utviklingen av trusselbildet ble den nasjonale strategien revidert i 2007 og 2012. Strategien som blir brukt i denne oppgaven vil være Norges fjerde strategi for digital sikkerhet fra 2019. Strategien skal møte utfordringene som følger av en gjennomgående digitalisering av det norske samfunnet. Strategiens primære målgruppe er myndigheter og virksomheter i privat og offentlig sektor. Strategien skal også legge til rette for at privatpersoner får nødvendig kunnskap og risikoforståelse for å kunne ta i bruk teknologi på en trygg måte.

NSMs grunnprinsipper for IKT-sikkerhet, utarbeidet av NSM i 2020 (versjon 2) er et sett med prinsipper og anbefalinger for hvordan virksomheter kan beskytte sine informasjonssystemer mot uautorisert tilgang, skade eller misbruk (NSM, 2020, s. 5). Disse anbefalingene er relevante for alle norske virksomheter og benyttes derfor i denne oppgaven som et sett med generelle anbefalinger for hvordan organisasjoner skal kunne sikre sine verdier og informasjonssystemer i forbindelse med bruk av IKT-systemer. Hvilke anbefalinger som er relevante vil variere ut ifra hvilken virksomhet det er snakk om (NSM, 2020, s. 5).

Nasjonalt digitalt risikobilde (2021) av NSM er en årlig rapport som skal øke bevissthet rundt digital sikkerhet, samt motivere til sikrere bruk av digital sikkerhet i fremtiden. Rapporten bygger på en omfattende portefølje av risiko- og sårbarhetsrapporter fra myndigheter, næringslivet, akademia og bransje- og interesseorganisasjoner. Den tar videre opp problemstillinger knyttet til samfunnssikkerhet og individsikkerhet innenfor det digitale domenet. Rapporten brukes i denne oppgaven som et bidrag for å forstå risikobildet i dag, samt å få en dypere forståelse for hvordan et forebyggende sikkerhetsarbeid kan være med å redusere digital risiko (NSM, 2021).

2.0 Kontekst

I dag er det få arbeidsplasser som ikke er avhengige av IKT-systemer, og det er så og si ikke mulig å leve et liv uten å være på internett (Bergsjø, Windvik og Øverlier 2020, s. 19). Mesteparten av informasjon skjer nå over tekniske plattformer og for at teknologien skal bli stadig bedre, måles og registreres snart alt vi gjør. Teknologi har altså blitt en integrert del av oss, med stor makt over våre liv både på jobb og privat (NOU 2018: 14, s. 23). Med dette utgangspunktet er kompetanse om digital sikkerhet svært nødvendig og viktig for alle. I dette kapittelet vil det bli redegjort for noen viktige bidrag til det vi vet om digital sikkerhet i dag, hvor det vil bli rettet et særlig fokus på NSM sin tilnærming til temaet. NSM fyller rollen som Nasjonal Sikkerhetsmyndighet i henhold til sikkerhetsloven (NOU 2018: 14, s. 27).

Etterretningstjenesten, NSM og PST utgir årlige nasjonale vurderinger som viser hvilke trusler Norge som samfunn står overfor (NOU 2018: 14, s. 21). En stor andel av uønskede hendelser er utilsiktet. Feil og utfall i digitale systemer og tjenester viser seg ofte å skje på grunn av menneskelige feil (NOU 2018: 14, s. 21). I en rapport fra 2019 om det helhetlige digitale risikobildet, fremhever NSM at Norge må møte digitaliseringen vi står overfor på en sikker måte. For å få til dette lanserte Regjeringen i 2019 en nasjonal strategi for digital sikkerhet. I tillegg kom en egen strategi for digital sikkerhetskompetanse med fokus på forskning og utdanning (NSM, 2019, 6). Ny sikkerhetslov og etableringen av Nasjonalt cyberkrimsenter i Kripos skal være med å styrke innsatsen mot digitale trusler (NSM, 2019, s. 9).

Viktige suksessfaktorer for å lykkes med sikkerhetsarbeidet i en organisasjon hevdes å være involvering fra ledelsen, IKT-sikkerhetskompetanse i virksomheten og etablerte styrings- og rapporteringslinjer (NSM, 2020, s. 4). Gjennom Felles Cyberkoordineringssenter (FCKS), ser NSM et samarbeid mellom Etterretningstjenesten, Kripos, PST og NSM, hvordan norske virksomheter blir utsatt for mange typer digitale operasjoner. Eksempler er etterretning, kartlegging, eller svindel- og utpressingsforsøk som kryptomining og løsepengevirus. I tillegg blir intetanende, norske virksomheter kompromittert og brukt som del av komplekse infrastrukturer i operasjoner mot mål helt andre steder i verden (NSM, 2019, s. 15).

«Ofte er det vi mennesker som er sårbarheten som blir utnyttet»

(NSM, 2019, s. 16)

Oppsummert kan vi si at teknologiutviklingen bidrar til økt sikkerhet, men utviklingen introduserer også sårbarheter. Det mest utfordrende med teknologien vi står overfor er å vite hvor sårbarhetene er, og om verdiene er tilstrekkelig sikret mot ønskede digitale hendelser (NOU 2018: 14, s. 22). Det er vi mennesker som utvikler, setter opp, bruker og vedlikeholder datamaskiner og tjenester og dette vet også trusselaktørene å utnytte (NSM, 2019, s.18).

3. Teori

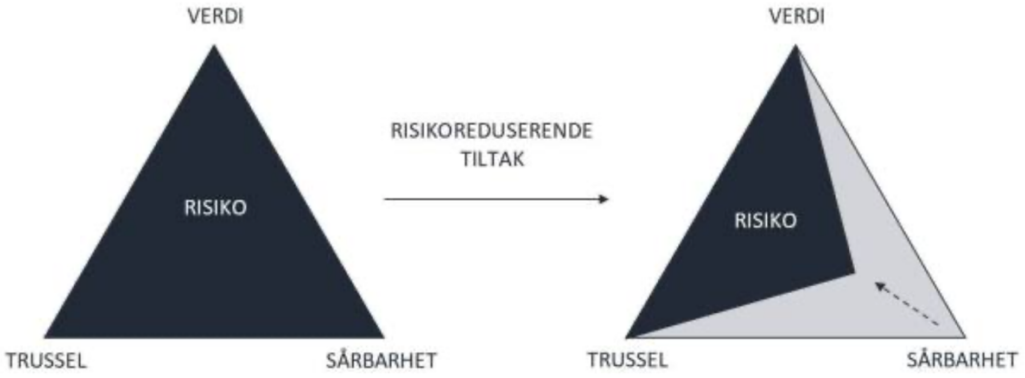
Ny teknologi og samfunnsutvikling har endret risikobildet for alle organisasjoner. På nesten alle felt går utviklingen i retning teknologisk kompliserte produkter og komponenter, og dette øker faren for utilsiktede og store katastrofer (Karlsen 2010, s. 88). De siste tiårene har det vært en betydelig interesse for sammenhengene mellom kultur, sårbarhet og sikkerhet i organisasjoner (Engen et al 2016, s. 156; Westrum 1993; Guldenmund 2000; Antonsen 2009; Kringen 2009). Med bakgrunn i NorSIS metodikk vil jeg i dette teorikapittelet forsøke å beskrive hva digital sikkerhet er, samt hvordan vi kan beskrive og kartlegge en digital sikkerhetskultur.

3.1 Sikkerhet, sårbarhet og effektive barrierer

Innledningsvis er det av betydning å si noe om hva vi legger i begrepet sikkerhet, da dette begrepet kan ha bred betydning. Sikkerhet kan defineres som en tilstand uten noen uønskede hendelser, frykt og fare. Begrepet brukes også om tiltak som bidrar mot denne tilstanden (Bergsjø, Windvik og Øverlier, 2020, s. 19). Ifølge Jore (2017, s. 3) kan vi i Norge skille mellom de engelske ordene "safety" og "security" som begge belyser viktige sider ved sikkerhet. "Safety" er et begrep som brukes for å beskrive sikkerhet mot uønskede hendelser som et resultat av noe tilfeldig som for eksempel tekniske feil eller uhell. "Security" er på den andre siden et begrep som brukes for å beskrive sikkerhet mot uønskede hendelser som et resultat av en tilsiktet handling (NOU 2000: 24; Jore, 2017, s. 3). I denne studien vil begrepet sikkerhet bli brukt med betydningen "safety" fordi det i denne oppgaven vil være mest fokus på hvordan virksomheter kan opprettholde og utvikle en robust digital sikkerhetskultur, mot tekniske feil eller mot andre digitale uhell. Tilsiktet digital kriminalitet vil også bli nevnt for å belyse viktige aspekter, fordi det vil være relevant å inkludere for å besvare oppgavens problemstilling, men vil ikke være et hovedfokus.

Norsk Standard (2012) definerer risiko som «forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifikke trusselen». Ut fra denne definisjonen kan vi med andre ord si at risiko kan ses på som en kombinasjon av trussel, sårbarhet og verdi. Det endrede trusselbilde som presenterer oss for nye sårbarheter er en betydelig stor risiko for bank – og forsikringsbransjen ettersom det digitale domenet kan by på uventede konsekvenser (Engen et al, 2016). Risikoen som det henvises til i denne oppgaven er risiko for tilsiktede

digitale angrep eller eventuelle utilsiktede digitale uhell. Vi snakker altså om risikoen for at informasjons- og kommunikasjonsteknologi og tilhørende systemer, infrastrukturer og prosesser blir utsatt for uønskede hendelser med ulikt konsekvenspotensial, eller at teknologien blir for komplisert for personer som ikke jobber med teknologi og sikkerhet til daglig.



Figur 1. Risikotrekanten

En slik prosess som vi kan se på risikotrekanten overfor handler om å identifisere egen risiko gjennom en kartlegging av egne verdier, kartlegging av hvem som har evne og vilje til å påvirke verdiene, samt identifisering av mangler og svakheter i egen sikkerhet som kan utnyttes (Norsk Standard, 2014). Verdier i denne sammenheng kan være bygninger, servere, mennesker eller kompetanse, alt ut fra det organisasjonen har av ressurser som den bryr seg om. I denne studien henvises det særlig til to verdier man ønsker å beskytte; data/informasjon og mennesker.

Sårbarhet kan beskrives som systemets manglende kapasitet til å stå imot en uønsket hendelse, samt systemets evne til å håndtere hendelsen, om den skulle inntreffe (Njå et al, 2020, s. 52). Noen systemer bringes lett i ubalanse og mangler samtidig interne korrigeringstiltak for å rette opp forstyrrelsene (Karlsen 2010, s. 81). Sårbarheten som undersøkes i denne oppgaven er digital sårbarhet gjennom avhengigheter, tilgjengelighet og integritet. Sårbarheten handler med andre ord om alt som er koblet til, eller er avhengig av informasjons- og kommunikasjonsteknologi. Det inkluderer ulike former for sikringstiltak, både tekniske, organisatoriske og administrative, for å sikre system og informasjon (Justis- og beredskapsdepartementet, 2017). Videre handler sårbarheten om de menneskene som bruker teknologi daglig, og hvordan disse forstår og vurderer risiko når de utfører sine daglige

arbeidsoppgaver. I all hovedsak handler risikotrekanten om å se sammenhengen mellom verdi, sårbarhet og trusler. På denne måten er man bedre rustet til å sikre de sårbarhetene man identifiserer, minimere risiko for å tape verdi og forhindre at truslene skaper negative konsekvenser for selskapet. Videre handler det om å implementere risikoreduserende tiltak og barrierer for å unngå at uønskede hendelser utvikler seg og gir store konsekvenser.

Vi kan betrakte teknologisk sårbarhet som en eller flere egenskaper ved systemet som gjør at det mangler evnen til å gjenopprette funksjonaliteten hvis den blir utsatt for påkjenninger (Engen et al 2019, s. 47). Man kan derfor si at sårbarhet er knyttet til mulig tap av verdi hvis et system ikke er redundant nok, samt har effektive barrierer eller sikringstiltak til å håndtere mulige feil (Aven 2006, s. 13; NOU 1986:12). Det motsatte av sårbarhet er robusthet som er et begrep nært knyttet til begreper som tilpasning, fleksibilitet og resiliens (Engen et al., 2019, s. 48). Begrepet robusthet brukes for systemer som klarer å justere den interne prosessen etter at de er i ubalanse fra omgivelsenes press. De makter altså å gjenvinne sin kapasitet og utføre sine normale funksjoner til tross for påkjenninger de ikke opprinnelig er konstruert for (Karlsen 2010, s. 81). Felles for disse begrepene er at de beskriver hvordan effektive barrierer eller beredskapssystemer kan håndtere eventuelle feil som skulle inntreffe (Aven, 2006, s. 13).

Informasjonsteknologien i dag når stadig nye grenser når det gjelder anvendelsesmuligheter og bruksområder og påvirker på denne måten vår hverdag - både på godt og vondt. «Det elektroniske samfunn» har sine åpenbare fordeler, men kan også ha sin pris (Daler m fl. 2010, s. 30). Økt kompetanse, økt bevissthet og en god digital sikkerhetskultur blant de ansatte, sammen med enkle fornuftige regler, retningslinjer og sikringstiltak vil både kunne redusere sårbarheten, redusere antall feil og dermed også bidra til konkurransekraft i virksomhetene i betydelig grad (Daler m.fl. 2010, s. 30).

3.2 En robust sikkerhetskultur

Kultur er et komplekst begrep som helt enkelt kan defineres som det fellesskap av ideer, verdier, normer og holdninger som en gruppe menneske deler, og som de prøver å overføre til den neste generasjonen (Schein 1987; Bergsjø, Windvik og Øverlier 2020, s. 34). Kulturer former oss, både hvordan vi er som gruppe og hvordan vi som individer opptrer basert på våre underliggende antakelser og verdier. I kulturen ligger det hva man anser som normalt eller unormalt, trygt eller utrygt, og rasjonelt eller irrasjonelt (Bergsjø, Windvik og Øverlier 2020, s.

34). En kultur blir altså et system av delte verdier, meninger og handlingsmønstre som sier noe om «hvordan vi gjør ting her hos oss». Med Peter Druckers kjente utsagn: *"*Culture eats strategy for breakfast*"*, kan vi forstå at det er vanskelig å endre en kultur, om det skulle være av strategiske eller sikkerhetsmessige grunner (Hennestad 2015). Det kjente sitatet sier noe om at selv om sikkerhetsarbeidet er forankret i mål og strategier, og man har ressurser til å gjennomføre, er det likevel stor sannsynlighet for at en for sterk kultur kan hindre bedriften i å lykkes (Jacobsen og Thorsvik 2019).

Turners "Manmade Disasters" teori fra 1976 kan være relevant å trekke inn når vi snakker om kultur. Teorien sier noe om hvordan antakelser og normer styrer den kollektive oppmerksomheten og atferd knyttet til risiko og sikkerhet i organisasjoner. Det kan ifølge Turner eksistere et grunnleggende og ofte langvarig avvik mellom kulturelle antakelser og det som faktisk foregår (Engen et al 2016, s.157). Kultur kan med andre ord forme en slags «blindhet» for farer og trusler, og kultur er derfor et sentralt begrep når det gjelder organisasjoners sårbarhet og årsak til feilkilder.

En sikkerhetskultur bidrar til at virksomhetens sikkerhetstiltak ivaretas av medarbeiderne. Når de ansatte i en organisasjon vet hva som er forventet av dem og har en forståelse for hvorfor sikkerhetstiltak eksisterer, vil de også kunne bli mer bevisst over, og sørge for å melde fra om sikkerhetsmessige forhold som virksomheten bør vite om (NSM, 2019, s. 19). Derfor er det også viktig at ledere kjenner til sikkerhetskulturen i egen virksomhet. Dette for å kunne forstå hvordan medarbeiderne forholder seg til digitaliseringen og digitale trusler. Lederne ønsker at de ansatte skal være motstandsdyktige mot slike trusler, samtidig som de gjør sikre valg når de bruker virksomhetens datasystemer (Nettvett, 2020).

I teorier om organisasjoner er kultur framhevet som en av faktorene som bidrar til pålitelighet og sikkerhet (Weick 1987; Reason 1997; Weick og Sutcliffe 2007; Roe og Schulman 2008). Engen et al (2016) belyser derfor spørsmålet om kulturen er et premiss for systemets sårbarhet og kan øke risikoen for ulykker eller om den er en del av løsningen. Eller om den eventuelt er begge deler på samme tid (Engen et al 2016, s. 157). For de aller fleste virksomheter er slurv, manglende eller dårlig kunnskap og for dårlig kontroll med kvaliteten på produkter og tjenester den største trusselen mot en stabil og trygg informasjonsbehandling. God informasjonssikkerhet, og derav en god sikkerhetskultur er med andre ord i stor grad avhengig av en motivert ledelse og sikkerhetsbevisste medarbeidere (Daler m.fl. 2010, s. 34).

Informasjonssikkerhet handler om at informasjonen ikke blir kjent eller endret av uvedkommende, og at informasjonen er tilgjengelig ved autoriserte behov (Datatilsynet, 2021). En god sikkerhetskultur bidrar til informasjonssikkerhet (Bergsjø, Windvik og Øverlier, 2020, s. 18).

3.3 Hvorfor bør ledere bry seg om å investere i sikkerhet?

Studier viser at lederens forpliktelse til sikkerhetsmål er den viktigste faktoren som skiller trygge fra usikre systemer og selskaper. Dårlig beslutningstaking fra ledelsen kan underminere ethvert forsøk på å forbedre organisasjonens sikkerhet, og bidrar til at ulykker eller katastrofer forekommer (Leveson 2011, s. 415). Leveson (2011) understreker videre viktigheten av at ledere investerer i sikkerhet med at investering i sikkerhet lønner seg og gir stor avkastning for en organisasjon over tid. Det er også ifølge NSM (2020, s. 4) helt avgjørende at toppledelsen tar eierskap til, og involverer seg i sikkerhetsarbeidet i egen virksomhet. Videre kan vi slå fast følgende:

«Virksomhetens leder har ansvaret for å påse at regelverket overholdes og skal sørge for at krav til sikkerhet innarbeides i avtaler med partnere, leverandører og andre det utveksles informasjon med» (Daler m.fl. 2010, s. 81).

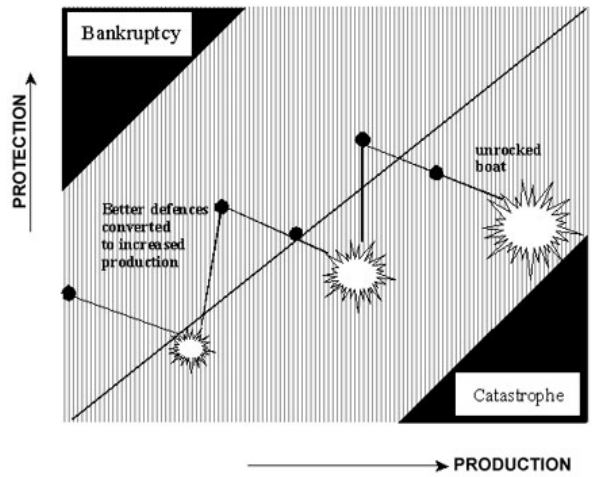
De fleste ledere bryr seg om sikkerhet, men problemene oppstår gjerne på grunn av en feilaktig forståelse av hva som kreves for å oppnå høye sikkerhetsnivåer og hva kostnadene er hvis sikkerhetsarbeidet gjøres riktig. Mange virksomheter fokuserer bevisst på å forbedre sikkerheten gjennom å modernisere, automatisere og profesjonalisere sine IKT- porteføljer, men fortsatt er det slik at hendelser kunne vært avverget eller fått mindre konsekvenser dersom virksomhetene jobbet mer strukturert og helhetlig med digital sikkerhet (NSM 2019, s.9).

Sikkerhet trenger ikke, ifølge Leveson (2011, s. 416), å medføre store økonomiske kostnader. God digital sikkerhet er et resultat av langsiktig, kontinuerlig og strukturert arbeid. Verdivurderinger og risikovurderinger må gjennomføres og digital sikkerhet må inn i alle prosesser og strategier (NSM, 2019, s. 13). Et styrings- eller ledelsessystem for digital sikkerhet er noe av det viktigste en virksomhet kan innføre for å forbedre sikkerheten både i møte med tilsiktede og utilsiktede handlinger (NSM, 2019, s. 13).

3.4 Balansen mellom produksjon og sikkerhet

Sikkerhet og produksjon er ofte viktig å balansere, men dette er ikke alltid like enkelt. «Det er lett å glemme å være redd for ting som sjelden skjer» (Reason, 1997, s.6, egen oversettelse). Sitatet er noe av kjernen i det James Reason kaller "the unrocked boat". Teorien er mest brukt for å forklare organisatoriske ulykker som er sjeldne, men med katastrofale konsekvenser, gjerne på skip eller store plattformer. Teorien er ikke ment i sammenheng med digital sikkerhet, da teknologi i 1997 ikke var sentralt for arbeidsmarkedet. Likevel kan man benytte modellen i sammenheng med digital sikkerhet, da samme prinsippet gjør seg gjeldene; Hvis man ikke opplever ulykker over lang tid, vil man gjerne glemme å arbeide med sikkerheten i organisasjonen, samtidig som man ikke velger å investere i ny sikkerhet. Når en større uønsket hendelse da skjer, velter båten og man har gjerne for lite sikkerhet til å hindre at en katastrofe skjer.

Balansen mellom sikkerhet og produksjon kan ifølge Reason (1997, s. 4) forklares med det faktum at det ideelle for en organisasjon ville være å balansere operasjoner i det som kalles "paritetssonen". Her vil farene ved produksjonen bli møtt med tilstrekkelig sikkerhet. Jo mer omfattende produksjonen er, desto høyere bør sikkerheten være. Hvis sikkerheten overstiger produksjonen, vil organisasjonen sannsynligvis gå konkurs. Dette vil skje fordi det å investere i sikkerhet vil være så dyrt at man ikke vil produsere nok til å dekke kostnadene igjen. På den annen side kan for lite investering i sikkerhet føre til en eventuell katastrofe som også kan gjøre at organisasjonen går konkurs. Det er vanlig at fokus i en organisasjon vil være i hovedsak på produksjon, men alle rasjonelle aktører vil ifølge Reason, 1997, s. 4) akseptere behovet for en viss sikkerhet.



Figur 2. Unrocked boat av Reason (1997, s.4).

Et hovedpoeng bør ifølge Daler (2010, s.42) være å forsikre objekter som kan gjenskaffes for penger og å sikre mest mulig forsvarlig de systemer og verdier som ikke kan kjøpes igjen. Dilemmaet mellom sikkerhet og produksjon er at man noen ganger tar snarveier til sikkerhet slik at man kan nå frister og operasjonelle krav (Reason, 1997, s.4). På denne måten kan sikkerhetstiltak både ha både positive og negative konsekvenser. Problemet blir da om man skal innføre tiltaket og muligens la det gå utover produksjonen, eller om man skal avstå fra å innføre det og kanskje la det gå utover sikkerhet.

Når teknologien og samfunnet endres, endres også årsakene til ulykkenes natur og organisasjoners systemsikkerhetsteknikk holder ikke tritt med teknologiens raske utvikling. Spesielt digital teknologi har skapt en stille revolusjon på de fleste felt. Mange av tilnærmingene som tidligere fungerte for å beskytte mot systemfeil i en organisasjon som Reason (1997) belyser, er ineffektive i å kontrollere ulykker som oppstår ved bruk av digitale systemer og programvare (Leveson 2011, s. 3).

Ifølge Leveson (2011, s.416) er det en klassisk myte at sikkerhet er i konflikt med å oppnå andre mål og at kompromisser er nødvendig for å forhindre tap. Sikkerhet er nødvendig for å oppnå de fleste organisatoriske mål, inkludert fortjeneste og videreført eksistens (Leveson 2011, s. 416). Det finnes mange eksempler på store ulykker som fører til enorme økonomiske tap og at selskaper går konkurs som et resultat av disse hendelsene. Etter mange eksempler med katastrofer, synes Leveson (2011, s.416) at det er overraskende at få organisasjoner ser ut til å lære av disse hendelsene og se nærmere på sine egne sårbarheter. Hun hevder at det gjerne ikke handler om mangel på innsats og ressurser hos ledelsen, men at det kan handle om hvordan innsatsfaktorene og ressursene blir brukt. Kostnadene til sikringstiltak må imidlertid stå i forhold til verdien av de IT-systemene og den informasjonen som skal sikres (Daler m.fl. 2010, s. 41). Det kan være vanskelig å vurdere hvilken verdi IT-systemene og informasjonen representerer, men en risikoanalyse[1] vil kunne være til hjelp for å få satt verdi på de ulike faktorene.

[1] Det vil ikke bli laget en egen risikoanalyse, men nevnes for å belyse viktigheten av en ROS-analyse i arbeidet med digital sikkerhet.

3.5 Kompleksitet i systemer

Kompleksitet kommer i mange former. Driften av kompleksitet er noen ganger så komplisert at det trosser forståelsen til alle, bortsett fra noen få eksperter (Leveson, 2011, s.4). Problemet kan være at vi bygger systemer som er utover vår evne til å intellektuelt klare seg. Med andre ord vil økt kompleksitet av alle typer gjøre det vanskelig for designere å vurdere alle potensielle systemtilstander eller for operatører å håndtere normale og unormale situasjoner trygt og effektivt. Faktisk kan kompleksitet ifølge Leveson (2011, s.4) defineres som intellektuell uhåndterlig.

Mennesker deler stadig mer kontroll over systemer med automatisering og dette medfører nye typer menneskelige feil, som for eksempel ulike typer modusforvirring. Den nye kommunikasjonen mellom mennesker og maskiner blir en økende faktor i ulykker (Leveson 2011, s.5). Leveson (2011, s.5) påpeker viktigheten av å se nærmere på at all menneskelig atferd er påvirket av konteksten det skjer i. Mange nylige ulykker som har fått skylden for operatørfeil, kan mer nøyaktig merkes som følge av feil i miljøet der de opererer (Leveson 2011, 5). Derfor kan det tenkes at disse ønskede hendelsene ha sammenheng med svakheter i organisasjonens digitale sikkerhetskultur.

3.6 Dimensjoner for en digital sikkerhetskultur

Digital sikkerhet handler om å beskytte digitale verdier fra ulike former for trusler som rettes mot interne sårbarheter i selskapet. Digital sikkerhetskultur kan dermed forstås som de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til digitale verdier (Bergsjø, Windvik og Øverlier, 2020, s. 36). For å gjøre det mest oversiktlig bruker jeg i dette kapittelet digital sikkerhet synonymt med begrepet datasikkerhet. Mange organisasjoner tenker på hva folk gjør eller tidligere har gjort når de setter søkelys på atferd og sikkerhet. Dette sier noe om et bilde av sikkerhet fra fortiden, men sier imidlertid lite om hva som kommer til å skje i fremtiden. Sikkerheten må være i forkant, og virke forebyggende og derfor er ikke tidligere atferd den beste indikatoren på dette (Bergsjø, Windvik og Øverlier, 2020, s. 36). Derfor retter vi heller fokuset på holdninger, verdier og følelser som kan si noe om hva folk vil gjøre eller reagere i kommende situasjoner, for å kunne predikere fremtiden og dermed tenke sikkerhet i forkant.

En virksomhets digitale sikkerhetskultur kan ifølge NorSIS (2016) beskrives ved hjelp av åtte nøkkelkomponenter eller dimensjoner (Malmedal & Røislien, 2016).

1) Fellesskap
2) Styring og kontroll
3) Tillit
4) Risikoforståelse
5) Vilje til digitalisering/optimisme
6) Kompetanse
7) Interesse for IT og teknologi
8) Atferdsmønstre

Figur 3. Åtte nøkkelkomponenter for en digital sikkerhetskultur

3.6.1 Felleskap

Kulturer formes som nevnt av individer som inngår i et felleskap. Samtidig vil kulturen forme individene som er en del av den. «Sikkerhet er alles ansvar» må ikke bare være et tomt slagord, men implementeres som en del av organisasjonskulturen (Leveson, 2011, s. 402). Ifølge integreringsperspektivet av Jacobsen & Thorsvik (2019) virker kulturen i organisasjonen integrerende på samtlige medlemmer, hvor organisasjonen beskrives som et kulturelt fellesskap basert på felles konsensus. Ettersom organisasjonsstruktur i stor grad bestemmer hvem som skal samhandle, vil den også sterkt prege og legge føringer for kulturen(e) som vokser frem (Jacobsen & Thorvik 2019). Noen kulturer er mer individualistiske, mens andre kulturer er mer orientert mot felleskapets behov der man setter sine egne behov til side til fordel for felleskapet. I denne sammenhengen kan det bety at enkelte følger regler som ivaretar sikkerheten til virksomheten som helhet, selv om det kan gå utover noen enkelte personer. Et annet eksempel kan være at den enkelte velger å stå frem når de har gjort en sikkerhetstabbe slik at fellesskapet kan lære av det, selv om det er belastende for vedkommende (Bergsjø, Windvik og Øverlier, 2020, s. 37). Her handler det ifølge NorSIS (2016) om å se på fellesskap som et av kjerneområdene, hvor man primært fokuserer på hvordan individet forholdet seg til fellesskapet, og om individet opplever seg selv som en del av et større «digitalt fellesskap» (Bergsjø, Windvik og Øverlier, 2020, s. 37).

3.6.2 Styring og kontroll

Styring og kontroll relaterer seg til felleskap; «Hvordan skal fellesskapet reguleres og av hvem?». Sikkerhet starter ifølge Leveson (2011, s.177) med en klar ledelse og engasjement, og uten disse hevder hun at organisasjonen er dømt til å mislykkes. Ledelse skaper kultur, og kulturen driver fellesskap og atferd (Leveson 2011, s.177). Foruten å sette kulturen gjennom sin egen atferd, må ledere etablere sikkerhetspolitikken og opprettholde en sikkerhetskontrollstruktur hvor ansvarlighet, autoritet og tilbakemeldingskanaler er viktige elementer. Ledelsen må også etablere sikkerhetsstyringsplan og sikre at et sikkerhetsinformasjonssystem og kontinuerlige lærings – og forbedringsprosesser er på plass og er effektive (Leveson 2011, s.177). Her er det hensiktsmessig å høre på hva felleskapet mener bør reguleres og forsøke å finne en balanse mellom styring og kontroll for å sikre virksomheten mot uønskede hendelser, samt den enkeltes behov for privatliv. Et viktig spørsmål blir hvor mye overvåkning, styring og kontroll som er akseptabelt når både felleskapets og den enkeltes sikkerhet og trygghet står på spill (Bergsjø, Windvik og Øverlier, 2020, s. 38).

3.6.3 Tillit

I en virksomhet er man avhengig av tillit mellom menneskene som jobber i organisasjonen og mellom menneskene og systemene for å oppnå effektiv drift. De fleste aksepterer at det finnes systemer på jobb som logger en del av aktiviteten i løpet av dagen, men man stoler som regel på at denne informasjonen ikke blir utnyttet (Nettvett, 2020). En virksomhet lagrer også mye informasjon om de ansatte og potensielt mye informasjon om andre interessenter som f.eks. kunder og leverandører. Hvor stor grad av tillit man har til systemene og menneskene i det digitale livet har stor betydning for hvordan man velger å handle i ulike situasjoner. Noe Leveson (2011, s.405) ønsker å gjøre flere oppmerksom på er at tillit er vanskelig å få og lett å miste. Når tilliten er tapt, er det enda vanskeligere å få tillit igjen. Digitaliseringen er både avhengig av, og sårbar for tillit. Både organisasjoner og befolkningen ellers, blir ikke bare oppfordret til å ta i bruk teknologi, de blir i noen tilfeller også tvunget til det (Bergsjø, Windvik og Øverlier, 2020, s. 38). Kommunikasjonen mellom de fleste ledd i alle prosesser skal i dag primært foregå digitalt, og føyer man ikke seg etter denne utviklingen risikerer man å gå glipp av de positive gevinstene med digitaliseringen, og i noen tilfeller også store ulemper.

3.6.4 Risikoforståelse

Kompetanse, læring og risikoforståelse henger sammen (Bergsjø, Windvik og Øverlier, 2020, s. 39). Å sende lenker i en e-post er en vanlig måte å plante ondsinnede koder i datamaskiner

på norske arbeidsplasser. Bare når de ansatte har kunnskap om at dette er mulig, kan forstå at det er en risiko. Det er imidlertid nødvendig å vite noe mer enn at det er mulig, en bør også vite noe om hvor ofte slike ting skjer og hva som kjennetegner en utrygg e-post for at man skal kunne gjøre riktige vurderinger (Bergsjø, Windvik og Øverlier, 2020, s. 39). Risikopersepsjon handler altså om hvordan den enkelte bedømmer risiko for ulike aktiviteter og trusler, i denne sammenhengen digitale trusler. Renn (2008) definerer risikopersepsjon som: "tolkning av fysiske signaler og/eller informasjon om potensielt skadelige hendelser eller aktiviteter, der man danner seg en vurdering av alvor, sannsynlighet og aksept for den respektive hendelsen eller aktiviteten" (Renn, 2008, s. 98, egen oversettelse).

Risikoforståelse eller risikopersepsjon har også subjektive faktorer. Hvordan personer og virksomheter oppfatter risiko varierer. Det kan både være fordi den enkelte har ulike forutsetninger for å bedømme det, og fordi trusselbildet varierer fra virksomhet til virksomhet (NSM, 2019). Risikopersepsjon har gjerne sammenheng med tidligere erfaringer, enten i fellesskapet eller hos den enkelte. Vi vet også fra studier, at alder er en faktor som spiller inn, særlig når vi snakker om forståelse av teknologi (Keuter & Strecher, 1995). Studier viser også at man har høyere toleranse for å ta risiko, jo mer kompetanse man har innenfor et felt (Nettvett, 2020). Det er altså mulig at medarbeidere med mye kunnskap innenfor cyberspace og det digitale domenet, kan overvurdere sin egen evne til å stå imot trusler og derfor ta høyere risiko (Keuter & Strecher, 1995). Hvis man vet noe om risikoforståelsen til de ansatte, kan man lettere lage rutiner og kontrollmekanismer som bedre beskytter både virksomheten og den enkelte (Nettvett, 2020).

3.6.5 Vilje til digitalisering

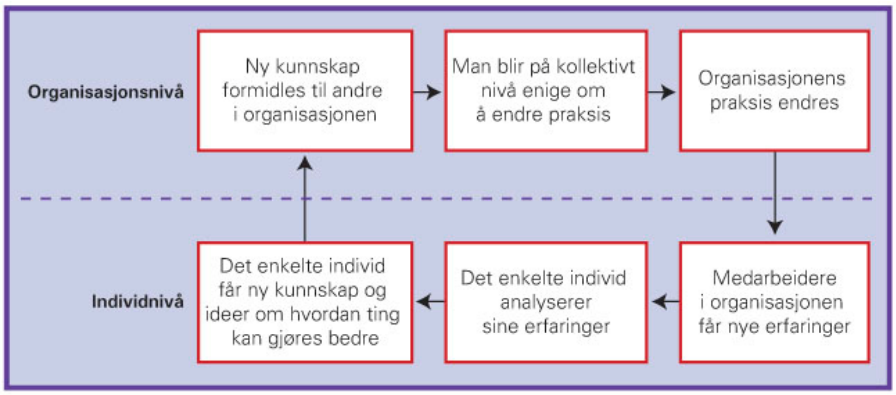
Ifølge NorSIS (2016) påvirker vår holdning til digitalisering måten vi forholder oss til teknologi, fordi en trygg digital innbygger presumptivt er en forutsetning for digitaliseringen nasjonalt. Det vil åpenbart være en forskjell i hvilken innstilling de ansatte har til teknologi og endring. Det vil også være en stor forskjell virksomheter imellom. I en teknologibedrift er det sannsynligvis en høyere andel ansatte med høy kompetanse innen teknologi, sterk vilje til digitalisering og større vilje til å ta risiko, enn i andre bedrifter som ikke er like avhengig av slik teknologi (NSM 2020). Hvordan digitale tjenester utvikles og tilbys, hvordan sikkerheten ivaretas, hvilke sikkerhetshendelser som skjer og hvordan de blir håndtert er faktorer som er med å påvirke holdningene til det digitale, og derav også ens vilje til digitalisering og optimisme for teknologi (Bergsjø, Windvik og Øverlier 2020, s. 40).

Vi som individer er drivere for kontinuerlig endring og utvikling, og ikke passive mottakere av dette. Motstand mot endring og i denne sammenhengen mot ny teknologi kan, og vil likevel mest sannsynlig oppstå, men det kan også være positivt. Motstand mot digitalisering kan være bra for organisasjonen fordi at det er alltid en fare for at teknologien eller en eventuell endring ikke er grundig gjennomtenkt. Diskusjon rundt teknologi kan føre til åpen debatt som gir viktig informasjon og innspill om forhold som ledere gjerne ikke har tenkt over (Jacobsen & Thorsvik, 2019).

3.6.6 Kompetanse

Kompetanse kan forstås som atferd som resulterer i effektiv utførelse av en jobb (Jacobsen & Thorsvik, 2019). Samsvar er et viktig nøkkelord når man snakker om kompetanse, og vi er opptatt av at det må være et samsvar mellom personen og de krav som stilles til en jobb. Kompetanse kan ifølge Linda Lai defineres som: «De samlede kunnskaper, ferdigheter og holdninger som gjør det mulig å utføre aktuelle funksjoner og oppgaver i tråd med definerte krav og mål» (Jacobsen & Thorsvik, 2019). Alle nordmenn må ha et sett med grunnleggende digital kompetanse for at de skal kunne ta del i et moderne samfunn (Bergsjø, Windvik og Øverlier 2020, s. 41).

Kompetanse i forbindelse med digitale trusler er tresidig (Daler m.fl. 2010, s. 407). Den første delen handler om generell kompetanse hos de ansatte. Del 2 handler om ledelsens kompetanse på datasikkerhet og tredje del omfatter kompetanse i selskapet (alle som har sikkerhetsansvar). Virksomheter forventer at de ansatte skal følge reglene, og ikke utsette seg selv eller virksomheten for unødig risiko (Nettvett, 2020). Da kreves det kompetanse og læring. Læring er en prosess der mennesker og organisasjoner tilegner seg ny kunnskap, og endrer sin atferd på grunnlag av denne egenskapen (Jacobsen & Thorsvik, 2019). Virksomheten må sørge for at de ansatte kan det som skal til for at de skal ta de riktige sikkehetsvalgene på jobb, og det må brukes metoder som faktisk motiverer og skaper læring hos de ansatte. For noen er e-læring det riktige, mens for andre passer dilemma-trening eller bruk av ”sikkerhetsambassadører” best.



Figur 4. Organisatorisk læringssløyfe

Figuren er en generell modell for læring som viser at hvis organisatorisk læring skal finne sted, så forutsetter det at de enkelte individer i organisasjonen lærer og at den læringen som foregår på individnivå også spres til andre i organisasjonen. Videre må organisasjonen som et felleskap utvikle tiltak for å løse problemet og iverksetter disse tiltakene. Dette danner en læringsløyfe når individene videre skal vurderer hvor gode eller dårlige organisasjonens løsninger er, og eventuelt starter en ny læringssirkel for ytterligere å forbedre tilstanden (Jacobsen & Thorsvik 2019).

For å kunne forbedre sikkerhetsarbeidet og øke kompetanse om sikkerhet, er det nødvendig å forstå hvordan organisasjoner lærer, og hva organisasjoner lærer. På denne måten kan man skape innsikt i hvordan de ansatte foretrekker å lære, samt hvem de lærer best fra. Det vil gjerne være noen personer eller miljøer som gir større innflytelse på læring enn andre (Bergsjø, Windvik og Øverlier 2020, s. 41), og disse bør identifiseres for mest optimal læring (Jacobsen og Thorsvik, 2019). De man beundrer og lytter til, påvirker felleskapets verdier og holdninger og gjennom dette påvirker de hvilke atferdsmønstre som etableres (Bergsjø, Windvik og Øverlier 2020, s. 41). Det finnes flere aktører man særlig lytter til når det kommer til digital sikkerhet. Det kan være blant annet aktører som NorSIS, Datatilsynet, Nasjonal Sikkerhetsmyndighet eller sikkerhetsavdeling innad i bedriften man jobber i. Det spiller en sentral rolle hvordan og spesielt *hvem* man lærer fra, og hva som anses som «riktig kunnskap». Dette kan ha stor innvirkning på hva man faktisk lærer, og hvor godt rustet man er til å motvirke digitale trusler (Bergsjø, Windvik og Øverlier 2020, s. 41).

Peter Senge hevder at forutsetningen ligger i at det på ledelsesnivå utvikles en bevisst læringsstrategi for hele organisasjonen som er forankret i systemtenkning. En lærende

organisasjon i dette perspektivet er en organisasjon der alle medlemmer tenker på en spesiell måte som kan kalles systemtenkning. Dette er altså i stor grad et kulturelt aspekt ved organisasjonen. Det innebærer at man ser helheten og sammenhenger i egen organisasjon og den situasjon organisasjonen befinner seg i (Jacobsen & Thorsvik, 2019).

3.6.7 Interesser

Det vi er interessert i former vår innstilling, evner og kunnskap. Interessen vår påvirker hvilke mennesker vi søker mot, og hvem vi lærer fra (Nettvett, 2020). Med interesse kommer bevissthet, nysgjerrighet og tid (Jacobsen & Thorsvik 2019). Det er derfor fristende å anta at de som er interessert i teknologi og informasjonssikkerhet har et fortrinn fremfor de som ikke er interessert i dette og ser på det som bortkastet å bruke tid på å lære (Nettvett, 2020). Kunnskap om interesser kan gi ny innsikt i hvilke metoder virksomheten bør bruke for å motivere og lære opp de ansatte. Ved rekruttering kan organisasjonen forsøke å ansette eller leie inn personer som har mål og interesser som faller sammen med dens egne, altså som har et fokus på sikkerhet og digitalisering og dermed bidrar positivt for en robust sikkerhetskultur i organisasjonen (Daler m.fl. 2010, s. 408).

2.6.8 Adferd

Å designe effektive rapporteringssystemer er veldig vanskelig, og spesielt å få medarbeiderne til å bruke disse aktivt. Et effektivt rapporteringssystem krever tydelige retningslinjer på prosedyrer for feilmeldinger, avvik eller andre problemer som dukker opp. Dette inkluderer hvem informasjonen skal sendes til, og hvem som skal være ansvarlige for at problemene rettes opp i og tas hånd om (Leveson 2011, s. 405). I tillegg bør mottak av problemrapport/feilmeldinger resultere i en bekreftelse, spesielt når den primære kommunikasjonskanalen er over nett. Senere, når et problem blir identifisert, bør informasjonen gis videre til reporteren av problemet og hva som ble gjort med det for å vise medarbeiderne at sikkerheten blir tatt hånd om (Leveson 2011, s. 205).

Ifølge Arbeidsmiljøloven skal alle bedrifter ha et rapporteringssystem hvor arbeidstakeren kan varsle om kritikkverdige forhold i virksomheten (Arbeids- og sosialdepartementet, 2014). For å oppnå en god sikkerhetskultur må denne type rapporteringsverktøy være etablert på en god måte. Et effektivt rapporteringssystem krever også at medarbeiderne er overbevist om at informasjonen vil bli brukt til konstruktive forbedringer i sikkerhet, og ikke som grunnlag for kritikk eller disiplinærtiltak (Leveson 2011, s.405). Hvis rapportering anses å ha negative

konsekvenser for reporteren, kan anonymitet være nødvendig. Reason (1997) beskriver en rettferdig kultur «just-culture» som en atmosfære av tillit der mennesker oppmuntres og gjerne også belønnes for å rapportere eller videreføre viktig sikkerhetsrelatert informasjon.

For virksomheten er det viktig å vite om de ansatte følger reglene som er satt, og at de har en adferd som bidrar til at sikkerheten blir ivaretatt. Når en kartlegger sikkerhetsatferden, kan en også få innsikt i om opplæring har hatt ønsket effekt. Hva som er" best-practice" innenfor informasjonssikkerhet endrer seg over tid, så de ansatte må ha jevnlig påfyll av slik kunnskap (Nettvett, 2020). Svært ofte viser det seg at bedragerier, misligheter og sabotasjer utføres av egne ansatte og ofte av medarbeidere i betrodde posisjoner (Daler m.fl. 2010, s. 78). Det kan i disse tilfeller stilles spørsmål til hvorvidt ledelsen har gjort sin plikt med hensyn til å utvikle et godt arbeidsmiljø, ivareta personalressurser og etablere gode kontrollrutiner (Daler m.fl. 2010, s. 79).

4. Metode

I dette kapittelet presenteres de ulike valgene som er gjort i forbindelse med metode og datainnsamling. Med metode menes den planmessige fremgangsmåten for hvordan forskningsprosjektet gjennomføres (Johannessen et al., 2016, s. 95). Hensikten med kapittelet er å skape innsikt metoden brukt i studien, samt vise til viktige refleksjoner vedrørende metodevalg, informanter og de dokumentene som er valgt for å belyse problemstillingen. Jeg kommer også til å si noe om hvilke etiske betraktninger jeg har tatt hensyn til i arbeidet med denne masteroppgaven.

4.1 Valg av metode

Denne studien er basert på problemstillingen og har et eksplorativt design. Ettersom jeg retter blikket mot utfordringer knyttet til digital sikkerhetskultur, ser jeg det mest hensiktsmessig å benytte en kvalitativt orientert metode da det å gå i dybden kan skape et godt grunnlag for å forstå utfordringene organisasjoner står overfor (Askheim og Grenness 2018). Metoden skal på en systematisk måte hjelpe å velge riktig tilnærming til innhenting og analysering av data (Gripsrud, Olsson og Silkoset, 2016). I denne dybdestudien er det derfor valgt å besvare problemstillingen ved hjelp av å se nærmere på seks relevante dokumenter, samt intervjue åtte nøkkelpersoner via en kvalitativt orientert metode.

4.2 Dokumenter og rapporter

De seks dokumentene som blir brukt gjennomgående i denne oppgaven blir viktige funn i empiridelen av oppgaven. Disse har jeg sortert i en tabell for å vise på en oversiktlig måte hvilket fokusområde dokumentet legger vekt på, samt hvilken relevans det har til denne oppgaven. De dokumentene som er valgt ut er sentrale dokumenter i forhold til nasjonale strategier og politikkutforming når det kommer til digital sikkerhet i Norge. Jeg har bevisst valgt å se på utviklingen de siste seks årene for å få med meg om det har skjedd en utvikling på fagområdet. Dokumentene er derfor sortert ut i fra årstall fra 2016 og frem til i dag.

Dokument	**Fokusområde**	**Relevans til oppgaven**
"The Norwegian Cybersecurity Culture" (NorSIS, 2016)	Åtte nøkkeldimensjoner for å beskrive digital sikkerhetskultur på et generelt plan.	Sentrale for å beskrive hvordan organisasjoner imøtekommer disse og dermed hvordan de legger til rette for en digital sikkerhetskultur innad i organisasjonen.

Meld. St. 38 (2016-2017) «IKT-sikkerhet: et felles ansvar».	Stortingsmelding som la føringer for digital sikkerhet i Norge. Legger grunnlag for forventninger knyttet til handlinger rundt digital sikkerhet.	Bidrar til forståelse rundt det at digital sikkerhet er et felles ansvar for alle.
«IKT-sikkerhet i alle ledd» (NOU: 2018).	Organisering og regulering av nasjonal IKT-sikkerhet. Et særlig fokus på lover og forskrifter som stiller krav om IKT-sikkerhet.	Veiledning for hvordan organisasjoner kan sikre sine informasjonssystemer på en trygg måte.
«Nasjonal strategi for digital sikkerhet» (Departementet, 2019)	Helhetlig tilnærming til digitaliseringen i det norske samfunn	Strategien som legges frem i denne rapporten bidrar til at privatpersoner og organisasjoner får nødvendig kunnskap og risikoforståelse for å kunne ta i bruk teknologi på en trygg måte.
«NSMs grunnprinsipper for IKT-sikkerhet» (NSM, 2020)	Prinsipper og anbefalinger for hvordan virksomheter skal beskytte sine informasjonssystemer og sikre verdier mot digitale trusler.	Benyttes i oppgaven som generelle anbefalinger rundt bruk av IKT-systemer.
«Nasjonalt digitalt risikobilde» (NSM, 2021)	Rapporten tar opp problemstillinger knyttet til samfunnssikkerhet og individsikkerhet innenfor det digitale domenet.	Øker bevissthet rundt digital sikkerhet, samt motivere til sikrere bruk av digital sikkerhet i fremtiden.

Tabell 1. Relevante documenter og rapporter

4.3 Kvalitativt orientert metode

Argumenter for en kvalitativ orientert tilnærming er at jeg vil forstå mer om samspillet mellom mennesker og teknologi, samt gå i dybden på sammenhenger eller motsetninger som kommer frem. En fordel med denne metoden er at man får være til stede med informantene, og stille relevante spørsmål som gir meg økt innsikt i rutiner og forståelse rundt sikkerhetsarbeidet. Tanken bak intervjuene var å skape en viss oversikt over hvilken risikoforståelse de ansatte har overfor trygg nettbruk. Denne delen av intervjuguiden var lik for ledere og medarbeidere og i form av at informanten skulle forsøke å rangere noen påstander på en skala fra 1-5 når det kommer til trygg nettbruk, trusler og hvilken risiko de forbinder med bruk av teknologi på jobb.

Videre i intervjuet undersøkes hvilke rutiner som er etablert for digital sikkerhet og i denne sammenhengen stilles det spørsmål for å få informantene til å snakke mer fritt. Her var det også spørsmål om hvilke endringer som er innført som et resultat av eventuelle tidligere hendelser.

Spørsmålene til medarbeidere og ledere var relativt like, men hos lederne ble det rettet et ekstra fokus på hva de selv har gjort for å bidra til bedre digital sikkerhet internt.
Avslutningsvis ble det stilt spørsmål om deres forståelse av eventuelle trusler teknologien kan ha for organisasjonens verdier og om man forstår omfanget av dette. Ved å undersøke disse delene nærmere vil jeg totalt sett kunne fange opp relevante aspekter, som gir meg et troverdig diskusjons – og beslutningsgrunnlag for å diskutere problemstillingen om utfordringer ved en digital sikkerhetskultur innenfor bank- og forsikringsbransjen.

4.3.1 Strategisk utvelgelse av informanter

Utvalget av informanter til studiet skal reflektere det jeg faktisk ønsker å finne svar på og derfor ser jeg det hensiktsmessig å velge enheter som hjelper meg å forstå, og finne svar på problemstillingen på best mulig måte. Jeg benyttet meg i denne studien derfor av en strategisk utvelgelse av informanter hvor jeg spesifikt valgte informanter som ikke direkte har erfaring med sikkerhetsarbeid. Det kunne ha vært en fordel og skapt mer dybde i studien å ha én eller to informanter som jobber innenfor sikkerhetsavdelingen innen denne bransjen, men det var en utfordring å få noen av disse til å delta på undersøkelsen selv om jeg kom i kontakt med disse. Likevel vil hensikten med undersøkelsen være å skape en dypere innsikt i hvordan sikkerhetskulturen faktisk er, noe jeg får svar på gjennom de 7 informantene jeg har som jobber innenfor ulike roller i bank – og forsikring. Utgangspunktet for undersøkelsen er altså hensiktsmessighet og dypere forståelse av den digitale sikkerhetskulturen i organisasjonene (Johannessen, Tufte og Christoffersen, 2016).

Et bevisst valg er tatt når det kommer til valg av informanter fra flere ulike organisasjoner innenfor bank – og forsikring. Ene grunnen for å inkludere flere selskaper er for å sikre total anonymitet for hvert enkelt selskap og ingen mulighet for å spore hvor informasjonen kommer fra. Dette av hensyn til at den type informasjon som blir samlet inn kan være sensitiv og noe organisasjonene ikke ønsker skal komme på avveie. Videre er det interessant å inkludere flere selskaper for å få innblikk i om det er noen forskjell mellom bank og forsikring, selv om ikke det er et mål i seg selv med sammenligning i denne studien.

4.3.2 Semistrukturert intervju

Jeg så det mest hensiktsmessig å benytte en semistrukturert tilnærming på intervju, hvor det stilles spørsmål i en fast rekkefølge, ut fra en intervjuguide som utformes på forhånd (se vedlegg

2). Her kommer det gjerne innslag av oppfølgingsspørsmål til intervjuobjektet, noe som kan gi meg interessante vinklinger rundt det som blir spurt om (Askheim og Grenness, 2018). Det er altså et planlagt og fleksibelt intervju, hvor målet var å få intervjuobjektet til å snakke mest mulig på egne premisser, samtidig som man har en viss retning på intervjuet (Krumsvik, 2015). På denne måten er det lettere å kunne fortolke, kategorisere og analysere dataen i ettertid, da intervjuobjektet ikke får frie tøyler til å trekke tråder til helt andre temaer, men man holder seg innenfor en gitt ramme.

Det er blitt gjennomført 2 intervjuer ved fysisk oppmøte og 6 intervjuer over Teams. Intervjuene tok alt fra 30 til 35 minutter, bestående av en liten introduksjon på 5 minutter, og selve intervjuet som tok rundt 25-30 minutter.

4.4 Koding og behandling av data

De seks dokumentene ble sendt til et grafisk trykkeri for å sette de sammen i et kompendium. Dette for å få dokumentene på papir for å kunne markere hva som anses som særlig viktig å ha med som funn.

Rangeringen fra de syv informantene sorterte jeg i et skjema for å skape en oversikt over forskjeller og likheter mellom informantene. Videre var det hensiksmessig å sortere disse etter farge etter prinsippet til trafikklysmodellen for å gjøre det ryddig og oversiktlig å sammenstille svarene til syv informanter. Der er grønt noe man ikke trenger å bekymre seg for, gult noe man trenger å være varsom for, og rødt noe man trenger å gjøre noe med. Disse nyansene viser hvordan de ulike informantene tenker i forhold til hverandre. Disse er beskrevet nærmere i empiriske funn i del 4.1 av oppgaven.

Ettersom jeg fikk godkjent å ta lydopptak av NSD, ble også intervjuene transkribert i ettertid for å få en mest mulig korrekt gjengivelse av intervjuet. Jeg gjennomførte transkriberingen kort tid etter at intervjuet var avholdt for å huske mest mulig kontekst, samt å ha intervjuet friskt i minnet. Transriberte intervjuer ble deretter printet ut på papir og markert i ulike fargekoder ut fra hvilket tema og forskningsspørsmål som informasjonen ga meg kunnskap om. Dette ga oversikt over hvor funnet hørte hjemme, og hvilke utsagn fra dokumentene som underbygget eller sto i kontrast til det som ble nevnt. Jeg sørget for at kodene var tett forankret i empirien, empirinære koder, hvor kodene er utviklet fra dataen jeg har innsamlet (Tjora 2020). Videre fokuserte jeg på om det var noen av informantenes utsagn som stakk seg

ut i mengden og som jeg kunne sette «merkelapper» på. Dette bidro til å få frem interessante aspekter som kunne brukes til å belyse forskningsspørsmålene.

Jeg valgte å basere kodingen på begreper som allerede fantes i datamaterialet, fremfor å oppsummere hvert avsnitt slik man gjør ved sorteringsbasert koding (Tjora 2020). Fordelen med empirinære koder er at kodene ligger tett på deltakernes eksakte utsagn, som gjør det mulig for meg å ivareta hva informanten faktisk sier i detalj slik at det informanten sier blir oppfattet slik informanten har tenkt (Tjora 2020). Å ligge tett på empirisk materiale er viktig for å ikke fatte forhastede konklusjoner basert på min egen forforståelse for temaet.

4.5 Validitet og reliabilitet

For å sikre validitet og sikre at jeg måler det jeg faktisk har til hensikt å måle, har jeg foretatt et pilotintervju på en person som jobber i bank – og forsikringsbransjen. Vedkommende er en person jeg kjenner godt og ikke har med i studien, men på denne måten kunne jeg få en tilbakemelding på hvor forståelig spørsmålene er. Her var jeg spesielt opptatt av om jeg brukte for krevende fagbegreper eller om spørsmålene forstås slik de er ment. Under pilotintervjuet var også en medstudent til stede for å kunne observere min intervjuteknikk, slik at hun kunne gi meg konstruktive tilbakemeldinger om hva jeg bør gjøre annerledes eller hva som fungerte særlig godt. Tilbakemeldingene brukte jeg for å optimalisere og korrigere intervjuguiden. Validitet handler altså om hvor godt man måler det som man har til hensikt å måle, og sees på som undersøkelsens gyldighet (Gripsrud, Olsson & Silkoset 2017, 61).

Reliabilitet dreier seg om i hvilken grad man kan stole på at resultatene er pålitelige. Dette betyr at tilfeldige feil må være minst mulig, for at undersøkelsen skal være reliabel (Gripsrud, Olsson & Silkoset 2017, 61). For å sikre pålitelighet ved studien er mitt eget kritiske syn å betrakte som et viktig instrument for å sikre at man er objektiv i studien. For å ivareta objektivitet valgte jeg ut organisasjoner jeg ikke har noe personlig forhold til, og en bransje jeg ikke har jobbet i selv. Videre gjorde jeg meg selv bevisst på mine egne oppfatninger som kunne danne en forforståelse for svarene jeg kunne få, slik at jeg ikke skulle se forbi viktige funn basert på min forforståelse av temaet. Selv om jeg tok flere forhåndsregler for å sikre pålitelighet i studien, er det likevel slik at i prosessen fra empiri til analyse at resultatene kan bli preget av mitt engasjement for undersøkelsen. Videre gjorde jeg meg oppmerksom på at det kunne ha innvirkning på resultatene, at mennesker lærer på hver sin unike måte. Det vil si at én medarbeider kan få utbytte av et kurs innenfor digital sikkerhet som en annen medarbeider ikke opplever å få utbytte

av. Uavhengige variabler kan også bli glemt å ta hensyn til, noe som kan gjøre resultatene av denne undersøkelsen mindre pålitelige.

En kvalitativ metode kan gjøre at vi forveksler informasjonen vi får med kunnskap, samt at man kan skape informasjon, ved å tillegge meninger som respondenten ikke selv har uttrykt. Vi mennesker tolker også virkeligheten rundt oss ulikt, og en fare kan da være at undersøkelsen blir annerledes om en utførte den på nytt med samme metode, noe som vil svekke påliteligheten til forskningsprosjektet (Askheim og Grenness 2018).

4.6 Gjennomføringsplan

Når	Hva ble gjort?	Hensikt	Oppnådd resultat
Januar	Utarbeidet problemstilling og forskningsspørsmål, Laget en skisse av oppgaven, innsamling av teori og metodevalg, Søkte etter relevante dokumenter og rapporter, trykket et kompendium bestående av viktige rapporter/bidrag til oppgaven	Tidlig ute med en god plan for å kunne møte på eventuelle utfordringer Lese meg opp på teori og rapporter og få en bedre forståelse for temaet slik at jeg kunne modnes og forstå bedre kontekst	Et førsteutkast ga meg retning og motivasjon til oppgaven. Skapte meg forståelse og hadde en klar pekepinn på hvor jeg ville med oppgaven.
Februar	Skrev videre på teori og metode, Kontaktet bedrifter. Siktet meg inn på bank- og forsikringsbransjen Skrev kontekstkapittel og tidligere forskning Spesifiserte 3 forskningsspørsmål og endret problemstilling	Sørge for at metoden var gjennomførbar og teorien samsvarer med det jeg ville undersøke Kontekst og tidligere forskning ville gi meg kunnskap om temaet og systemene jeg hadde å sette meg inn i	Fikk tilbakemelding på skisse om at oppgaven er gjennomførbar og spennende Forskningsspørsmål ga meg retning på oppgaven, og ga rom for å omformulere problemstilling

Mars	Laget liste over aktuelle intervjukandidater Søkte til NSD (norsk senter for forskningsdata). Laget intervjuguide + samtykkeskjema, Avtalte tid for intervjuer, samt holdt et pilotintervju	Finne kandidater som hører til ulike bedrifter for å sikre anonymitet og for å få nok intervjuobjekter til studien. Her var det planlagt å intervjue avdelingsledere, medarbeidere, sikkerhetssjef og personer innenfor IT. Søke til NSD for å kunne nevne fullt navn på ekspert fra NSM Avtale tid for intervjuer for å sikre å få tid til alle intervjuer.	Fikk intervjuet en del av de jeg hadde planlagt, men fikk ikke lov å intervjue sikkerhetssjef i verken bank eller forsikring. Dette ville gitt meg mer dybde i oppgaven. Fullt navn på ekspert skaper troverdighet til uttalelsene hans. Pilotintervju ga meg konstruktive tilbakemeldinger
April	Gjennomføring av 5 intervjuer innenfor bank og forsikring, samt 1 intervju med ekspert fra NSM Transkribering og koding, lagde skjema for sammenligning Jobbet med empirisk funn og å koble dette til relevante dokumenter	Empirikapittelets utforming og foreløpige funn bidro til å spisse problemstilling og strukturere valg av teori. Transkribering og koding skapte god oversikt over informantene	Gjennomførte 4 intervjuer over Teams og 2 intervjuer ved fysisk oppmøte. Farger i tabell for funn fungerte bra for å tydeliggjøre forskjeller og likheter mellom informantene.
Mai	Gjennomføring av 2 intervjuer Tilbakemelding på hele oppgaven av veileder, ferdigstilte funn og startet på drøftingskapittelet.	Flere intervjuer gir mer dybde i funnene og en bredere forståelse. Inkluderte flere dokumenter da det skaper kontraster og likheter i funnene mine.	Funn og drøfting gir mer mening, og teorien ble knyttet tettere mot det jeg fant ut gjennom intervjuene og i rapporter.
Juni	Ferdigstilte oppgaven, sjekket referanser og dobbeltsjekket tabeller og figurer. Korrektur på hele oppgaven. Levering av oppgaven 14. juni	Sørge for at det er en rød tråd i hele oppgaven og se at jeg besvarer problemstillingen på en god måte. Printe oppgaven for å lese korrektur	gjennomsyn og rettelse av tekst førte til bedre formuleringer og mer forståelig innhold og refleksjoner Ferdigstilling av oppgaven og levering av masteroppgave.

Tabell 2. Gjennomføringsplan

4.7 Forskningsetiske hensyn

Informantene har fått fullstendig informasjon om deltakelse i forskningen og jeg var særlig opptatt av at deltakerne i forkant av undersøkelsen var klar over forskningens hensikt, samt hva de takker ja til. Informantene som takket ja til deltakelse, har derfor avgitt et fritt informert samtykke (Tjora, 2020).

Jeg har også utformet et samtykkeskjema i tråd med «Den nasjonale forskningsetiske komité for samfunnsfag og humaniora» sine retningslinjer for forskningsetikk og vektla i dette skjemaet frivillighet i undersøkelsen. Dette impliserer at det ikke skal oppstå noen form for press til deltakelse (Jacobsen 2015). I tillegg har jeg også fremlagt hvilke gevinster og utfordringer en deltakelse kan medføre, slik at informantene selv kunne vurdere fordeler og ulemper ved å delta. Jeg fremhevet også eksplisitt undersøkelsens hensikt og formål, samt hvordan jeg skal bruke datamaterialet. Dette ble også nevnt på nytt igjen før selve intervjuene ble holdt, for å sikre meg at denne informasjonen er forstått av informantene.

Forskningsprosjektet er godkjent av NSD (Norsk senter for forskningsdata). Etter avtale med Jørgen Dyrhaug som min ekspertinformant fra NSM, velger jeg å ikke holde han anonym for å skape troverdighet til uttalelsene hans. Selskapene og informantene jeg snakker med innenfor bank - og forsikring sikres full anonymitet og skal ikke kunne gjenkjennes.

Mulige etiske dilemmaer jeg kunne ha møtt på handler i høyest grad om sensitivitet vedrørende den informasjonen som blir samlet inn og at man ikke skulle ønske å delta i frykt om at det skal gå an å gjenkjenne hvilket selskap som har hvilke rutiner. Det kunne blant annet vært sårbart å utgi informasjon om interne retningslinjer, sikkerhetsrutiner og måter å håndtere et eventuelt cyberangrep eller andre mulige trusler, i tilfelle denne informasjonen blir misbrukt en gang i fremtiden. Dette gjorde også at det var utfordrende å få sikkerhetssjefer til å stille til intervju, da de til tross for å bli lovet full anonymitet ikke ønsket å delta.

4.8 Sterke og svake sider ved metoden

En del av arbeidet for å skape høy kvalitet på intervjuene, har vært å reflektere rundt egne styrker og svakheter. Slike refleksjoner har gitt meg grobunn for å kunne forbedre formuleringen av oppfølgingsspørsmål og tempo. Ved å reflektere over egen intervjuteknikk la jeg etter hvert merke til at kvaliteten på intervjuene økte gradvis. Dette ser jeg som et resultat av mer erfaring med å avholde intervju, samt det å få mer kompetanse innenfor fagområdet rundt digital sikkerhet.

Jeg anser det som en svakhet ved egen forskning at det enkelte ganger ble stilt multiple eller tvetydige oppfølgingsspørsmål. Jeg tror dette kan begrunnes med at jeg lurte på flere ting samtidig, etter at informantene hadde gitt meg mye informasjon på én gang. Det er også viktig å trekke frem at jeg noen ganger brukte fagterminologi som kunne bli utfordrende eller forvirrende for informanten, særlig for de som ikke jobber med digital sikkerhet til daglig. En fare ved å bruke for avansert språk er at intervjuobjektet kan svare noe uten at de forstår spørsmålet, for å unngå å virke uviten og at dette kan gi feilaktige resultater og påvirke studiet (Tjora 2020). Jeg merket her et åpenbart skille mellom de som jobber med IKT-sikkerhet i det daglige og de som jobber innenfor helt andre roller i selskapet.

Det er også av betydning å nevne at det kan være en svakhet ved oppgaven at den bare baserer seg på én bransje og ett case; bank – og forsikring. Det vil derfor være vanskelig å generalisere resultatene til en annen bransje, selv om ikke generalisering er et mål i seg selv. Videre har jeg kompensert for dette ved å bruke en ekspertinformant som snakker generelt for alle bransjer, samt at jeg har supplert med dokumenter og rapporter som gjør seg gjeldene utover bank – og forsikringsbransjen. Deler av det jeg finner ut i denne oppgaven kan derfor forstås utover bransjen som er studert.

5. Empirisk funn

I dette kapittelet vil sekundærdata fra de seks dokumentene som er presentert i del 4.2 være et hovedfokus. Videre vil primærdata i form av 7 kvalitative intervjuer fra informanter fra bank – og forsikringsbransjen bli presentert. Fire av disse informantene jobber i bank, mens de tre resterende jobber innenfor forsikring. I tillegg vil det komme frem primærdata fra et intervju med Jørgen Dyrhaug[2] fra NSM og deler fra rapporter og dokumenter som står i kontrast eller underbygger svarene som kommer frem. Kapittelet vil bli delt opp i to, hvor jeg først vil presentere et skjema hvor jeg har sammenlignet noen verdier basert på at informantene (i) har tallfestet opplevd risiko, bekymringer og trusler når det kommer til trygg nettbruk og datakriminalitet. Disse har jeg gitt noen korte kommentarer til, og blir videreført til drøftingsleden av oppgaven. Videre i kapittelet vil jeg presentere og gi en oversikt over interessante funn når det kommer til hva ledere gjør i arbeidet med sikkerhet, rutiner, teknologi og trusler. Disse er strukturert i henhold til de tre definerte forskningsspørsmålene. Det må påpekes at flere av funnene glir over i hverandre, noe som gjør at det ikke alltid er tydelige skiller mellom muntlige eller skriftlige funn. Funn fra intervjuet med Jørgen Dyrhaug fra NSM, tidligere sikkerhetssjef i Forsvarsdepartementet, vil fungere som «ekspertuttalelser» og som en veiledning på hvordan det er mulig å tenke rundt digital sikkerhet og de konsekvensene teknologien kan føre med seg.

5.1 Sammenstilling av opplevd risiko, bekymringer og trusler

Kategori	**Påstand**	***i1***	***i2***	***i3***	***i4***	***i5***	***i6***	***i7***
Stillingstittel		*Takstmann*	*Kunderådgiver mot bedrift*	*Avdelingsleder*	*Kunderådgiver*	*Avdelingsleder*	*Software Engineer, IT*	*Finansrådgiver*
Type bedrift, tid i bedriften		*Forsikring, 11 år*	*Bank, 1,5 år*	*Bank, 4 år*	*Forsikring, 2 år*	*Forsikring 8 år*	*Bank 3 år*	*Bank 1,5 år*
Alder		*58 år*	*27 år*	*32 år*	*22 år*	*42 år*	*30 år*	*27 år*
1. Generell risikoforståelse								
1 =	1) Du er positiv til teknologi	*1*	1	1	1	1	1	1
	2) Du vet hva informasjonssikkerhet er	1	1	1	1	1	1	1

[2] Gitt tillatelse til bruk av fullt navn og godkjent av NSD.

helt enig *5= helt uenig*	3) Du utsetter deg selv for risiko når du bruker internett	*1*	1	2	1	2	3	2
	4) Det er greit at din aktivitet på internett blir overvåket dersom det fører til at du blir tryggere på nett	*3*	4	5	5	4	3	3
	5) Du har tillit til at myndigheter sikrer informasjonen de har registrert på deg.	*2*	4	2	4	2	2	4
Kommentarer: *Tydelig at samtlige av informantene er positive til teknologi og hevder de vet hva informasjonsteknologi handler om. Det er mer sprik når det gjelder tillit til overvåkning og andre kontrollmekanismer. Informant 1 nevner han blir skeptisk med en gang det nevnes overvåkning, men stiller seg nøytral som også informant 6 og 7 velger å gjøre, og informant 2 og 4 svarer at de er delvis uenig i at overvåkning er nødvendig for å sikre sikkerhet. Informant 3 og 4 er helt uenig i at overvåkning er greit uavhengig av at det fører til at man blir tryggere på nett.*							
2.Bekymringer								
1= ikke bekymret *5= svært bekymret*	1) At dine dokumenter skal bli ødelagt på dine enheter?	*2*	1	1	2	1	4	1
	2) Få virus på pcen din?	*1*	2	2	1	3	2	2
	3) At du blir lurt til å gi fra deg sensitiv informasjon?	*2*	3	2	2	3	5	1
	4) At du trykker på en lenke du tror er ekte, men som er svindelforsøk?	*2*	2	1	2	3	5	1

	5) At noen skal utgi seg for å være deg på nett?	*2*	2	2	3	2	5	1
Kommentarer: *Det kommer frem av de fleste av informantene at de er lite bekymret for at dokumenter skal bli ødelagt fordi de opplever et stort fokus på digital sikkerhet innad i organisasjonene. Likevel er det en av informantene som skiller seg ut, og det er vedkommende som jobber i en IT-avdeling. Det er ellers også samsvar mellom informantene når det kommer til hvor bekymret de er for at andre hendelser skal skje, slik som virus eller annen datakriminalitet. Likevel kan man se noe forskjell mellom svarene mellom vedkommende som jobber innenfor IT – avdelingen og andre medarbeidere som ikke jobber med teknologi til vanlig. Blant annet rangerer IT-programmerer 3 av 5 svar på nivå 5. Her kan vi se at informant 6 som jobber i IT-avdelingen til vanlig er mer bekymret enn de andre informantene for at de ulike hendelsene skal skje, noe som kan ha noe med erfaring og kompetanse å gjøre, eller at han har et annet grunnlag å vurdere spørsmålet på enn det de andre har ut fra sin utdanning innen IKT.*							
3. Risiko og trusler								
1= liten risiko *5= stor risiko*	1) Hvor stor risiko forbinder du med å bruke e post på jobb?	1	4	2	1	1	1	1
	2) Dele passord med andre?	5	5	4	5	5	5	4
	3) Bruke samme passord på flere nettjenester?	3	4	3	4	4	5	3
	4) Bruke bank eller kredittkort på nett?	3	2	2	2	2	2	3
	5) Å ikke ta sikkerhetskopi?	1	1	4	1	4	4	4
Kommentarer: *I kategorien om hvor stor risiko informantene opplever rundt disse påstandene spriker svarene mer enn de gjør i det foregående kategoriene. For eksempel er det store forskjeller i hvordan informantene vurderer risiko ved bruk av e-post. Informant 1 og 4 ser ingen risiko ved bruk av e-post fordi de begge synes at systemene oppleves sikre. Det kan nevnes at dette begge er informanter fra forsikring, og at det derfor kan tenkes at det da kan være andre faktorer som gjør at de i bank opplever mer risiko ved bruk av e-post. Informant 2 forteller blant annet om en hendelse der han fikk en e-post mens han fysisk satt ved siden av en kunde. Det foregikk altså et svindelforsøk rett foran øynene på de begge. Han vurderer derfor risikoen som høy, da han synes slike svindelforsøk ofte kan virke reelle og ekte. Det er derimot enstemmig at det er svært høy risiko ved å dele passord med andre, men informant 3 understreker at det finnes dimensjoner ved dette, og for eksempel at det å dele passordet med en nær kollega som du velger å stole på er greit i noen tilfeller. Tillit blir i denne sammenhengen en viktig faktor.*							

Tabell 3. Sammenstilling av opplevd risiko, bekymringer og trusler

5.2 Empirisk funn: dokumenter og intervjuer

5.2.1 «Hva gjør lederne for å bygge opp en digital sikkerhetskultur?»

Hovedfunn

- Medarbeiderne stoler på at sikkerhetsavdeling tar seg av digital sikkerhet
- Jevnlige kurs og oppgaver for å friske opp i digital forståelse
- Lederforankring og erkjenne et behov for sikkerhet
- Fokus på digital sikkerhet ved nyansettelse viser viktigheten av sikkerhet

Å ivareta digital sikkerhet er først og fremst et virksomhetsansvar (NOU 2017, s. 3). Jørgen Dyrhaug jobber til daglig med datasikkerhet i Nasjonal sikkerhetsmyndighet (NSM). Han hevder at det viktigste for å bygge opp en digital sikkerhetskultur handler om lederforankring. Mørketallsundersøkelsen fra Næringslivets sikkerhetsråd (2018) har kartlagt 1500 norske virksomheter og gir et innblikk i norske virksomheters holdninger til digital sikkerhet, kunnskap, forebygging og beredskap (NOU 2018:14, s. 57). Undersøkelsen viser at norske virksomheter investerer generelt alt for lite i IKT-sikkerhet (NOU 2018:14, s. 57). Det at ledelsen erkjenner og forstår behovet for et fokus på digital sikkerhet mener han er helt avgjørende for en god digital sikkerhetskultur;

> *«Jeg opplever altfor ofte ledere som peker på en eller annen 'stakkar' nede i organisasjonen og sier: Ja, men han er sikkerhetsleder - det er han som er ansvarlig, og det er han som driver med sikkerhet»*

Det kommer frem av rapporten fra NSM (2019, 13) at ledelsen må integrere digitalt sikkerhetsarbeid i prosesser og styring for å skape langsiktig, kontinuerlig og et strukturert sikkerhetsarbeid. Nesten halvparten i mørketallsundersøkelsen sier de er for dårlige til å identifisere nye cybertrusler (NOU 2018:14, s. 57).

Dyrhaug sammenligner det med julebordskomiteen for få frem poenget sitt. Selv om julebordskomiteen er den som planlegger julebordet, så er det jo ikke bare de som kommer på julebord. De skal legge til rette for julebordet for alle. Det samme gjelder når vi snakker om sikkerhet, hevder Dyrhaug;

> *«Folk som jobber med sikkerhet er jo ikke de eneste som jobber med sikkerhet. De skal legge til rette for at alle andre også forstår at de jobber med sikkerhet! De har kanskje litt mer av dette i hverdagen, men alle i en virksomhet driver jo med dette når alt kommer til alt».*

Samtlige av intervjuobjektene nevner at de stoler på *´de som driver med sikkerhet´* og at det gjøres en grundig jobb med sikkerhet. Det nevnes blant annet at det holdes jevnlige kurs for de ansatte for å sikre god digital forståelse. Hyppighet av kursene varierer noe fra bedrift til bedrift, men det kommer frem at det holdes minst ett kurs i måneden, eller gjerne fler. Det nevnes av samtlige informanter at kursene må bestås, og at alt blir registrert digitalt. Hvis du er sen og ikke svarer på kurs får du en påminnelse om at dette må gjøres innenfor en viss tidsfrist. Det er noe forskjell på om de ansatte opplever at de får utbytte av kursene. En av informantene innenfor forsikring, mener at kursene ofte kan bli litt for bankfokuserte og oppleves noe irrelevant. Vedkommende nevner også i samme setting;

> *«Jeg personlig må jo si at: «off, må jeg ta det kurset der og?». Men samtidig så sier jeg meg til meg selv at det handler om sikkerhet».*

En av lederne fra bank legger også til at det sporadisk sendes ut noen e-poster til de ansatte for å sjekke om de ansatte faktisk er kritiske og oppdaterte når det kommer til digital sikkerhet;

> *«Det skjer at det blir sendt ut eposter sporadisk for å teste folk litt. Ikke for å arrestere noen på det, men for å rett og slett se hvor nivået ligger uten at det er noen reell fare ved disse epostene».*

Under spørsmålet om noe kunne vært gjort annerledes for å øke den digitale sikkerheten svarer en av informantene innenfor bank at:

> *«Jeg stoler på at vi har nok sikkerhet, og det virker veldig sånn da og at alle gjør sitt. Men hvis jeg skulle gjort noe annerledes ville jeg sett og forstått alle brannmurene og sånt, hva de gjør, men det hadde tatt meg veldig mange år å lære og forstå, så det er jo en tillit der da. Tillit til at de som har ansvar for sikkerhet gjør sitt».*

Dyrhaug mener at det er virksomhetskritisk at en ledergruppe faktisk forstår at ansvaret for daglig gjennomføring av sikkerhet sprer seg nedover i virksomheten. Han mener det viktigste en leder kan gjøre er å få hvert enkelt menneske til å skjønne at de er en viktig bit av det større bildet og at de ikke kan gjøre hva de vil.

> *...«Man kan ikke gå å tenke at ´Hans Petter på IT´ som er sikkerhetssjef fikser. Men **** Hans Petter på IT kan jo ikke gjøre alt. Det er du som klikker på lenker, det er du som kobler til et eller annet. Hans Petter på IT kan ikke styre det, det er din adferd som styrer om det gikk bra eller ikke gikk bra hos deg. Hans Petter på IT han prøver liksom desperat å fortelle alle hva de skal gjøre, men det er til syvende og sist deg og meg og alle andre som da gjør eller ikke gjør noe».*

Det nevnes også et særlig fokus på digital sikkerhet når det kommer til nyansatte. Det nevnes både innenfor bank og innenfor forsikring at alle nyansatte må bestå spesifikke kurs for å få lov å begynne å arbeide med de vanlige arbeidsoppgavene.

> *«Alle nye i løpet av de tre første månedene gjennomgår et opplæringsprogram som inneholder alt fra datasikkerhet til ting de skal holde på med. De blir kalt inn en gang i uken for å ta diverse kurser og ganske tett oppfølging de første 3 måneder så går de over på de vanlige arbeidsoppgavene».*

> *«Ved et aktivt fokus på slike kurs forstår gjerne også de nyansatte viktigheten av slike ting når de må gjennom disse kursene før de kan begynne å jobbe».*

> *«Alle får de samme kursene. Noen har 10 år i bedriften og noen har 2 måneder. Alle må gå gjennom rutinemessige ting der man får med seg ting på oppsummeringer og repetisjon».*

Institusjonelt for en svær bedrift er det et musklikk som teoretisk sett kan nulle ut en bedrift. Når konsekvensene er så svære og risikovurderingen så dårlig så er det en mismatch her, uttaler Dyrhaug fra NSM.

For å gi en bedre beskrivelse av risiko og hva ledere kan gjøre for å bygge opp en digital sikkerhetskultur trekker Dyrhaug frem risikotrekanten som beskriver sammenhengen mellom verdi, trusler og sårbarhet og avhengigheten mellom disse. Hovedbudskapet hans er at risiko i det digitale domenet er egentlig et spørsmål om å kunne forstå sine egne sårbarheter, fordi man

ikke kan gjøre noe med trusselaktørene, og verdiene mener han vi ikke ønsker å gjøre noe med. Det er altså bare sårbarhetene man får gjort noe med; *«Du må gjøre det så upraktisk for innbruddstyven at de lar være. Men samtidig må du akseptere at en viss svakhet må det være, ellers får du ikke gjort det du skal gjøre i systemet ditt».*

Det er her hensiktsmessig å påpeke det departementet beskriver rundt sårbarheter og avhengigheter. Rapporten beskriver en strukturell sårbarhet i samfunnet, der de fleste virksomheter er avhengige av digitale tjenester som er levert av andre (NOU 2018:14, s. 20). Sårbarheter og feil forplanter seg raskt mellom leddene i verdikjeden og kan få uante konsekvenser. Tjenester, systemer og infrastrukturer arver sårbarheter fra hverandre (NOU 2018:14, s. 20). Med andre ord kan det plutselig dukke opp sårbarheter man ikke helt var klar over hvis det skulle skje noe uventet hos en annen organisasjon i egen verdikjede. Gjensidige avhengigheter og sårbarheter i digitale verdikjeder kan i verste fall påvirke samfunns- og statssikkerheten (NOU 2018:14, s. 20). Det samme vil Dyrhaug få frem når han sier at det er helt nødvendig at ledere gjør seg klar over hvilke sårbarheter som finnes i sin egen verdikjede og ikke overlater dette ansvaret til «de som driver med sikkerhet». Dette samsvarer også med det som kommer frem i «prioiterte områder» i den nasjonale strategien for digital sikkerhet fra 2019, der det helt spesifikt er beskrevet at; «en virksomhet bør vite hvilke tjenester de selv er avhengige av og hvilke mulige konsekvenser hendelser i egen digital infrastruktur kan ha for andre» (Departementene, 2019, s. 15).

5.2.2 «Hvilke rutiner er etablert for å vedlikeholde digital sikkerhet i organisasjonen?»

Hovedfunn

- Bruk av sikre nettverk / VPN
- Regelmessig sikkerhetskopiering
- Sperre av ukjente internettkilder
- Sterke passord og flerfaktorautentisering
- Årvåkenhet blant ansatte

Å bygge opp motstandsevne mot operasjoner fra trusselaktører og å være robust i møte med tilfeldige hendelser krever kontinuerlig arbeid, evne og vilje (NSM 2019, s. 9). Ledelsen må integrere digitalt sikkerhetsarbeid i prosesser og styring, samt prioritere dette i budsjettene (NSM 2019, s. 13).

Samtlige av informantene sier det finnes regler for informasjonssikkerhet. Det som nevnes flest ganger er å ikke bruke offentlige wi-fi nettverk og å bruke sikre nettverk. Innenfor bank blir det nevnt at det er en absolutt regel å ikke jobbe på kafé;

> *«Du kan for eksempel aldri jobbe et sted der du kan utsettes for at noen kan se eller høre det du sier. Du kan ikke sitte på kafé. Du kan jobbe på toget, men da må du også være litt påpasselig med hvem er det som sitter rundt deg, hva du kommer til å snakke om og disse tingene».*

Innenfor forsikring blir de samme tingene nevnt, men mer som en anbefaling enn en regel;

> *«Når du skal ha hjemmekontor så må du jo ta med deg pc hjem, men eneste advarsel vi har fått er å være obs på å helst ikke bruke wi-fi nettverk, for eksempel hvis du sitter på en kafe eller andre steder. Du skal forholde deg til sikre nettverk og ikke offentlige nettverk. Dette er i utgangspunkt en anbefaling og ikke en absolutt regel. Man skal være oppmerksomhet på det».*

Videre blir det nevnt flere ganger retningslinjer når det gjelder lagring av informasjon, samt når det kommer til brannmurer og totrinnsautourasjon. Samtlige nevner skytjenester som den måten man skal lagre informasjon.

> *«Vi skal ikke bruke USB og lignende til lagring av informasjon. Vi har skytjenester som skal brukes som er koblet mot brukerne på vårt nettverk og mot intranett. Da er dette innenfor sikkerhetsmuren».*

> *«All vår informasjon lagres i skyen og oppdateres automatisk gjennom sentralbordet. Vi har nylig gått over til å lagre alt i skyen fordi det skal være mye sikrere».*

> *«Vi har brannmurer og sikkerhetsprogramvarer for å vedlikeholde digital sikkerhet, men kan ikke utdype hvilke fordi det er ikke informasjon vi kan dele».*

Kort oppsummert hevder Dyrhaug at når det kommer til rutiner er det visse ting som en virksomhet må ha på plass. Dette er rutiner på å faktisk vite hva slags systemer de har, vite hva man har av informasjonssystemer og digitale systemer, være i stand til å ta vare på de systemene, vedlikeholde dem med å holde dem oppe, samt være i stand til å oppdage at det skjer noe i systemet hvis en hendelse skulle inntreffe.

Det følger av NSMs grunnprinsipper at man skal ha kontroll på egen IKT-infrastruktur og ikke bare «viktige» systemer. Man må kjenne til alle sammenkoblinger og hvilke systemer som har tilgang til hvor (NOU 2018: 14, s. 72). Når risikonivået øker er det krevende å gjennomføre raske endringer i virksomhetens sikkerhetstilstand. Ifølge NSM (2022) er det noen fokusområder som imidlertid bør ha prioritet;

1) Kartlegging av systemer og en oppdatert oversikt over systemer og programvare som kjører i organisasjonens nett, samt en oversikt over oppdateringsstatus (NSM, 2022a). Å ha oversikt over sine egne systemer er noe av det Dyrhaug beskriver som helt grunnleggende og nødvendig når en hendelse først inntreffer. Flere av informantene nevner også viktigheten av dette, men mener det er sikkerhetsansvarlige og ledelsen sitt ansvar å sørge for at disse blir fulgt opp. Noen av medarbeidere innenfor både bank og forsikring nevner at de ikke vet hvilke systemer som brukes, mens andre hevder at dette er informasjon de ikke ønsker å oppgi på grunn av at dette kan være sensitiv informasjon for organisasjonen å dele.

2) Årvåkenhet blant ansatte og gjennomføring av tiltak rettet mot medarbeidere for å styrke sikkerhetskultur og risikoforståelse. Å ha skjerpede sikkerhetstiltak mot nettfisking og sosial manipulasjon, gjennom menneskelig årvåkenhet og ved tekniske løsninger som for eksempel spamfilter (NSM, 2022a). Samtlige av informantene nevner at det er gode rutiner for sterke passord og flerfaktorautentisering, samt et fokus på bevissthet i kurs og andre tester som blir sendt ut. Videre nevnes det at det er filter på både nettleser og på mail som skal bidra til å sile ut det som kan være av fare for organisasjonen.

En undersøkelse NVE gjennomførte i 2017 om IKT-sikkerhet viser at rundt halvparten av virksomhetene som svarte, hadde hatt uønskede hendelser. Undersøkelsen viste videre at 40% av virksomhetene som hadde hendelser de kategoriserte som deres alvorligste hendelse ikke gjorde noen endringer i organisasjonen som følge av dette (NSM 2019, s. 13). Informantene i denne studien sier de har ingen kjennskap til noen tidligere cyberforsøk eller større digitale trusler som kunne ha vært årsak til at rutiner rundt digital sikkerhet er innført. Samtlige nevner at det er ukjente epostforsøk daglig, men nevner ikke mye utover dette. En av lederne sier imidlertid at det kan være at det har skjedd forsøk selv om ikke vedkommende har fått høre om det;

> *«Vi bare skraper i overflaten når det kommer til det der. Vi sørger jo for at de ansatte håndterer informasjon på en god måte, men i min avdeling jobber de jo ikke med IT-*

sikkerhet. Det som er viktig er jo at de håndterer informasjon riktig og at de tråt varsomt. Det er jo det vi ser, men det kan jo være ting som har skjedd i organisasjonen uten at vi nødvendigvis får beskjed om det».

Det er imidlertid slik at fullstendig åpenhet om digitale sårbarheter og tidligere hendelser kan bety åpenbare sikkerhetsutfordringer og at dette kan være grunnen til at virksomheter ikke ønsker at spesifikke svakheter skal komme frem i offentligheten (NOU 2018: 14, s. 62). I flere land, blant annet Nederland, er det utarbeidet retningslinjer for hvordan man skal få til en mer styrt tilnærming til å ta imot varsler og offentliggjøre digitale sårbarheter, også kalt «responsible vulnerability disclousure Guidelines» (NCSC, 2018). I Norge mangler vi en slik tilnærming for digitale sårbarheter, fordi det er uklart hvilken myndighet som skal være ansvarlig for dette, men det kan se ut som om dette er en tilnærming Norge også er på vei mot.

Tradisjonelt har passord vært en rekke med tall, symboler og bokstaver bare den enkelte bruker skal kjenne til, men svakheten er selvsagt at passord kan gjettes (NSM, 2022b). En meget alvorlig og utbredt sårbarhet er ofte at man benytter passord som er alt for lett å gjette, noe som er en stor utfordring (NOU 2018: 14). Dette kan være passord blant vanlig ansatte eller passord for kontoer som benyttes i forbindelse med drift av IT-systemene (NSM, 2022b). Det kommer frem av intervjuene at informantene i denne undersøkelsen forbinder høy risiko ved det å dele passordet sitt med andre. Det kommer også frem at en av retningslinjene for å sikre digital sikkerhet er at det hver tredje måned kreves at de ansatte må bytte passordet sitt og at dette blir ugyldig når det er gått tre måneder. Imidlertid sier en av informantene at;

«Men jeg må jo si det er noen svakheter i det. Det går jo an å bare endre de siste to sifrene i passordet. Jeg har jo veldig mange programmer og veldig mange innloggingspassord og det kan bli vanskelig å huske alt hvis man skal forandre alt for mye».

5.2.3 «Hvordan forstår de ansatte trusler og farer ved bruk av ny eller eksisterende teknologi?»

Hovedfunn

- Mennesker har ingen digital intuisjon
- Et kompleks teknologibilde i endring
- Et digitalt kjempemonster som vi ikke forstår omfanget av
- Kunnskap og atferdsendring
- Det digitale fundamentet er virksomhetskritisk

Ifølge en mørketallsundersøkelse fra 2018 er det kun 24 % av norske toppledere som mener deres virksomhet enten er «svært godt» eller «godt» forberedt på cyberangrep, og nesten halvparten sier de er for dårlige til å håndtere digitale trusler (NOU 2018: 14, s. 57). Av intervjuet med Dyrhaug kommer det frem at vi i det digitale domenet ikke reddes av intuisjon. Ubehaget som vi kan kjenne når vi fysisk står utenfor et stup for eksempel, kommer helt automatisk og naturlig for oss mennesker. Vi føler ingen fysisk fare når det kommer til teknologi, noe som kan gjøre at risikoforståelsen vår ikke henger med*; «Vi har ingen digital intuisjon. Vi dingler på kanten av stupet, men vi ser ikke stupet!»*, understreker Dyrhaug. Videre påpeker han at;

> *«Når man er i ferd med å trykke på en lenke, åpne et vedlegg eller gjøre en tabbe i det digitale domenet så er det ingen varsler om at det er noen fare. Det gjør at den digitale risikoforståelsen ikke er i nærheten av å være så stor som den gjerne burde ha vært».*

Dette underbygges også av rapporten av Malmedal og Røislien (2016, s. 43) der det kommer frem at; *«Our interactions with information technology, and the risks associated with them, are changing and becoming more complex».*

Samtlige av informantene svarer at de mener de vet hva informasjonssikkerhet handler om og at de tenker de kan litt mer om teknologi enn sine kolleger. Som vi ser i del 5.1 punkt 3) hvordan informantene svarer på i hvilken grad de opplever risiko og trusler ved teknologi ser vi at informantene er uenige når det kommer til risiko. Dyrhaug hevder han vet forklaringen på dette; «*Man skjønner ikke at man ikke skjønner cyberspace og datamaskiner. Det er egentlig forklaringen på alt».*

> *«Du har sagt ja til noe du egentlig ikke forstår omfanget av når du tok i bruk datamaskiner. Du har sagt ja til noe du ikke ser, og som er da et monster. Som egentlig bare liksom troner over deg! Du ser ikke monsteret. Du ser ikke det digitale monsteret for du er egentlig ikke i stand til å identifisere at: Å helvete, dette er et kjempemonster».* Jørgen Dyrhaug, NSM, 2022.

Likevel er 96 % av alle nordmenn på internett, og mer enn 90 % av disse er åpen til å ta i bruk ny teknologi. Videre hevder 6 av 10 at de er kapable til å vite hva som er sikkert og ikke å gjøre på nett (Malmedal og Røislien 2016, s. 8). Dette understreker at både informantene og resten av den norske befolkningen ikke ser ut til å tenke på teknologien som et monster. Det kan diskuteres om dette har med kunnskap eller kompetanse å gjøre. Dette er også hvorfor det stilles så strenge krav til dokumentasjon om sikkerhetsrutiner.

> *«Det er ikke bare å dytte dokumentasjon på folk. Kunnskap eller informasjon som man ikke bruker til noe mer betyr ingenting. Det er det øyeblikket folk er informert nok og kunnskapsrike nok til at de begynner å oppføre seg annerledes – til vi ser en sånn atferdsendring at ting begynner å skje»*

Noe av det samme ser vi i cybersikkerhetsrapporten fra 2016; *«Interest in technology and ICT correlates with a pattern where people learn from experts, and from their own trial and error… interest correlates directly with a more secure behavioural pattern" (Malmedal og Røislien 2016, s.50).*

Videre forteller Dyrhaug at det er klart at digital sikkerhetskultur egentlig er akkurat det samme som sikkerhetskultur i den fysiske verden. Det er hva du gjør og ikke gjør – når det å gjøre noe er bra og det å ikke gjøre noe er bra. Vi snakker med andre ord om din atferd sett i forhold til situasjonen. Dyrhaug poengter avslutningsvis; *«Ofte er det mismatch mellom hva de skriver at de skal gjøre og hva de faktisk gjør».*

Å stille krav om forsvarlig IKT-sikkerhet i en lov kan være klargjørende og bidra til økt bevissthet for mange virksomheter. Utfordringen med for detaljerte krav om forsvarlig IKT-sikkerhet er at det kan bli veldig omfattende, fordi det skal dekke mangle ulike forhold (NOU 2018: 14, s. 73).

Jørgen Dyrhaug fra NSM uttaler følgende;

> *«For meg handler dette om adferd. Jeg bryr meg ikke om dokumenter. Jeg har vært på besøk i mange virksomheter som har all dokumentasjon på plass, og det er hyllemeter med dokumentasjon og det ser pent ut. De gjør det fordi de må. Men hvis jeg må velge så er det jo atferd som trumfer hyllemeter på hyllemeter med meningsløs dokumentasjon. Det skjer ikke noe før du gjør noe.».*

De fleste ledere bryr seg om sikkerhet, men problemene oppstår gjerne på grunn av en feilaktig forståelse av hva som kreves for å oppnå høye sikkerhetsnivåer og hva kostnadene er hvis sikkerhetsarbeidet gjøres riktig. Et eksempel på dette kan være viktigheten av å også tenke sikkerhet hjemme, og ikke bare på arbeid (NSM 2019, s.9). Det nevnes av flere informanter at det er like viktig å tenke sikkerhet på arbeidsplassen og hjemme. Likevel skiller en av lederne i bank sitt svar seg ut i mengden;

> *«Det er viktig privat også, men de økonomiske konsekvensene ved mistet informasjon i jobb kan være veldig store. Men det er viktig å ha samme nettvett privat og. For dine personopplysninger er og viktig, men det er ikke så økonomisk katastrofalt nødvendigvis».*

En mørketallsundersøkelse fra 2018 avdekker at tilfeldigheter og uflaks blir oppgitt som årsak til hendelser i to av tre tilfeller, etterfulgt av menneskelige feil og mangel på sikkerhetsbevissthet (NSM 2019, s. 13). Når informantene blir spurt om hva de opplever som den største trusselen på nett er det noe variasjon i svarene. De yngre informantene nevner at de er mest redd for å bli hacket på sine enheter, mens de informantene over 50+ nevner at de er mest redd for å bruke kortet sitt på nett og at dette skal bli mishandlet. Et interessant funn er at lederne i undersøkelsen svarer at de forbinder stor risiko ved å ikke ta sikkerhetskopi, mens medarbeidere på lavere nivå i organisasjonen ser på dette som lite risikofylt. Videre blir telefonen nevnt som en av de største truslene på nett;

> *«Muligens telefoner. At telefonen er det mest utsatte, mer enn pcen. Fordi her kommer kanskje mer av det private inn og. Man har gjerne jobbtelefon som brukes privat, og åpne nettverk og sånne ting. Ting kan kanskje bli hacket der da».*

En annen informant deler at han ser på hacking som den største trusselen:

> *«Den største trusselen for meg i jobbsammenheng er det å bli hacket. Enten bli lurt eller det man kaller for pishing, altså nettfisking. Eller bare bli hacket hjemme på en av mine enheter».*

Dyrhaug beskriver det han mener er det viktigste å tenke på;

> *«Det viktigste er å forstå at det digitale fundamentet enhver virksomhet i Norge står på, er helt virksomhetskritisk! Uten en sunn digital plattform så får du ikke gjort en dritt fordi det alltid ligger en datamaskin og styrer så utrolig mye mer av butikken din enn det du kanskje tror».*

For de aller fleste virksomheter sies det at slurv, manglende eller dårlig kunnskap og for dårlig kontroll er den største trusselen mot en stabil og trygg informasjonsbehandling (Daler m.fl. 2010, s. 34). Det er sprik i svarene når informantene blir spurt om de bevisst har måttet bryte noen retningslinjer for informasjonssikkerhet, noe som kan reflektere slurv eller andre type måter å ikke ta den digitale sikkerheten på alvor. Flere nevner at de aldri har brutt noen regler og vil ikke utdype mer utover dette. Likevel innrømmer en av lederne fra bank at det er noen ganger er blitt lagret informasjon over USB, til tross for at man er fullt klar over at dette ikke er lov.

> *«Det har vært eksempler på at det er blitt brukt USB uten at det er skjedd noe dramatisk rundt det da. Der er det også noe forskjell på en USB du har mottatt eller bare har funnet, eller en helt ny USB for eksempel. Eller gjerne til eget bruk til fremvisning av en presentasjon ute hos en kunde. Det er jo en varsomhet rundt dette, og det kan gjøres på en mer forsvarlig eller mindre forsvarlig måte dette med USB».*

6.0 Analyse

I analysen blir funnene fra del 5 diskutert for å forsøke å finne svar på undersøkelsens problemstilling. I denne sammenheng vil jeg diskutere relevante aspekter av de åtte dimensjonene som ifølge teorien beskriver en digital sikkerhetskultur og drøfte på hvilken måte det innenfor bank – og forsikring er knyttet eventuelle utfordringer til å utvikle en digital sikkerhetskultur.

6.1 «Hva gjør lederne for å bygge opp en digital sikkerhetskultur?»

Studier viser at lederens forpliktelse til sikkerhetsmål er den viktigste faktoren som skiller trygge fra usikre systemer og selskaper (Leveson 2011, s. 415). De holdninger og verdier som kommer frem gjennom funnene fra informantene i studien kan reflektere et felleskap av verdier innenfor bank – og forsikringsbransjen. Til tross for at det er informanter fra ulike selskap, kommer det frem mange likheter når det kommer til måten å tenke digital sikkerhet innenfor bransjen, både mellom ledere og medarbeidere. Svarene jeg har fått gir meg en pekepinn på hvordan kulturen i de ulike organisasjonene er, der hva som sees på som normalt, trygt, rasjonelt eller irrasjonelt kommer frem. Samtlige av informantene tror at organisasjonen de jobber i gjør det de kan for å sikre at ikke datakriminalitet skal forekomme i deres selskap. Både ledere og medarbeidere virker å vite lite om hvem som faktisk har ansvaret, og hevder at de må ha tillit til «de som jobber med sikkerhet». Det er ifølge NSM (2020, s. 4) helt avgjørende at toppledelsen tar eierskap til, og involverer seg i sikkerhetsarbeidet i egen virksomhet.

Tillit er en av de åtte komponentene som ifølge Malmedal & Røislien (2016) kan være med å beskrive en digital sikkerhetskultur. For at selskapet skal kunne styre effektivt, samtidig som de opprettholder stabilitet, trenger de tillit fra sine ansatte (Malmedal & Røislien 2016, s. 32). Hvor stor grad av tillit man har til systemene og menneskene i det digitale domenet har stor betydning for hvordan man velger å handle i ulike situasjoner (Nettvett, 2020). Det at samtlige informanter påpeker at de har tillit til at «de som jobber med sikkerhet» har kontroll uten å engang bli spurt om dette på intervjuet, viser at informantene i studien har stor tillit til systemet de jobber innenfor noe som kan være en stor trussel for organisasjonen. Digitaliseringen er både avhengig av, og sårbar for tillit, og det kan virke som tillit er sentralt når det kommer til informantenes forståelse av digitale sikkerhet.

De fleste aksepterer at det finnes systemer på jobb som logger en del av aktiviteten i løpet av dagen (Nettvett, 2020). Mange velger å stole på at denne informasjonen ikke blir utnyttet. Ut

ifra svarene fra informantene i undersøkelsen kan vi se at informantene forbinder overvåkning med moderat til høy risiko. Ingen av informantene mener det er helt greit at deres aktivitet på internett blir overvåket dersom det fører til at de selv blir tryggere på nett. Dette sier noe om hvor viktig det er for informantene med tillit, og et viktig spørsmål blir dermed hvor mye overvåkning, styring og kontroll som er akseptabelt når både felleskapets og den enkeltes sikkerhet og trygghet står på spill (Bergsjø, Windvik og Øverlier, 2020, s. 38).

Det kommer ikke frem at medarbeiderne eller lederne vet om noen tidligere hendelser av datakriminalitet i noen av selskapene. Dette kan også ha innvirkning på det tillitsnivået medarbeiderne viser overfor systemet de jobber i. Det kan for eksempel tenkes at systemet er redundant og robust nok til at det ikke vil skje i fremtiden heller, selv om det i virkeligheten kan være tilfeldige grunner til at ikke selskapet er angrepet. Det kan også være ulike grunner til at selskapet skulle ønske å holde et eventuelt tidligere digitalt angrep eller uhell skjult. For det første kan det indikere sårbarhet og at systemet ikke er redundant nok, noe som kan gjøre særlig kunder bekymret for at bank – eller forsikringstjenesten de benytter seg ikke er så til å stole på som de trodde. For det andre kan det spre usikkerhet internt i organisasjonen, hvis det spekuleres i hvordan de interne prosessene ble håndtert eller pekes fingre mot hvem som har gjort feil. Videre kan det være at lederne ikke har klart å håndtere den uventede situasjonen på en måte de er stolt av å dele, for eksempel hvis de ikke klarte å gjenvinne normale funksjoner og gjenopprette funksjonalitet fort eller godt nok.

Det er viktig at ledere kjenner til sikkerhetskulturen i egen virksomhet, slik at medarbeidere er motstandsdyktige og gjør sikre valg når det kommer til virksomhetens datasystem (Nettvett, 2020). «Det er lett å glemme å være redd for ting som sjelden skjer» (Reason, 1997) er et poeng her som kan gjøre at ledere glemmer å legge vekt på sikkerhetsarbeidet. Slurv eller lite kunnskap om digital sikkerhet nevnes som en av de største truslene mot en trygg informasjonsbehandling, og det er ikke uten grunn at kompetanse nevnes som en av de åtte nøkkelkomponentene til en digital sikkerhetskultur. Når informantene i denne studien blir spurt om de tror de har like mye, mindre eller mer kunnskap enn medarbeidere innenfor digital sikkerhet, sier samtlige at de tror de har mer kunnskap enn sine kolleger. Videre nevner ingen av dem at det noensinne slurves eller tas raske løsninger som de vet bryter regler for informasjonssikkerheten, til tross for at noen nevner at de har gjort eller gjerne gjør det privat. Det kan så klart være tilfelle at ingen av informantene faktisk har brutt noen regler for informasjonssikkerhet, ellers kan det tenkes at de som blir intervjuet ønsker å fremstille seg i et

godt lys når de besvarer spørsmålene. Dette kan være av flere grunner. Kanskje for å stille selskapet i et godt lys, eller at ikke de ønsker å innrømme feil de er klar over at de har gjort.

Når informantene blir spurt hva lederne gjør for å bygge en digital sikkerhetskultur nevnes det kursing. Noen sier det er kontinuerlig kurs, der de hele tiden må oppdatere seg innenfor sin teknologiske kompetanse og forståelse, imens andre hevder kursene er mer sporadiske og spesifikke. De to avdelingslederne jeg har pratet med, tar imidlertid de samme kursene som de andre medarbeiderne, noe som indikerer at kursene lages og styres på et høyere nivå enn på disse ledernes nivå. Det vil med andre ord si at avdelingslederne i studien ikke er så mye mer involvert i sikkerhetsarbeidet enn sine medarbeidere. Det kan ut fra dette stilles spørsmål til hvorfor vi automatisk tenker det er lederne som trenger å bry seg med å investere eller fokusere på sikkerhet hvis det ikke er de som har det endelige ansvaret bak dette arbeidet. Et enkelt svar på dette kan være at det er desto viktigere at lederne bryr seg om sikkerhet og går foran som et godt eksempel og bidrar til at det er en felles forståelse innad i avdelingen. Her er det viktig at lederen får frem at den digitale sikkerheten påvirker absolutt alle, og bidra til at hver enkelt medarbeider forstår viktigheten av dette individuelle ansvaret som har så mye å si for hele selskapet. «Sikkerhet er alles ansvar» må ikke bare være et tomt slagord, men implementeres som en del av organisasjonskulturen (Leveson, 2011).

Likevel kan det tenkes man har en vei å gå før lederne også faktisk forstår viktigheten og alvorligheten av sikkerhetsarbeidet, da de ikke jobber med dette i sine daglige oppgaver og gjerne ikke klarer å tenke seg hvor store konsekvenser et lite tasteklikk faktisk kan ha. Lederne sin oppgave må være å være pådriver for at individene i avdelingen opplever seg selv som en del av et større «digitalt felleskap» (Bergsjø, Windvik og Øverlier, 2020, s. 37), selv om ikke lederne nødvendigvis har mer forståelse rundt digital sikkerhet enn sine medarbeidere. Ledelse skaper kultur, og kulturen driver fellesskap og atferd hvor ansvarlighet og autoritet blir viktige elementer å være et godt forbilde på (Leveson 2011, s.177).

En bank eller et forsikringsselskap er et stort komplekst selskap. Noen ganger kan selskapets systemer, særlig når det kommer til teknologi, være så komplisert at det trosser forståelsen til alle, bortsett fra noen få eksperter som jobber med digital sikkerhet til det daglige (NSM 2019). Problemet med teknologi hevder Dyrhaug fra NSM er at vi ikke forstår hvilken fare vi faktisk står overfor og at vi ikke klarer å kjenne det med vår intuisjon hvis vi er nære å trykke på noe som kan ødelegge noe av betydning for selskapet, eller slippe uvedkommende inn i systemet.

Vi mennesker er ofte sårbarheten som blir utnyttet, og det er en økende trend som viser at kompleks teknologi fører til modusforvirring og nye typer menneskelige feil.

Det som er så komplisert med det digitale domenet er at farene ligger «skjult» på en helt annen måte enn tidligere. Før kunne man fysisk se én eller flere mennesker rane en bank, gjerne maskerte og bevæpnede. I dag kan svindelen skje på et blunk uten at noen legger merke til hvem som står bak angrepet. Derfor kan det også være vanskeligere å beregne hvordan man skal ligge i det Reason (1997, s.4) kaller for paritetssonen, hvor det ideelle er å møte produksjonen og/eller tjenester med tilstrekkelig sikkerhet. For mye digital sikkerhet eller for mye fokus på negative konsekvenser og risiko man er utsatt for, kan på den ene siden gjøre at ikke inntrengere klarer å komme til og at organisasjoner klarer å bevare sine egne og kundene sine verdier på en god måte.

På den andre siden kan det bli en utfordring å overinvestere i sikkerhet, hvis dette går utover kvaliteten av det selskapet leverer av produkter og tjenester til sine kunder. Dette samsvarer med det Reason (1997, s. 4) beskriver i modellen Unorcked Boat, der man ser at det ikke er lang vei til konkurs eller til katestrofe hvis man lar enten for mye fokus på produksjon eller for mye fokus på sikkerhet ta overhånd. Som også Leveson (2011, s.416) beskriver skal det være en myte at sikkerhet er i konflikt med å oppnå andre mål, men det kan tenkes at det er først når sikkerhetsarbeidet får for mye fokus at det kan gå på kompromiss med andre verdier i organisasjonen. Sikkerhetspolitikken og et felles sikkerhetsinformasjonssystem er dermed viktig er på plass og er effektive ut fra de sårbarhetene man ønsker å beskytte (Leveson 2011, s.177)

Delkonklusjon:

- Tillit til «de som driver med sikkerhet» er ikke nok for å sikre selskapet mot digitale uhell eller cyberangrep, og det å forstå at sikkerhet er alles ansvar er helt avgjørende for utvikling av en digital sikkerhetskultur.
- Det bør være forankret i ledelsen at det er et behov for digital sikkerhet, og lederne i avdelingene bør gå foran som et godt eksempel på hvordan «vi vil ha det hos oss». På denne måten integrereres tanken om et felleskap når det kommer til digital sikkerhet, og blir en naturlig del av kulturen som helhet.
- Kursing for å friske opp i digital forståelse er et virkemiddel for å holde de ansatte oppdaterte og oppmerksomme. Likevel kan kursene bli for hyppige og noen ganger oppleves lite relevante da kursene lages høyere oppe i systemet og sendes ut til alle uavhengig av hvilken stilling man har eller avdeling man tilhører.

6.2 «Hvilke rutiner er etablert for å vedlikeholde digital sikkerhet i organisasjonen?»

Hvordan digitale tjenester utvikles og tilbys, hvordan sikkerheten ivaretas, hvilke sikkerhetshendelser som skjer og hvordan de blir håndtert er faktorer som er med å påvirke ens holdninger og optimisme for teknologi (Bergsjø, Windvik og Øverlier 2020, s. 40). Virksomheter forventer at de ansatte skal følge reglene, og ikke utsette seg selv eller virksomheten for unødig risiko (Nettvett, 2020). Da kreves det kompetanse og læring (Daler m.fl. 2010, s. 407). Virksomheten må sørge for at de ansatte kan det som skal til for at de skal ta de riktige sikkehetsvalgene på jobb, og det må brukes metoder som faktisk motiverer og skaper læring hos de ansatte.

Kurs nevnes flest ganger når det kommer til det informantene i undersøkelsen nevner som det de tenker gjøres for å sikre digital sikkerhet. Kurs blir stadig nevnt under intervjuene, men veldig få av informantene kunne utdype hvor ofte disse blir holdt, eller hva disse kursene handler om. Styring og kontroll relaterer seg til felleskap og handler om hvordan fellesskapet skal reguleres. Sikkerhet starter ifølge Leveson (2011) med en klar ledelse og engasjement som deretter fører til gode og solide rutiner for å sikre at ikke noe uforventet skal skje. Ved å motivere medarbeiderne til å handle på en måte som ivaretar sikkerheten, får man også gjerne medarbeidere som ønsker å tenke sikkerhet i flere ledd. Som det kommer frem i definisjonen av en sikkerhetskultur så er det menneskenes holdninger og tenkemåte som er en vesentlig faktor for hvordan en organisasjon kan klare å tenke sikkerhet; «et sett med verdier som deles av medarbeidere i en virksomhet, og som er med på å påvirke deres tanker og forventinger til sikkerhet» (NSM, 2021).

Risikotrekanten beskriver at verdi, trusler og sårbarhet er avhengige av hverandre. Med andre ord er risiko et spørsmål om å kunne forstå sine egne sårbarheter (Bergsjø, Windvik og Øverlier, 2020, s. 39). I utgangspunktet kan vi dermed gå ut ifra at det er menneskene som jobber i organisasjonen som er nøkkelen til en god digital sikkerhetskultur. Det er imidlertid vi mennesker som også kan trykke på ukjente lenker i e-poster, logge oss inn på ukjente nettverk eller ta i bruk ukjente minnepinner, så det er altså også vi menneskene som er sårbarheten som kan bli utnyttet (NSM, 2019, s. 16). Kompetanse innenfor teknologi og digital sikkerhet, gjerne via kursing og andre godt etablerte rutiner, bidrar altså til økt digital sikkerhet, fordi menneskene i organisasjonen får et åpnere sinn og mer kompetanse innenfor fagområdet. Det kan tenkes at så lenge man aktivt vet hvor sårbarhetene befinner seg, er det mer sannsynlig å klare å sikre sine verdier mot digital kriminalitet hvis det skulle inntreffe. For å kunne forbedre

sikkerhetsarbeidet og øke kompetanse om sikkerhet, er det nødvendig å forstå hvordan organisasjoner lærer, og hva organisasjoner lærer. På denne måten kan man skape innsikt i hvordan de ansatte foretrekker å lære, samt hvem de lærer best fra. Dette kan ha stor innvirkning på hva man faktisk lærer, og hvor godt rustet man er til å motvirke digitale trusler (Bergsjø, Windvik og Øverlier 2020, s. 41).

Grunnen til at det er sårbarhetene man mener bør ha mest fokus i arbeidet med digital sikkerhet kan handle om at verdiene til organisasjonen er såpass implementert at disse ønskes å bevares slik de er. Man ønsker ikke å kvitte seg med verdiene sine for å unngå trøbbel, fordi at det er verdiene som gir organisasjonen den identiteten den har og den plassen organisasjonen har i markedet. Videre får man heller ikke gjort noe med trusselaktørene. For det første fordi du ikke får tak i de som sitter på den andre siden i det digitale domenet, og for det andre fordi du ikke vet hvem som sitter der. Da sitter man igjen med de svakhetene i de digitale systemene som røverne utnytter – menneskene. Det er av betydning å nevne at en sårbarhet kan være noe vi vil ha og man velger som oftest å ha mennesker som jobber i organisasjonen, selv om dette introduserer en viss svakhet ved systemet. Hvis en organisasjon er klar over de sårbarhetene man har, vet man også hvilke rutiner som vil sikre systemet mest mulig og som vil skape barrierer der hvor de er svakest. Det handler med andre ord om veien inn til sårbarhetene, og for å finne denne veien er det viktig å forstå hvilke verdier man har, hvilke trusler eller røvere som har lyst på verdiene og hvordan disse vil komme seg inn for å få tak i det de har lyst på.

Når man først er klar over hvor sårbarhetene i systemet ligger, er det en del av sikkerhetskulturen å ha den lovpålagte dokumentasjon på plass. Mange har hyllemeter med dokumenter fordi det ser pent ut og fordi man må, mens andre har erkjent et behov for det og ser verdien i disse papirene. Atferdsmønstre beskrives som en av de åtte dimensjonene som er nødvendig for en digital sikkerhetskultur. Sikkerhetskultur handler ifølge Dyrhaug om din atferd sett i forhold til situasjonen. Samspillet mellom hendelser og atferd vil forandre seg hele tiden, og det å forstå dette og være i stand til å endre seg i takt med alt annet som endrer seg er en god sikkerhetskultur. Han beskriver at; *«Sikkerhetskultur er til syvende og sist hva man gjør og hva man ikke gjør, når det å ikke gjøre noe er det rette å gjøre».*

Dyrhaug beskriver at det ofte er mismatch i organisasjoner mellom det de skriver og dokumenterer de skal gjøre og det de *faktisk* gjør. Andre ganger møter han organisasjoner som ikke har skrevet noen ting, men det de gjør funker. Her kan det diskuteres om det hjelper å ha dokumentasjon på plass hvis ikke man gjør det man skriver at man skal gjøre. Det kan altså

tenkes at det å ha en atferd innad i organisasjonen som reflekterer at man tenker på sikkerhet kan være både viktigere og mer meningsfylt enn det å ha dokumentasjon på plass uten handling. Med andre ord kan man tenke at det er en sterkere sikkerhetskultur når atferden reflekterer dette, enn der hvor dokumentasjonen er på plass, men atferdsmønsteret ikke samsvarer med det man har sagt man skal gjøre. Svært ofte viser det seg at bedragerier, misligheter og sabotasjer utføres av egne ansatte og ofte av medarbeidere i betrodde posisjoner (Daler m.fl. 2010, s. 78). Det kan i disse tilfeller stilles spørsmål til hvorvidt ledelsen har gjort sin plikt med hensyn til å utvikle et godt arbeidsmiljø, ivareta personalressurser og etablere gode kontrollrutiner (Daler m.fl. 2010, s. 79).

Hvordan sikkerheten ivaretas, hvilke sikkerhetshendelser som skjer og hvordan de blir håndtert er faktorer som er med å påvirke holdningene til det digitale, og derav også medarbeidernes vilje til digitalisering og optimisme for teknologi (Bergsjø, Windvik og Øverlier 2020, s. 40). Som vi ser ut fra rangeringen til informantene rangerer samtlige det som svært risikofylt å dele passord med andre. Det kommer også frem at det er etablert en rutine internt i organisasjonene at det kreves at man bytter passord på sine enheter hver tredje måned. Selv om informantene jobber i helt ulike selskaper, ser vi at praksisen er det samme. Ledelsen i de ulike selskapene innenfor bank og forsikring har gjerne erkjent og forstått hvor sårbart det kan være hvis man bevarer samme passord over tid, og medarbeiderne forstår antakelig viktigheten av å ikke dele passord med andre. Dette er et eksempel på en måte å tenke digital sikkerhet på som kan reflektere hvordan deres digitale sikkerhetskultur er og deres vilje til å ivareta den digitale sikkerheten i organisasjonen. Kompetanse, læring og risikoforståelse henger sammen (Bergsjø, Windvik og Øverlier, 2020, s. 39), og vi kan ut fra dette tenke oss at økt kompetanse og fokus på forståelse rundt risiko ved digital sikkerhet fører til læring og en felles systemtenkning, som videre kan føre til at medarbeidere gjør færre feil enn de ville gjort hvis digital sikkerhet ikke ble fokusert på.

Delkonklusjon:

- Metoder som motiverer og skaper læring om digital sikkerhet hos de ansatte er viktig for å skape årvåkenhet og bevissthet hos de ansatte. Det er ofte menneskene i organisasjonen som er den sårbarheten som trusselaktører vil utnytte. Derfor er det virksomhetskritisk å vite om hvor sårbarhetene befinner seg og ha sterke nok barrierer for at ikke disse skal bli utnyttet.

- Atferd og holdninger blant de ansatte sier mer om den digitale sikkerhetskulturen enn det de spesifikke rutinene eller dokumenter sier at de skal gjøre. Det er altså hva den enkelte medarbeider eller leder velger å gjøre (eller ikke gjøre) som sier noe om deres forståelse rundt digital sikkerhet.
- Rutiner for å sikre en digital sikkerhetskultur handler om å kartlegge hva som er tilstrekklig sikring mot uønskede hendelser. For å finne denne balansen må man forstå hvilke verdier man har, hvilke trusler eller røvere som har lyst på verdiene og hvordan disse vil komme seg inn for å få tak i det de har lyst på.

6.3 «Hvordan forstår de ansatte trusler og farer ved bruk av ny eller eksisterende teknologi?»

Tilsiktede uønskede digitale hendelser er et økende problem og kan utgjøre en alvorlig trussel mot norske selskaper og privatpersoner (NOU 2018: 14, s. 21). Risikopersepsjon handler om hvordan den enkelte bedømmer risiko for ulike aktiviteter og trusler (Renn, 2008). Hvordan personer og virksomheter oppfatter risiko vil variere fra person til person, både fordi man har ulike forutsetninger for å bedømme risiko ut fra de erfaringene man har, og fordi trusselbildet varierer fra virksomhet til virksomhet (Nettvett, 2020).

Som vi ser i cybersikkerhetsrapporten (2016) er interesse og vilje til digitalisering noe som viser seg å ha innvirkning på hvilken grad man forstår trusler og farer ved det digitale domenet. Som det kommer frem i rapporten: *«Interest in technology and ICT correlates with a pattern where people learn from experts, and from their own trial and error… interest correlates directly with a more secure behavioural pattern" (Malmedal og Røislien 2016, s.50).*

En bank håndterer åpenbare verdier, og derfor vil det i digitale domenet være enda viktigere at banken sikrer verdiene sine og at de ansatte forstår truslene man kan møte på. Trusler i det digitale domenet kan være direkte mot bankens kunder der forsøk på svindel er aktuelt og kan føre til store konsekvenser, og/eller mot interne systemer som kan være en enda større trussel for selve organisasjonen som helhet, men også for kundene som har lagret både sensitive personopplysninger og økonomiske midler i banken. Rekkevidden av ringvirkningene et digitalt angrep kan ha er stor, hvor det er flere ledd og avhengigheter som blir påvirket.

Tilfeldige systemer innad i en organisasjon er i økende grad utsatt ved at de kan bli utnyttet for videre nettverksoperasjoner mot andre mål (NOU 2018: 14, s. 21). Dette kan i prinsippet være hvilke som helst systemer som ikke er et mål i seg selv, men som fungerer som et mellomledd mellom en angriper og det egentlige målet (NOU 2018: 14, s. 21). Informantene fra bank og

forsikring viser ikke likevel ikke særlig bekymring for at noe skal skje i deres avdeling. Flere av informantene sier at de har tro på at selskapet har såpass gode rutiner at de ikke tror noe vil skje. Dyrhaug fra NSM hevder at vi burde stoppe opp og tenke oss om og sier at; *«Man skjønner ikke at man ikke skjønner cyberspace og datamaskiner. Det er egentlig forklaringen på alt».*

Risikoforståelse er en av de åtte faktorene som er viktig for en digital sikkerhetskultur. I en fersk rapport av NorSIS «Nordmenn og digital sikkerhetskultur 2021» kommer det frem at flere hundre tusen norske arbeidstakere mener de selv ikke kan vurdere om det er trygt å åpne en e-post (Lystad, 2022), mens i denne undersøkelsen er det kun 1 av 7 informanter som forbinder noe risiko ved bruk av e-post på jobb. Dette kan bety to ting; enten at informantene som er tatt ut til denne undersøkelsen er særlig kompetanserike når det kommer til teknologi og digital sikkerhet, ellers kan det være at de undervurderer hvor farlig det digitale domenet faktisk kan være. NSM NCSC erfarer at den mest vanlige måten for trusselaktører å komme seg inn i norske virksomheter er via e-post med vedlagt skadevare eller lenker (NSM 2019, s.15). Hele 5 av 7 informanter rangerer det å bruke e-post på jobb på 1, som viser til laveste risiko på skalaen. Dette begrunner informantene i at maskinen har programmer til å automatisk sile ut e-poster som virker suspekte og at disse ved ett tastetrykk kan sendes over til sikkerhetsavdelingen for klarering.

En annen utfordring er knyttet til om selskapet offentliggjør digitale sårbarheter eller eventuelle forsøk på angrep i selskapet. En forutsetning for å skape forståelse rundt digital sikkerhet, samt redusere og rette opp i sårbarheter er at man vet hvor sårbarhetene er (NOU 2018: 14, s. 62). Samtlige av informantene hevder at de ikke vet om at det har vært noen forsøk på tilsiktede digitale angrep eller utilsiktede digitale uhell så lenge de har jobbet der. Dette kan enten være av den grunn at det faktisk ikke er skjedd noen større hendelser, eller at selskapene ikke ønsker å vise frem sine digitale svakheter offentlig for å ikke virke som et lett mål som ikke har gode nok sikkerhetssystemer. Når det ikke snakkes om tidligere hendelser eller eventuelle situasjoner som kan oppstå kan det tenkes å være vanskelig for de ansatte å forstå at en slik hendelse faktisk kan skje. Likevel skal kurs i digital sikkerhet rette et fokus på truslene ved nettbruk og gjøre medarbeiderne bevisste på at utilsiktede eller tilsiktede digitale hendelser kan skje.

Tillit er en grunnleggende faktor som må være på plass for at man skal kunne imøtekomme digitaliseringen på en hensiktsmessig og trygg måte (Malmedal 2020, s. 23). De ansatte må ha tillit til at data om dem blir beskyttet og kun brukt til det som er avtalt, og ikke til noe som ikke er i deres interesse. De må også ha tillit til at de digitale tjenestene virker slik man har forutsatt,

og at de ikke inneholder feil som kan true de ansattes eller selskapets sikkerhet (Malmedal 2020, s. 23). Likevel bør ikke det å ha tillit forveksles med å fraskrive seg ansvar. Som nevnt tidligere i analysen virker det som både ledere og medarbeidere i undersøkelsen virker å vite lite om hvem som faktisk har ansvaret, og hevder at de må ha tillit til «de som jobber med sikkerhet». Ansvarsfraskriving når det kommer til digital sikkerhet kan utgjøre en stor trussel, fordi hvilken som helst e-post eller hvilket som helst system kan bli angrepet. Tar ikke man ansvar og lar være å melde fra om suspekte forhold og tenker at «dette blir ordnet i sikkerhetsavdelingen» kan det tenkes at det kan gå veldig gale og ha store konsekvenser for selskapet.

Videre er det av betydning å nevne at det kommer frem i en nylig rapport: «Nordmenn og digital sikkerhetskultur 2021» at nesten halvparten av alle nordmenn vet at arbeidsplassen har regler for digital sikkerhet. Imidlertid oppgir tre av ti nordmenn at de ikke ville fortalt ledelsen eller sikkerhetsavdelingen om det dersom de gikk på et svindelforsøk på nett (Lystad, 2022). Dette kan ifølge Leveson (2011, s.405) ha sammenheng med at det ikke er tydeliggjort godt nok i den digitale sikkerhetskulturen at slik rapportering ikke vil komme med noen negative konsekvenser for noen enkeltpersoner. Tvert imot burde de ansatte få belønning for å rapportere eller videreføre så viktig sikkerhetsrelatert informasjon som (Reason 1997) beskriver som en «just-culture»/en rettferdig kultur. Det er som nevnt en trend at mennesker angripes i større grad enn maskiner. Da er kunnskap om truslene og lav terskel for å varsle viktigere enn noensinne (Lysand, 2022).

Dyrhaug fra NSM beskriver at han ofte møter ledere som sier at «*det er han som er ansvarlig, det er han som driver med sikkerhet».* Dyrhaug beskriver dette som en misforståelse. Det er jo ikke bare de i sikkerhetsavdelingen som driver med sikkerhet. Sikkerhetsavdelingen skal *legge til rette* for sikkerhet, men resten av de ansatte i organisasjonen jobber også med daglig gjennomføring av sikkerhet. Det er ikke de som jobber i sikkerhetsavdelingen som trykker på lenker i e-poster – det kan være en rådgiver i bank eller en takstmann i forsikring som da må vite hva man skal eller ikke skal gjøre i denne situasjonen. Det skal nevnes at informantene er klar over hvilke retningslinjer som gjelder hvis det skulle oppstå en situasjon der de er usikre, og her nevnes rapportering til sikkerhetsavdeling og å snakke med sine ledere. Likevel kan det ifølge Dyrhaug være vanskelig å forstå faren ved digitale trusler før det er for sent, fordi vi ikke har noe digital intuisjon og kjenner på fare på samme måten som hvis vi står ved et stup.

En av nøkkelkomponentene for en digital sikkerhetskultur er de ansattes interesse og holdninger til digitalisering. Holdningene til digitale tjenester påvirker måten man forholder seg til

teknologi (Malmedal 2020, s. 12). Mistillit til digitale tjenester, eller frykt for sikkerhetshendelser og datakriminalitet, er noen av utfordringene som de fleste organisasjoner må forholde seg til. Hvordan digitale tjenester utvikles og tilbys, hvordan sikkerheten ivaretas, hvilke sikkerhetshendelser som skjer og hvordan de blir håndtert, vil påvirke holdningene til det digitale domenet (Malmedal 2020, s. 12). Den enkeltes holdning til det digitale blir derfor en faktor som kan bidra til å beskrive den digitale sikkerhetskulturen.

I undersøkelsen bes respondentene å ta stilling til noen påstander som beskriver holdningene deres til teknologi. Samtlige av informantene i undersøkelsen rangerer seg på (1) at de er svært positive til teknologi. Holdningene deres vil være med å prege hvorvidt man forstår farer ved det digitale domenet eller ikke og hvorvidt man ønsker å sette seg inn i ny eller eksisterende teknologi. Ifølge NorSIS (2016) kan man være fristet til å konkludere med at personer med interesse for teknologi har større fordel når det gjelder digitalisering fremfor de som mangler denne interessen, nettopp fordi interessen former våre holdninger (Malmedal & Røislien 2016, s. 34). Med interesse kommer også bevissthet og nysgjerrighet som er viktige grunnpilarer for læring og viktig for å kunne forstå tusler og farer teknologien introduserer oss for.

Delkonklusjon:

- Det kan være vanskelig å forstå faren ved digitale trusler før det er for sent, fordi vi ikke har noe digital intuisjon og kjenner på fare på samme måten som hvis vi står ved et stup.
- En hovedutfordring er at hver enkelt medarbeider eller leders forståelse rundt digital sikkerhet vil variere fra person til person. Det å få alle til å få en felles tankegang rundt sikkerhet er derfor avgjørende og vil ha en innvirkning på i hvilken grad de ansatte vil forstår trusler og farer ved det digitale domenet.
- Tillit er en nøkkelutfordring, men ser også ut til å være en del av løsningen. Den enkelte medarbeider må stole på at selskapet har rutiner som sikrer mot digitale tusler, mens ledelsen må ha tillit til at de ansatte melder fra om forhold som kan være kritisk hvis disse skulle oppstå. Tillit må imidlertid ikke forveksles med ansvarsfraskriving. Sikkerhet er alles ansvar, og hver enkelt medarbeider og leders atferd bør reflektere en sikkerhetsorientert tankegang.

7.0 Konklusjon

Denne oppgaven omhandler en særdeles aktuell tematikk som gjør seg gjeldende for absolutt alle organisasjoner. Studien bidrar til å belyse viktigheten av digitalt sikkerhetsarbeid og hvor avgjørende en sikkerhetsorientert tankegang blant de ansatte er for deres digitale sikkerhetskultur. Oppgaven baserer seg i hovedsak rundt relevante dokumenter fra aktuelle kilder, samt åtte kvalitative intervjuer. Til sammen skaper disse et grunnlag for å 1) diskutere hva ledere gjør i arbeidet med digital sikkerhet, 2) se på hvilke rutiner som er etablert for å vedlikeholde digital sikkerhet og 3) hvordan de ansatte forstår trusler og farer ved bruk av ny eller eksisterende teknologi.

Disse holdepunktene danner strukturen i oppgaven, samt et grunnlag for å reflektere rundt problemstillingen: *Hva er de viktigste utfordringene innenfor bank – og forsikringsbransjen for å utvikle en digital sikkerhetskultur?* Det er gjennomgående i oppgaven rettet et fokus både på utilsiktede digitale uhell, og på tilsiktet datakriminalitet, såkalte «cyberangrep». I denne sammenhengen diskuterer jeg åtte dimensjoner som skal sikre en digital sikkerhetskultur i en organisasjon; fellesskap, styring og kontroll, tillit, risikoforståelse, vilje til digitalisering, kompetanse, interesse og atferdsmønstre.

Det kommer frem at det ofte er usikkerhet rundt hvem som faktisk har ansvaret for sikkerhet, og at de aller fleste automatisk har tillit til at «de som jobber med sikkerhet» tar seg av arbeidet rundt dette. Digitaliseringen er både avhengig av, og sårbar for tillit, og det kan virke som tillit er sentralt når det kommer til informantenes forståelse av digitale sikkerhet. Sammenhengen mellom tillit og ansvarsfraskrivelse blir diskutert og en delkonklusjon er at den digitale sikkerheten er *alles* ansvar, også de som ikke jobber med sikkerhet i det daglige.

Videre kommer det frem at menneskene i organisasjonen ofte er den sårbarheten som trusselaktørene velger å utnytte. I denne diskusjonen kommer det frem at kompetanse innenfor teknologi og digital sikkerhet, gjerne via kursing og andre godt etablerte rutiner, bidrar til økt digital sikkerhet fordi menneskene i organisasjonen får mer kompetanse. Den enkelte medarbeiders risikoforståelse og tankegang rundt sikkerhet kan derfor bidra til å unngå eventuelle hendelser. I denne sammenhengen blir fellesskap og en kultur som setter sikkerhet høyt på agendaen viktig.

Nøkkelutfordringen knyttet til digital sikkerhetskultur handler om at teknologien er mer komplisert og farligere enn vi kan forstå. Nasjonal sikkerhetsmyndighet konkluderer med følgende; *«Man skjønner ikke at man ikke skjønner cyberspace og datamaskiner. Det er egentlig forklaringen på alt».*

8.0 Litteraturliste

Bergsjø, H., Windvik, R., & Øverlier, L. (2020). Digital Sikkerhet. En innføring, 1.

Blaikie, N. & Priest, J. (2019). *Designing Social Research.* (3. utg). Polity.

Charpenter, Perry. (2022). Back To Basics: Cybersecurity Is Everyone's Job. Forbes. Lest 08.02.2022. https://www.forbes.com/sites/forbesbusinesscouncil/2022/02/08/back-to-basics-cybersecurity-is-everyones-job/?sh=2d97992c57e5

Daler, T., Gulbrandsen, R., Høie, T. A., & Sjølstad, T. (2010). Håndbok i datasikkerhet: informasjonsteknologi og risikostyring. 3 utgave. Tapir Akademisk Forlag, Trondheim 2010.

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

Jacobsen, D. Ingvar og Thorsvik, J (2019). Hvordan organisasjonen fungerer. 5. utgave. Bergen: Fagbokforlaget.

Johannessen, A., Tufte, P. A. & Chrisoffersen, L. (2016). *Introduksjon Til Samfunnsvitenskaplig Metode* (bd. 5). Oslo: Abstrakt forlag AS.

Lavender, A. (2010). Digital Culture. In A. Lavender, S. Bay-Cheng, C. Kattenbelt, & R. Nelson (Eds.), Mapping Intermediality in Performance (pp. 125–134). Amsterdam University Press. http://www.jstor.org/stable/j.ctt46mwjd.23

Leveson, N. (2011). *Engineering a Safer World. Systems Thinking Applied to Safety.* The MIT Press.

Lystad, Elise. (2022). Ny Norsis-rapport: nordmenn sliter med sikkerhet. Computerworld. Lest 08.2.2022. https://www.cw.no/norsis-rapport-sikkerhet/ny-norsis-rapport-nordmenn-sliter-med-sikkerhet/1672915

Malmedal, B og Røislien, H. E (2016). The norwegian cyber security culture. NorSIS; Norsk senter for informasjonssikring. https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf

Moriset, B., & Malecki, E. J. (2009). Organization versus space: The paradoxical geographies of the digital economy. Geography Compass, 3(1), 256-274.

NHO (2022). NHO Rogaland. Publisert 21.01.2022. Lest 08.2.2022 https://www.nho.no/regionkontor/nho-rogaland/artikkelarkiv/1-av-5-bedrifter-rammet-av-dataangrep/

NSM (2019). *Helhetlig digitalt risikobilde 2019.* https://nsm.no/getfile.php/133669-1592830841/Demo/Dokumenter/Rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf

NSM (2020). *NSMs grunnprinsipper for IKT-sikkerhet. 2 versjon.* https://nsm.no/getfile.php/133735-1592917067/Demo/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

NSM (2022a*). Tiltak for skjerpet digital beredskap.* https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/nyheter-fra-ncsc/digital-beredskap-i-en-skjerpet-situasjon/
NSM (2022b) *Råd og anbefalinger om passord.* https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord

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

Standard Norge (2012) Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger-terminologi (NS 5830:2012).

Standard Norge (2014) Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse (NS 5832:2014).

Stromquist, Lars. (2008) Et sikkert IT-miljø : hva små og mellomstore bedrifter må vite for å kunne skape et sikkert IT-miljø. 3 utgave. Sverige: Symantec.

Tjora, Aksel Hagen. 2020. *Kvalitative forskningsmetoder i praksis*. 3. utgave. Oslo: Gyldendal akademisk.

Karlsen, J. E. (2010). Ledelse av helse, miljø og sikkerhet (3. utg., p. 257). Fagbokforl.

Kaufmann, Geir og Astrid Kaufmann (2015). *Psykologi i Organisasjon og Ledelse.* 5. utgave. Bergen: Fagbokforlaget.

Kreuter, M.W. og Stretcher, V.J. (1995). Changinginaccurate perceptions of health risk: Results from a randomized trial.

Krumsvik, Rune Johan (2014) *Forskningsdesign og kvalitativ metode*. Bergen: Fagbokforlaget.

Schein, Edgar H (1987) *Organisasjonskultur og ledelse - er kulturendring mulig?* Oslo: Libro forlag AS.

Bilde på forsiden: https://www.dreamstime.com/lock-digital-background-cyber-security-internet-security-security-concept-lock-icon-circuit-board-technology-image133647799 Hentet 4 juni 2022.

Vedlegg 1: Samtykkeskjema

Samtykkeskjema

Bakgrunn og formål med studien

Hensikten med intervjuet er å undersøke hva som er de viktigste utfordringene i utviklingen av den digitale sikkerhetskulturen i organisasjonen. Dette for å bidra til mer innsikt og forståelse for hvordan kultur, risiko og sikkerhet henger sammen og hvorfor det er viktig å investere i digital sikkerhet i fremtiden.

Personopplysninger

Det vil ikke bli samlet inn personopplysninger, og intervjuet, informanten og bedriften blir anonymisert.

Kryss av om du godtar følgende:

☐ Jeg forstår at min deltakelse er frivillig og at jeg har rett til å trekke meg fra forskningen dersom jeg ønsker det, uten å oppgi en grunn.

Respondent:

Dato:_____ Signatur:_____

Forsker:

Dato:_____Signatur:_____

Vedlegg 2: Intervjuguide

INTERVJUGUIDE

Generelle innledende spørsmål:
• Alder:
• Hvor lenge har du jobbet i organisasjonen og hva er din funksjon?
• Fortell kort om din utdanning/akademiske bakgrunn?

DEL 1 – *Generell risikoforståelse*

Når vi skal se nærmere på generell risikoforståelse ønsker jeg først å høre mer om hvordan du ser på trygg nettbruk i et samfunn der teknologi blir stadig viktigere.

Jeg vil si noen raske påstander og jeg ønsker at du rangerer hvor enig du er i påstandene fra 1-5.

1) Helt enig? 2) Delvis enig? 3)Nnøytral 4)Delvis uenig? 5) Helt uenig? Eller vet ikke?

1) Du er positiv til teknologi
2) Du vet hva informasjonssikkerhet er
3) Du utsetter deg selv for risiko når du bruker internett
4) Det er greit at din aktivitet på internett blir overvåket dersom det fører til at du blir tryggere på nett
5) Du har tillit til at myndigheter sikrer informasjonen de har registrert på deg.

BEKYMRINGER
Ranger fra 1-5 hvor bekymret du er for at det følgende skal skje. 1) ikke bekymret, 5) svært bekymret.

→ At dine dokumenter skal bli ødelagt på dine enheter?
1-5?

→ Få virus på pcen din?
1-5?

→ At du blir lurt til å gi fra deg sensitiv informasjon?
1-5

→ At du trykker på en lenke du tror er ekte men som er svindelforsøk?
1-5?

→ At noen skal utgi seg for å være deg på nett? *1-5?*

DEL 2 - *Hva gjør lederne i arbeidet med digital sikkerhet?*

Nå vil jeg gjerne spørre deg om hva du er opptatt av og hvordan du skaffer deg kunnskap om informasjonssikkerhet, og dermed komme litt nærmere inn på hva du gjør i arbeidet med digital sikkerhet.

1 → Kan du si noe om din interesse for teknologi og IT generelt?

Eventuelt oppfølgingsspørsmål:
Kan du mer eller mindre om informasjonssikkerhet i forhold til andre medarbeidere/ledere tror du?

2 → Hvordan lærer du vanligvis om informasjonssikkerhet?

Og spesifikk til ledere:
→ Hvordan sørger du for at dine ansatte lærer om informasjonssikkerhet?

3. → Har du ***fått*** noe opplæring i informasjonssikkerhet/digital sikkerhet i løpet av de siste årene?

Ekstra til lederne:
Har du ***gitt*** noe opplæring i informasjonssikkerhet/digital sikkerhet i løpet av de siste årene?

4 → Når noen blir nyansatt hos dere... Hva *gjøres* for å sikre at medarbeideren lærer om / forstår viktigheten av informasjonssikkerhet?

DEL 3 - *Rutiner*

→ Har arbeidsplassen regler for informasjonssikkerhet, hvilke eventuelt?

→ Hvilken sikkerhetsprogramvare har du på din pc på arbeid?

→ Undersøker du om en nettside er trygg før du bruker den?

→ Hvor ofte endrer du passord på enheter eller brukerkontoer du benytter deg av?

→Hvor ofte sikkerhetskopierer du data som er viktige for deg?

→Har du rutiner for å oppdatere programmene dine på maskinen din på jobb?

ENDRINGER....

→ Har det vært noen forsøk på svindel eller datakriminalitet de siste fem årene?
Fortell gjerne om type forsøk. Når?

Oppfølgingsspørsmål hvis ingen hendelser. → Hvorfor tror du at dere har klart å unngå det?

→ Er det innført noen regler, tiltak eller rutiner på grunn av noen spesifikke hendelser med forsøk på datakriminalitet/digitale uhell?
Oppfølgingsspørsmål hvis ja → Hvordan fungerer disse i dag?

Er det noe du tenker kunne vært gjort annerledes i rutiner som ville bidratt til økt sikkerhet mot digitale angrep?

Del 3 – teknologi og trusler

→ Hender det at du har bevisst brutt regler for informasjonssikkerhet? Hva skjedde/ hvordan håndterte du situasjonen?

→ Hvordan vurderer du hva som er trygt eller utrygt å gjøre på nett?

→ Hvor synes du det er viktigst å tenke informasjonssikkerhet?

→ Hva mener du er den største risikoen på nett?

→Hva gjør du hvis du blir utsatt for nettsvindel på jobb?

RISIKO
Hvor stor risiko forbinder du med følgende aktiviteter?
1 liten risiko – 5 stor risiko

→ Hvor stor risiko forbinder du med å bruke e post på jobb?
1-5?

→ Dele passord med andre?
1-5?

→ Bruke samme passord på flere nettjenester?
1-5?

→ Bruke bank eller kredittkort på nett?
1-5?

→ Å ikke ta sikkerhetskopi?
1-5?