Hvilke faktorer kan forklare ansattes bruk av sikkerhetstiltak på mobile enheter når de er ute på farten?

Ole Reidar Holm og Frode Mathias Bekkevik

Veileder

Tom Roar Eikebrokk

Masteroppgaven er gjennomført som ledd i utdanningen ved Universitetet i Agder og er godkjent som del av denne utdanningen. Denne godkjenningen innebærer ikke at universitetet innestår for de metoder som er anvendt og de konklusjoner som er trukket.

Universitetet i Agder, 2018
Fakultet for samfunnsvitenskap
Institutt for informasjonssystemer

“Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted. None of these measures address the weakest link in the security chain.”

– Kevin Mitnick

Forord

Denne avhandlingen markerer avslutningen og resultatet av to masterstudenters innsats i informasjonssystemer ved Universitetet i Agder (UiA). Godt samarbeid, kameratskap og mange strevsomme timer har bidratt til at vi nå kan pakke sammen skolesekken og endelig trekke inn i de voksnes rekker.

Målet med studien er å avklare om det finnes faktorer som forklarer ansattes bruk av informasjonssikkerhetstiltak når de er ute på farten. Informasjonssikkerhet er et tema vi begge er svært interessert i og har gitt oss mye motivasjon gjennom semesteret.

Det har vært noen innholdsrike måneder. Utredningen du nå leser har vært krevende og interessant på samme tid. Heldigvis er god hjelp ikke langt unna, og i den forbindelse er det flere vi må takke. Først ønsker vi å takke veileder Tom Roar Eikebrokk for konstruktive innspill og tilbakemeldinger underveis i arbeidet. Det har vært noen lange økter med diskusjon på kontoret, men takket være hans smittende humør og analytiske ferdigheter, kom vi frem til perspektiver og løsninger vi tvilsomt hadde fått til uten hans hjelp.

Studien hadde ikke blitt til uten gode kontaktpersoner i deltakende organisasjoner. Vi ønsker å rette en stor takk til dere for eksepsjonell innsats og nyttige svar. Videre ønsker vi å takke alle respondenter for at de tok seg tid til å delta i studien til tross for en travel arbeidsdag.

Vi ønsker spesielt å takke våre foreldre, besteforeldre og venner for deres hjelp med rettlesing, støtte og tålmodighet gjennom flere år som studenter.

Til slutt er det verdt å nevne at Universitetet i Agder, spesielt Informasjonssystemer, har en «slagside» mot kvantitative studier. Det finnes få eksempler på kvantitative masteroppgaver tilgjengelig. Denne studien gir forhåpentligvis fremtidige studenter nyttige tips og triks til deres kvantitative studie.

Kristiansand, 01. juni 2018

Ole Reidar Holm

Frode Mathias Bekkevik

Sammendrag

Kontekst: Brukeren er ofte omtalt som den største trusselen mot informasjonssikkerhet i virksomheter. I dag bruker de fleste en eller flere mobile enheter på jobben. Sammen med mobile enheter kommer også nye farer knyttet til informasjonssikkerhet, og det er derfor svært viktig at ansatte bruker anbefalte sikkerhetstiltak når de er på jobben, men også utenfor virksomheten. Målet med studien er å analysere hvilke faktorer som kan forklare bruk av sikkerhetstiltak på mobile enheter utenfor organisatoriske rammer («ute på farten»).

Målsetting: Denne avhandlingen rapporterer resultater fra en studie der det er brukt elementer fra kjente atferds- og personlighetsteorier for å se på faktorer som kan forklare holdninger til og faktisk bruk av informasjonssikkerhetstiltak på mobile enheter ute på farten.

Metode: Det er brukt en deduktiv forskningstilnærming, gjennomført en systematisk litteraturstudie og diskutert sikkerhetstiltak med eksperter innen informasjonssikkerhet. Det er gjort en oppsummering av risikoer samt tiltak med mobile enheter, atferdsteorier og personlighetspsykologi fra litteraturen. Deretter er det utført en empirisk studie med 210 respondenter som ofte jobber utenfor organisatoriske rammer med mobile enheter.

Resultater: Studien etterspurte forskjellige faktorer som kan forklare respondentenes holdninger til bruk og faktisk bruk av sikkerhetstiltak ute på farten. De ulike faktorene var: Personlighetstrekk, tro på egen mestringsevne, kjennskap til sikkerhetstiltak, normer, egenskaper med sikkerhetstiltak, kvalitet på support og antatt kontroll over atferd.

Alle faktorene ble testet i forhold til hvor godt de kunne forklare holdninger til bruk og faktisk bruk av sikkerhetstiltak. Studien fikk støtte for totalt fem av ni hypoteser. Den sterkeste sammenhengen ble funnet mellom oppfattet nytteverdi med sikkerhetstiltak og holdninger til bruk.

De positive signifikante sammenhengene i studien er:

- Normer --> holdninger til bruk av sikkerhetstiltak
- Nytteverdi med sikkerhetstiltak --> Holdninger til bruk av sikkerhetstiltak
- Brukervennlighet med sikkerhetstiltak --> Holdninger til bruk av sikkerhetstiltak
- Holdninger til bruk av sikkerhetstiltak --> Faktisk sikkerhetsatferd
- Kvalitet på support --> Faktisk sikkerhetsatferd

Personlighetstrekk («*Five-Factor Model*») ble også testet mot holdninger til bruk. Her ble det ikke funnet en signifikant sammenheng, men det var nært. Personlighetstrekkene planmessighet og ekstroversjon bidro mest til denne relasjonen.

Implikasjoner for praksis:

- Ansatte lytter til sine overordnede. Informer derfor ansatte om viktigheten av å bruke sikkerhetstiltak, også utenfor virksomheten.
- Lag tydelig definerte sikkerhetsrutiner som er enkle for ansatte å følge utenfor virksomheten. Sikkerhetstiltak bør være kortfattede og enkle å sette seg inn i.
- Skap en god sikkerhetskultur i virksomheten. Fokuser på én gruppe om gangen.
- IT-hjelp er en god støttespiller for ansatte ute på farten. Sørg for at IT-hjelp har nok kunnskap til å hjelpe ansatte med sikkerhetsrutiner utenfor virksomheten. Opplæring bør være adskilt fra hverdagslige oppgaver.

Konklusjon: Totalt sett viser resultatene fra studien at tidligere atferdsteorier kan forklare sikkerhetsatferd på mobile enheter utenfor virksomheten. Studien bidrar til å forstå hvilke faktorer som kan forklare ansattes bruk av sikkerhetstiltak når de er ute på farten, et relativt nytt fenomen i forskningen. Virksomheter kan bruke denne studien til å forbedre sitt fokus på informasjonssikkerhet med mobile enheter.

Nøkkelord: Informasjonssikkerhet, mobile enheter, holdninger til bruk, atferd, personlighetstrekk, Theory of Planned Behavior, Technology Acceptance Model, IS-Success Model, Five Factor Model

Innhold

Tabeller

Figurer

1. Innledning

Samfunnet man kjenner i dag har gått gjennom en enorm transformasjon de siste tiårene. Informasjons- og kommunikasjonsteknologi (IKT) har spilt en avgjørende rolle i denne transformasjonsprosessen og har blitt en stor del av manges sosiale liv (Kakihara & Sorensen, 2002). I dag har livsstilen endret seg gradvis fra en tradisjonell livsstil, hvor en startet og sluttet på jobb med faste tider, til en mobil livsstil hvor en kan jobbe stort sett hvor som helst takket være teknologiske fremskritt (Makimoto, 2013).

Ordet «mobil» kommer fra det latinske ordet *movere* som betyr «sette i bevegelse» (Språkrådet & Universitetet i Bergen, 2016). Å være mobil dreier seg ikke om mennesker som reiser, men det handler om muligheten til å være fleksibel i forhold til hvor og når en gjør ting, for eksempel i en jobbsetting (Kakihara & Sorensen, 2002). Makimoto & Manners argumenterte i boken deres, Digital Nomad (1997), at menneskeheten ville bli «geografisk uavhengig» i fremtiden ved at en stor del av tingene og verktøyene hjemme og på kontoret ville bli så små at de kunne bæres i lomma. Som en oppfølging av denne boken skriver Makimoto (2013) at man nå lever i et samfunn fylt av digitale nomader og svært sjeldent møter en forretningsmann uten smarttelefon. Nomader er folk som skifter boplass og stadig er på vandring (Sommerfeldt & Benjaminsen, 2017).

Mobile enheter har blitt en stor del av livene våre (NKOM, 2017). Takket være styrken og påliteligheten av Wifi- og mobilnettverk, samt den økende delen av usikrede offentlige nettverk, tillater brukere å være tilkoblet i mange forskjellige miljøer og situasjoner mellom hjemme og arbeidsplassen. Skiftet fra disklagring til skylagring er et godt eksempel på endring i teknisk infrastruktur og grensesprengende teknologier (Agudelo et al., 2016). Til tross for produktivitets- og effektivitetsgevinstene, kommer mobile enheter også med utfordringer knyttet til informasjonssikkerhet. Temaet informasjonssikkerhet er et viktig og dagsaktuelt tema som har utviklet seg i tråd med digitaliseringen. Innen norsk forskning har temaet fått mye oppmerksomhet. Det er blant annet opprettet ulike faggrupper innenfor temaet, som for eksempel NTNU CCIS, Sintef Informasjonssikkerhet og Difi Informasjonssikkerhet.

Ifølge rapporten «*The Norwegian Cyber Security Culture*» av Malmedal og Røislien (2016), har kun halvparten av ansatte i norske virksomheter fått opplæring i informasjonssikkerhet. I en casestudie fra Logan og Logan (2003), der en virksomhet ble lammet av malware, kunne mye av skaden vært forhindret med gode sikkerhetsholdninger blant de ansatte. God informasjonssikkerhet krever mer enn gode tekniske løsninger og høye ambisjoner. Selv om mange norske virksomheter har administrative og tekniske tiltak på plass, må de også tenke over ansattes holdninger, kunnskap og atferd. Ansatte blir ofte sett på som den svakeste lenken innen informasjonssikkerhet i virksomheter og er et område som har fått mye oppmerksomhet i forskningsverdenen, se for eksempel: (Ashenden & Sasse, 2013; Bulgurcu, Cavusoglu & Benbasat, 2010; Hagen, Albrechtsen & Johnsen, 2011).

I en virksomhet finnes det flere typer mennesker og personligheter. Det kan være store forskjeller mellom disse menneskene og hvilke informasjonssikkerhetsrisikoer de utgjør. Det finnes minst to motsettende personligheter (A og B). Personlighet A kan være opptatt av

kvantitet over kvalitet. De jobber fort og illustrerer hvor kompetente de er i form av arbeidstimer, men gjør ofte dårlige beslutninger fordi de jobber for fort. Personlighet B fokuserer på kvalitet, stresser aldri over tidspress, og tenker ofte to ganger før de gjør noe. Det finnes også ulike individuelle og personlige faktorer som alder, sivilstatus, utdanning, emosjonelle rammer, verdier og grunnleggende forutsetninger (Da Veiga & Eloff, 2010).

Det er viktig å notere seg at bruken av beskyttende teknologier, for eksempel antivirusprogrammer og brannmurer, er situasjonsavhengig. I de fleste organisasjoner er beskyttende teknologier allerede installert og kjører automatisk. Den enkelte ansatte vil derfor ikke bekymre seg for dette i en allerede stressende arbeidsdag. Derimot, når den ansatte er hjemme, er det opp til en selv å innføre de sikkerhetstiltakene som er nødvendig. Det som gjør saken enda mer komplisert, er at disse to tilsynelatende totalt forskjellige miljøene (hjemme og på jobb) ofte blandes. Det blir stadig flere som bruker bærbar datamaskin, mobiltelefon og/eller nettbrett både hjemme og i en jobbsetting (Bello, Armarego & Murray, 2015; Thompson, McGill & Wang, 2017), noe som fører til en rekke sikkerhets- og personvernsrisikoer (Alsaleh, Alomar & Alarifi, 2017; Das & Khan, 2016; Hovav & Putri, 2016).

Al-Hadadi og Al Shidhani (2013) illustrerer at de fleste smarttelefon-brukere ikke vet hva de skal gjøre eller hvem de skal rapportere til dersom de opplever et sikkerhetsrelatert problem med enheten sin. Studien viser også en mangel på bevissthet til informasjonssikkerhet blant de studerte brukerne. Forskerne foreslår å fokusere på de menneskelige eller personlige faktorene rundt informasjonssikkerhet, fremfor å øke de tekniske sikkerhetstiltakene på smarttelefonen.

Å beskytte personlig og organisatorisk informasjon krever en bevisst og aktivt bruk av informasjonssikkerhetstiltak både hjemme og på jobb (Dinev & Hu, 2007). Dermed er det viktig å forstå hvordan brukere ser på ulike trusler og hvordan de velger å bruke beskyttende teknologier designet for å hjelpe dem å redusere eller eliminere risikoen.

1.1. Problemstilling

Informasjonssikkerhet generelt har fått mye oppmerksomhet i forskningen. Det finnes allerede en del forskning på sikkerhetsbevissthet blant brukere av mobile enheter (se for eksempel: (Alsaleh et al., 2017; Gkioulos et al., 2017; Zhang, Li & Deng, 2017) og overholdelse av sikkerhetsregler (Bulgurcu et al., 2010; Safa, Von Solms & Furnell, 2016; Siponen, Mahmood & Pahnila, 2014)), men svært få har tatt for seg hvorvidt individuelle og personlige faktorer kan påvirke brukerens mobile sikkerhetsatferd i en organisatorisk kontekst.

Mobile enheter brukes både innenfor og utenfor organisasjonen. Når en ansatt jobber utenfor organisasjonen, er ute på forretningsreise, eller av andre grunner oppholder seg i det offentlige rom, må den ansatte selv passe på å følge anbefalte informasjonssikkerhetsretningslinjer. Hvordan ansatte forholder seg til bruken av sikkerhetstiltak når de er utenfor organisatoriske rammer, er en studie vi ikke har sett i tidligere IS-litteratur. Denne studien har dermed som mål å adressere dette forskningsgapet

ved å analysere ulike faktorer som kan forklare brukerens holdninger til bruk av sikkerhetstiltak på mobile enheter «ute på farten».

Studien tar for seg følgende problemstilling:

Hvilke faktorer kan forklare ansattes bruk av sikkerhetstiltak på mobile enheter når de er ute på farten?

I et forsøk på å besvare problemstillingen bygger studien en teoretisk modell inspirert av tidligere atferds- og personlighetsforskning. Modellen inneholder variabler hentet fra «*Theory of Planned Behavior*», «*Technology Acceptance Model*», «*Five Factor Model*» og andre kjente teorier fra litteraturen.

1.2. Motivasjon

IT-sikkerhet, personvern og håndteringen av dette er et interessant tema, spesielt for bedrifter som til daglig jobber aktivt med dette. Temaet er svært aktuelt i dag, hvor bedrifter besitter enorme mengder sensitive forretningsdata som er kritisk for virksomheten og må håndteres riktig.

Tidligere erfaring fra offentlig sektor bidro til å aktualisere problemstillingen for denne studien. Her har det blitt observert alt fra hvordan organisasjoner henger opp gule lapper med passord, til hvor lett det er å søke opp noen man kjenner i en database. Personlige interesser og erfaring fra arbeidslivet har gitt en stor motivasjonsfordel, alt fra menneskelige faktorer til tekniske detaljer. Det ville vært svært interessant og sett i hvilken grad ansatte forstår hvorfor man praktiserer informasjonssikkerhet, og i hvilken grad de følger retningslinjene for dette.

1.3. Oppbygging og innhold

- Kapittel 2 presenterer det teoretiske grunnlaget for studien og er delt opp i to deler. I første del gjennomføres en relativt omfattende systematisk litteraturgjennomgang. Deretter beskrives relevant teori for å bygge den konseptuelle forskningsmodellen. Til slutt følger en oppsummering og diskusjon av teoriene.
- Kapittel 3 tar for seg forskningsmodellen og hypotesene.
- Kapittel 4 forklarer forskningstilnærmingen, operasjonalisering av spørsmål, metode for datainnsamling og dataanalyse, samt kravene til reliabilitet og validitet.
- Kapittel 5 rapporterer resultatene fra studien.
- Kapittel 6 diskuterer studiens resultater, implikasjoner for forskning og praksis, samt begrensninger.
- Kapittel 7 presenterer studiens konklusjon, før referanser og vedlegg.

2. Teoretisk grunnlag

Denne delen av rapporten inneholder en gjennomgang av relevant litteratur rundt temaet informasjonssikkerhet og mobile enheter. For å få innsikt i sikkerhetspraksis med mobile enheter, er det gjennomført en litteraturstudie basert på Kitchenham (2004). I neste del er det presentert sentrale områder fra et avgrenset område innen informasjonssystemer. Formålet med litteraturgjennomgangen er å presentere en relativt omfattende gjennomgang av litteratur omkring sikkerhetspraksis og atferds- og personlighetsteorier.

Tidligere forskning på temaet er viktig for å få dyp innsikt i problemområdet og for å finne eventuelle gap i forskningen. Da det ble søkt etter litteratur, var det viktig å forsikre seg at artiklene var fra anerkjente fagfellevurderte tidsskrifter. Dette var for å forsikre at kilden er lest gjennom og kvalitetssikret av flere fagpersoner før den er publisert.

Det er viktig å være kildekritisk og søke i kjente databaser. Kildekritikk dreier seg kort fortalt om å vurdere avsenderen av informasjonen og troverdigheten til informasjonen (Orgeret, 2017). I praksis betyr dette å se på kilden med kritiske øyne og stille seg selv noen ulike spørsmål. Eksempler på ting man bør fokusere på er: Forfatter, struktur, aktualitet, kvalitet, referanser og hvor den er publisert (Kildekompasset, 2016). For å finne kjente akademiske søkemotorer og databaser, ble biblioteksiden til Universitetet i Agder benyttet. Under denne siden ligger det blant annet lenker til Oria, Google Scholar, Web of Science og fagsiden til Informasjonssystemer.

2.1. Litteraturstudie

Litteraturstudien er utført som en systematisk litteraturgjennomgang («*systematic litterature review*») basert på Kitchenham (2004). Kitchenham (2004) er ei anerkjent forsker som har skrevet gode guider for hvordan gjennomføre slike litteraturstudier (se for eksempel Kitchenham et al. (2009)), og vi valgte derfor å lytte til disse veletablerte rådene for litteraturstudien.

Tradisjonelle litteraturgjennomganger kan ofte bli unøyaktige eller mangelfulle fordi de ikke følger klare og eksplisitte retningslinjer. Slike litteraturgjennomganger mangler en slags oppskrift på hvordan man skal gå frem for å rapportere og filtrere funnene.

2.1.1. Litteraturstudiens problemstilling

Denne litteraturstudien har tatt for seg følgende problemstilling:

> **«Hvilke risikoer og tiltak rundt temaet sikkerhetspraksis ved bruk av mobile enheter har blitt adressert i tidligere forskningslitteratur?»**

2.1.2. Søkestrategi og -kriterier

For å finne relevante studier til litteraturstudien, ble det definert ulike søkeord og -kriterier. Slike kriterier bidrar til å øke litteratursøkets troverdighet og gir mer passende artikler (Kitchenham, 2004). Dette er et dynamisk felt hvor trusler og tiltak er i rask utvikling og det er dermed særlig viktig å fokusere på nyere artikler. Utvalgskriteriene for å filtrere vekk irrelevant litteratur var:

1. Fagfellesvurderte tidsskrifter
2. Engelskspråklig
3. Artikkel i tidsskrift
4. Fulltekst tilgjengelig
5. Publisert i 2008 og senere

Søkeordene bestod av relevante kombinasjoner ved sikkerhetskonteksten, samt ulike varianter av mobilkonteksten (illustrert i tabellen under). Primærsøkeordet (A) er sikkerhet og sekundærsøkeordet (B) er mobile enheter med tilhørende terminologi.

Kategori	Forklaring	Søkeord
A	Sikkerhetskontekst	Security behavi* Security exposure Security incident Security awareness Security risk*
B	Mobil kontekst	Mobile device* Mobile context Mobile computing Smartphone Mobile phone Bring your own device BYOD

Tabell 1 – Søkeord i litteraturstudie

Dersom et ord er sammensatt av flere, ble det brukt et anførselstegn for å øke søkets relevans. Videre ble «AND» og «OR» operatorene benyttet for å konkretisere søket enda mer. AND-operatoren sørget for at primærsøkeordet (A) og sekundærsøkeordet (B) begge måtte være tilstede. OR-operatoren passet dersom søkeordet hadde flere betydninger, eller hvis det var behov for en kompleks søkestreng.

Erfaring viste at noen databaser ikke inkluderte ord med en annen bøyningsform enn det som ble søkt etter. I slike situasjoner ble det anvendt en stjerne (*****) for å inkludere flere betydninger av samme søkeord. For eksempel vil «*behavi**» inkludere ord som «*behaviour*»

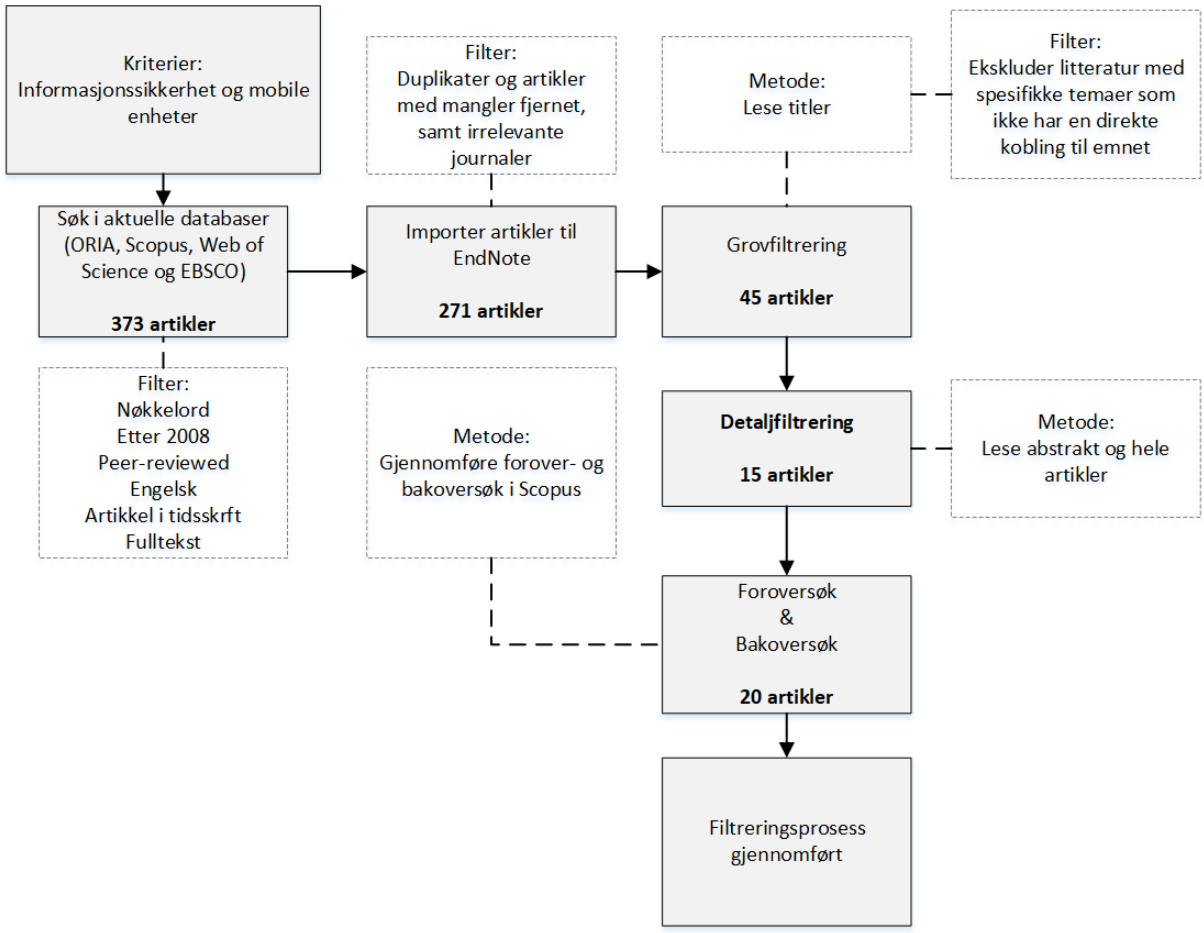
og «*behavior*». En komplett oversikt over utførte søk finnes i **Tabell 2 – Søkekriterier i litteraturstudie**.

NR.	Primær	Sekundær	Database	Begrensninger	Treff
1	A	B	EBSCO-host	Peer-reviewed, engelsk, artikler, år 2007<, fulltekst	18
2	A	B	ORIA	Peer-reviewed, engelsk, artikler, år 2007<, fulltekst	142
3	A	B	Scopus	Peer-reviewed, engelsk, artikler, år 2007<, fulltekst	165
4	A	B	Web of Science	Peer-reviewed, engelsk, artikler, år 2007<, fulltekst	48

Tabell 2 – Søkekriterier i litteraturstudie

2.1.3. Utvalgsstrategi og evaluering av kvalitet

Utvalgsprosessen er skissert som følgende:



Figur 1 – Utvalgsprosess i litteraturstudie

Det ble søkt i til sammen fire databaser. Alle søketreff der fulltekst var tilgjengelig ble lagt inn i kildehenvisningsprogrammet EndNote. Her ble artiklene delt inn i fire kataloger, slik at

det skulle være enklere å vite hvilken database artikkelen var hentet fra. Eksempelvis fikk kombinasjonen Primærsøkeord (A) og Sekundærsøkeord (B) en egen kategori med treff fra de fire databasene (EBSCO, ORIA, Scopus og Web of Science). På denne måten kunne relevante treff fra de ulike databasene enkelt sammenliknes.

Duplikater ble fjernet etter at søketreffene var eksportert. Deretter ble det opprettet noen utvalgskriterier for å konkretisere videre. Målet med kriteriene var at det skulle bli lettere å fjerne irrelevante artikler. Utvalgskriteriene er listet opp i **Tabell 3 – Utvalgskriterier i litteraturstudie**.

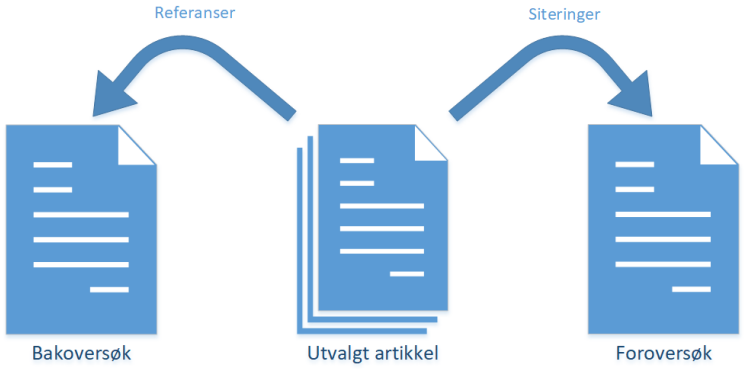
Utvalgskriterier	
Kriterier	Beskrivelse
Et eller flere av søkeordene må være nevnt i tittelen	For å sikre at artikkelen er spisset mot riktig tema må et eller flere av søkeordene være nevnt i artikkeltittelen.
Ekskluder litteratur med spesifikke temaer som ikke har en direkte kobling til emnet	Mobile enheter og informasjonssikkerhetskontekster har sosiale og tekniske aspekter. Spesielle teknologiske aspekter, for eksempel kryptografi, sikkerhet i mobiloperativsystemet og liknende blir ekskludert.
Ekskluder artikler fra journaler som ikke skriver om IS-relaterte temaer	Journaler som ikke omfatter informasjonssystemer er irrelevant. For eksempel medisin, jus og industri.
Ekskluder artikler med feil eller mangler	Artikler med mangelfull informasjon blir fjernet. For eksempel hvis artikkelen ble importert uten forfatter og/eller journal o.l.

Tabell 3 – Utvalgskriterier i litteraturstudie

Alle titlene ble lest over for å bestemme hvilke artikler som skulle beholdes. Titlene ble sammenliknet for å se om det var enighet om hvilke artikler som innehold riktige kriterier. For å øke litteraturens relevans og redusere litteraturgrunnlaget ytterlige, ble det gjennomført en kvalitetsvurdering av hver enkelt artikkel. Dette ble gjort ved hjelp av en utvalgsprosess som har til hensikt å øke kvaliteten av det endelige resultatet. En slik kvalitetsvurdering bidrar til å avdekke artikkelens grad av relevans (viktighet) i forhold til tema.

Etter at abstraktene var lest, var det 30 artikler igjen i utvalget. Disse (30) utvalgte artiklene ble lest i fulltekst. Deretter ble artiklene gjennomgått i plenum, som en siste sjekk mot kriteriene. Til slutt bestod utvalget på 15 relevante artikler.

For å identifisere ytterligere artikler, ble det gjennomført ulike bakover- og foroversøk. Et bakoversøk vil si å «se tilbake» ved å søke etter relevant litteratur i referansene til en utvalgt artikkel. Motsatt, vil et foroversøk «se fremover» ved å søke etter relevant litteratur som har sitert en utvalgt artikkel.



Figur 2 – Bakover- og foroversøk i litteraturstudie

Bakover- og foroversøkene ble gjennomført i Scopus. Bakoversøkene resulterte i to artikler og foroversøket tre artikler. Det endelige utvalget ble på 20 relevante artikler og framgår i **Vedlegg A – Artiklene fra litteraturstudie**.

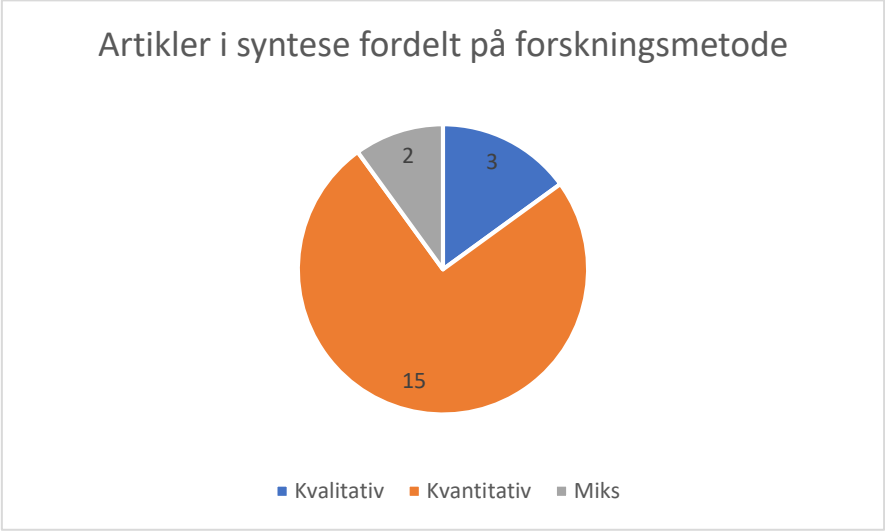
2.1.4. Datainnsamling og -analyse

En artikkelmartrise ble opprettet for å samle inn og strukturere data fra artiklene. Matrisen ble kontinuerlig endret underveis, dermed ble konsepter, kategorier og annet lagt til og/eller fjernet gjennom hele prosessen.

Artikkelmatrisen er delt inn i to deler. Først presenteres en metaanalyse og deretter funnene i studien. Funnene representerer erfaringer fra de forskjellige studiene, og er delt opp i to kategorier: «identifiserte risikoer» og «tiltak for å løse risikoen». Ideen er hentet fra Webster & Watson (2002) som skriver at litteraturgjennomgangen bør være konseptstyrt istedenfor forfatterstyrt.

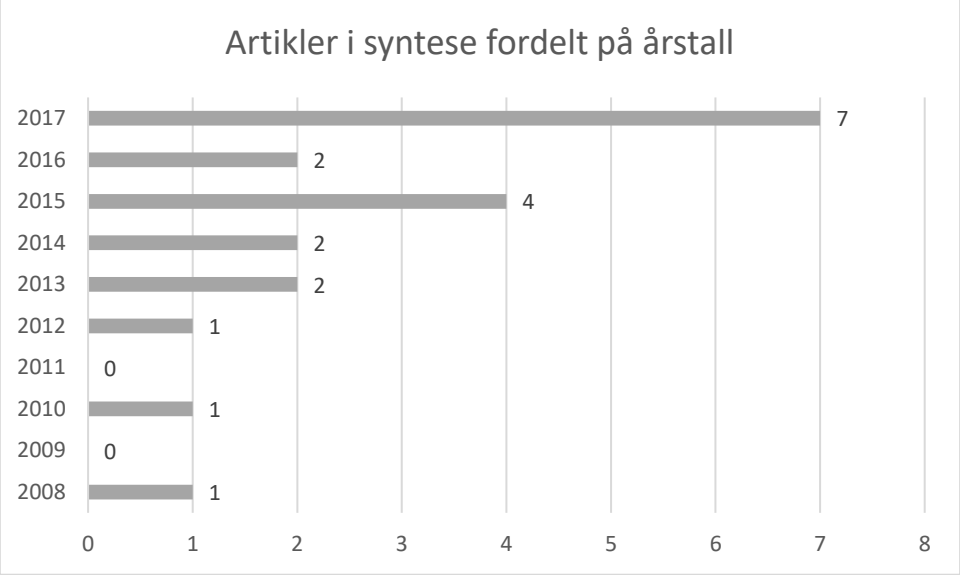
Analyse av metadata

For å få en bedre oversikt over artiklene, ble det gjennomført en metaanalyse. Av totalt 20 artikler hadde 15 artikler brukt kvantitativ og 3 kvalitativ forskningsmetode. De resterende 2 brukte en blanding av metodene.



Figur 3 – Fordeling av artikler (forskningsmetode) i litteraturstudie

Teknologien har forandret seg mye de siste 10 årene. Det var derfor viktig at artiklene i syntesen var forholdvis nye. 7 av artiklene var publisert i 2017. Dette kan tyde på at mobile enheter har vært et aktuelt forskingsemne det siste året.



Figur 4 – Fordeling av artikler (årstall) i litteraturstudie

Studiene er høyest representert i Europa med 7 artikler, der 2 av dem ble utført over flere kontinenter. Resterende studier er fra Asia, Australia, Sør-Afrika og Nord-Amerika.

Ståstedet til informantene ble også tatt med. Det ble det delt opp i 5 underkategorier med leder/management, ansatt, ekspert/forsker, hjemmebruker eller student. Her kom det frem at 6 av artiklene omhandlet studenter. Det var overaskende mange artikler som studerte studenter i forhold til ansatte.

Det ble skilt mellom privat og organisatorisk kontekst. Artikler hvor brukeren brukte smarttelefonen både hjemme og på jobb fikk to markeringer og forklares som et miljø der enheten ble brukt både i privat- og i jobbsammenheng. Til sammen omhandlet 9 artikler i en blandet kontekst, 2 i privat kontekst og de resterende i organisatorisk kontekst.

Analyse av konsepter

Her presenteres funnene fra litteraturstudien. Funnene ble lagt opp i en artikkelmatrise basert på Webster og Watson (2002). Artikkelmatrisen inneholder forskjellige konsepter identifisert ut ifra problemstillingen til dette studiet. Først blir de ulike risikoene presentert, etterfulgt av de løsninger som foreslås i litteraturen. Underkapitlenes oppbygning starter med å presentere kategoriene for så å gå i dybden på de individuelle funnene som er gjort.

Kategori	Forfatter	Alsaleh, Alomar & Alarifi (2017)	Bello, Armarego & Murray (2015)	Bello, Murray & Armarego (2017)	Bonne et al. (2017)	Das & Khan (2016)	Gkioulos et al. (2017)	Goode, A. (2010)	Harris Mark & Patten Karen (2014)	Harris, Ives & Junglas (2012)	Hovav & Putri (2016)	Markelj & Bernik(2015)	McGill & Thompson (2017)	Mylonas, Kastania & Gritzalis (2013)	Ngoqo & Flowerday (2015)	Pramod & Raman (2014)	Shih et al. (2008)	Thompson, McGill & Wang (2017)	Tu et al. (2015)	Uffen, Kaemmerer & Breitner (2013)	Zhang, Li & Deng (2017)
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	Bruker	x	x	x	x	x	x	x	x			x	x	x	x	x		x	x	x	x
	Enhet	x		x			x		x		x			x		x	x				x
Sikkerhetsrisikoer knyttet til	Organisasjon		x	x						x	x		x				x		x	x	
	Opplæring og sikkerhetskampanjer		x	x		x					x	x	x		x					x	x
	Tekniske sikkerhetskontroller og -applikasjoner	x	x	x	x		x		x	x	x	x	x	x		x	x	x	x		x
	Organisatoriske regler og standarder		x	x	x	x		x	x	x	x						x				
	Kunnskapsdeling og samarbeid	x		x									x					x	x		
Tiltak for å minske risikoen	Toppledelsens engasjement			x				x	x								x		x		

Tabell 4 – Funn fra litteraturstudie (konseptmatrise)

Sikkerhetsrisikoer med mobile enheter

I alt ble det identifisert tre generelle sikkerhetsrisikoer med mobile enheter:

- Sikkerhetsrisikoer knyttet til brukeren av enheten (17*)
- Sikkerhetsrisikoer knyttet til enheten (9*)
- Sikkerhetsrisikoer knyttet til organisasjonen (8*)

Disse risikoene er ikke gjensidig utelukkende. I en gitt situasjon vil man ofte møte en eller flere av sikkerhetsrisikoene sammen. Eksempelvis kan sikkerhetsrisikoene til brukeren trigge en eller flere sikkerhetsrisikoer knyttet til enheten og organisasjonen samtidig.

** Tallet i parentes representerer antallet artikler som tok for seg risikoen.*

Sikkerhetsrisikoer knyttet til brukeren av enheten

Ansatte blir ofte sett på som den svakeste lenken i informasjonssikkerheten i virksomheter (Bulgurcu et al., 2010). Når det gjelder mobile enheter er det ikke annerledes. Etter at bruken av smarttelefoner skjøt i været i 2013, dukket det også opp nye sikkerhetsrisikoer relatert til brukeren (Harris & Patten, 2014). Uvitende brukere kan finne på å laste ned skadelig programvare, koble seg til usikrede nettverk og gjøre annet som kan gi alvorlige konsekvenser for dem selv, samt virksomheten de jobber i (Alsaleh et al., 2017; Bello et al., 2015; Bello, Murray & Armarego, 2017; McGill & Thompson, 2017).

McGill og Thompson (2017) skriver at brukere er mer villige til å innføre sikkerhetstiltak på datamaskinen enn på mobiltelefonen. Brukerne i undersøkelsen mente at det var større sannsynlighet for at datamaskinen ble utsatt for en sikkerhetsrisiko enn smarttelefonen deres. At brukeren mangler risikoforståelse, kommer også frem i artikkelen til Bonne et al.

(2017). De undersøkte brukerne tok ikke hensyn til hvilke risikoer som kan oppstå ved å koble seg til et åpent nettverk, eller når de gir en applikasjon tilgang til deres mobile enhet.

Das og Khan (2016) studerte sikkerhetsatferden til smarttelefonbrukere. Resultatene fra denne studien viser at brukere ofte gjør dårlige sikkerhetsbeslutninger. Dårlige sikkerhetsbeslutninger kan for eksempel være å ikke ha PIN-kode, droppe å oppdatere programvare regelmessig, ingen bruk av antivirusprogramvare og/eller lagre konfidensiell informasjon på enheten (passord, detaljer for å logge inn i nettbanken, forretningshemmeligheter, o.l.).

Mylonas, Kastania og Gritzalis (2013) skriver at de fleste av smarttelefonbrukere tror det er helt risikofritt å laste ned applikasjoner fra det offisielle applikasjonsbiblioteket (App Store, Google Play, o.l.). Applikasjoner fra disse bibliotekene kan inneholde skadevare og dermed sette konfidensiell informasjon i fare (Gkioulos et al., 2017; Mylonas et al., 2013; Tu et al., 2015). Brukere har også en tendens til å ignorere advarsler, noe som er utfordrende siden advarslene ofte informerer om sikkerhetsproblemer, for eksempel feil i SSL-sertifikatet og forsøk på phishing (Mylonas et al., 2013).

Ifølge Alsaleh et al. (2017) er den vanlige mobilbrukeren flink til å bruke låsekode på enheten. 70% av de undersøkte låste mobilenheten med PIN-kode, fingeravtrykk eller mønster. Av de som brukte PIN-kode, indikerte litt over halvparten (65%) at PIN-koden deres var koblet til en viktig dato eller et telefonnummer. Overraskende nok var det kun halvparten av de undersøkte som oppga at de låste telefonen for å forhindre innsyn av en ukjent tredjepart. Resten låste telefonen fordi de ikke ville at familie, barn eller venner skulle få tilgang til telefonen deres.

Et spennende funn fra denne studien er at atferden relatert til låsing av enhet korrelerer med praksis knyttet til sikkerhetskopiering, lagring av bilder i tredjepartsapplikasjoner og tilkobling til åpne offentlige nettverk. Eksempelvis vil det være mer sannsynlig at en person som ikke låser telefonen, også lagrer bilder i tredjepartsapplikasjoner, kobler seg til åpne offentlige nettverk og dropper å sikkerhetskopiere enheten sin (Alsaleh et al., 2017). Bonne et al. (2017) kan bekrefte at brukere ofte verken tenker på sikkerhet eller hvilke risikoer det innebærer å koble seg til et åpent nettverk.

Demografi spiller også en viktig rolle i brukernes sikkerhetsatferd, hvor noen grupper oppfører seg sikrere enn andre grupper. I forbindelse med låsing av enhet ble det observert at de under 36 år var flinke til å låse mobiltelefonen og generelt flinkere på sikker mobilatferd (Alsaleh et al., 2017). Det er også forskjell i hva slags mobilatferd det er snakk om. Den yngre generasjonen (også kjent som «*digital natives»*), er villige til å utsette seg for andre typer sikkerhetsrisikoer, som å laste ned applikasjoner fra ikke-autoriserte biblioteker eller ved å tukle med operativsystemet («*Jailbreak/Rooting*») for å få tak på ekstra adganger og applikasjoner på smarttelefonen eller nettbrettet sitt (Gkioulos et al., 2017). Yngre brukere har også en tendens til å prioritere brukervennlighet og ytelse (batteritid, lagringskapasitet, hastighet, o.l.) fremfor sikkerhet på mobile enheter (Das & Khan, 2016; Gkioulos et al., 2017; Pramod & Raman, 2014).

I virksomheter er det nå blitt normalt at ansatte tar med seg sin egen enhet. Dette skaper et større skadeomfang dersom brukeren skulle bli utsatt (Mylonas et al., 2013). Brukeren risikerer å sette både personlig- og jobbrelatert informasjon i fare. I en undersøkelse fra Bello et al. (2015), sier over 60% seg uenige i at virksomheten skal ha kontroll over enheten i et slikt miljø. Det var heller ingen som sa seg villige til at enheten skulle bli overvåket og sporet av virksomheten. Ansatte mener at å miste eller få enheten stjålet, er en av de største risikoene knyttet til mobil sikkerhet. Chin et al. (2012) argumenterer for at redselen kommer fra frykten av å miste data på enheten.

Sikkerhetsrisikoer knyttet til den mobile enheten

Mobiltelefoner har i nyere tid blitt en bærbar datamaskin man tar med seg overalt. Det økende antallet smarttelefoner og nettbrett har ført til at hackere ser større muligheter for å tjene penger. Skadevare («*malware*») blir nå spredt gjennom flere kanaler enn tidligere. Tidligere var det vanlig at skadevare ble spredt gjennom e-post og i nettleseren på en datamaskin. Nå kan skadevare bli spredd gjennom sosiale medier, SMS, Bluetooth, interne applikasjoner, trådløse nettverk m.fl. Skadevare er beregnet å koste virksomheter globalt milliarder av dollar årlig, og skaper mye frustrasjon for både brukerne og virksomheter (Shih et al., 2008).

Litteraturen beskriver også forskjeller i operativsystemene. Android, et operativsystem eid av Google (Ulseth, 2012), kan kategoriseres som et «åpent» operativsystem som lar brukeren konfigurere det meste selv. At brukeren får muligheten til å kontrollere det meste selv åpner for andre sikkerhetsrisikoer enn dersom brukeren ikke hadde samme muligheter. iOS, et operativsystem utviklet av Apple (Ulseth, Abrahamsen & Aleksandersen, 2017), gir brukeren mindre muligheter til konfigurering, som igjen gir brukeren mindre muligheter til å velge bort sikkerhet (Harris & Patten, 2014).

Dette gjelder kun dersom operativsystemet ikke er tuklet med. Å modifisere operativsystemet, kalt «*Rooting*» på en Android-enhet og «*Jailbreaking*» på en iOS-enhet, åpner for flere muligheter og tredjepartsapplikasjoner. I det offisielle applikasjonsbiblioteket kan brukere laste ned programmer til enheten sin. Apple sitt applikasjonsbibliotek (App Store) stiller høyere krav til applikasjonene enn det Google (Google Play Market) gjør. Android-enheter på den andre siden viser deg hva slags rettigheter applikasjonen trenger, men tillater også å laste ned applikasjoner fra en tredjepart. Ulempen med å kunne laste ned fra ukjente sider og tredjepartsbiblioteker, er at man ikke vet hva programvaren inneholder og kan dermed inneholde skadevare (Chin et al., 2012; Harris & Patten, 2014; Pramod & Raman, 2014; Zhang et al., 2017).

Sammen med mobile enheter, har også trådløse nettverk blitt utbredt de siste årene. Folk kobler seg til åpne nettverk så fort de får muligheten til det uten at de enser risikoen dette representerer (Bonne et al., 2017). Ved tilkobling til et usikret åpent nettverk (trådløst nettverk uten passordbeskyttelse) risikerer brukerne å få all nettverkstrafikken overvåket. Et slikt nettverk kan tvinge enhetene til å bruke ukryptert kommunikasjon, noe som betyr at all internettrafikk foregår i klartekst (inkludert passord).

Sikkerhetsrisikoer knyttet til organisasjonen

Det er ingen tvil om at det finnes mange fordeler med datadrevne og alltid-tilgjengelige mobile enheter, men hvilke implikasjoner vil de gi for informasjonssikkerheten i virksomheten? Informasjonssikkerhetsmål må være samordnet med de formelle forretningsprosessene for at de skal kunne gi gode resultater. Selv om det eksisterer ulike informasjonssikkerhetsstandarder for å koble forretningsprosesser og sikkerhet sammen, er ofte virkeligheten litt mer kompleks enn som så.

I denne studien defineres informasjonssikkerhetsregler og -rutiner som de roller og ansvarsområder ansatte gjør for å sikre ressursene til organisasjonen. Sikkerhetsreglene («*Information System Policy*», ISP) inneholder etablerte standarder og regler som forklarer ansatte hva de skal gjøre for å beskytte virksomhetens ressurser. Mange virksomheter har ikke utformet regler og prosedyrer for hvordan ansatte skal håndtere den mobile enheten (Bello et al., 2017; Goode, 2010). Et resultat av manglende ISP er at virksomheter i økende grad vil være sårbare for tap av konfidensiell informasjon og andre ISP-relaterte sikkerhetsrisikoer (Bello et al., 2017).

Mobile enheter i en virksomhetskontekst kommer med flere risikoer. Ansatte kan for eksempel miste mobilenheten (Tu et al., 2015), laste ned skadevare (Shih et al., 2008), bruke usikrede nettverk (Bonne et al., 2017), snakke høyt i telefonen eller jobbe på offentlige steder. Derfor dreier en stor del av det å beskytte virksomhetens ressurser om å styre ansatte i riktig retning. I en «*Bring Your Own Device*» (BYOD) kontekst har det vist seg å være vanskelig å innføre informasjonssikkerhetsregler som alle ansatte godtar. BYOD kan defineres som det å bruke personlige eide enheter i en jobbsetting (Bello et al., 2017), eksempelvis ved å bruke din egen personlige telefon til å svare på jobbrelaterte e-poster.

Selv om enhetene er eid av de ansatte, tilhører imidlertid ressursene organisasjonen (for eksempel e-post, applikasjoner og nettverkstrafikk). Et organisatorisk forsøk på å kontrollere de ansattes personlige enheter kan bli sett på som en trussel mot den ansattes privatliv (Hovav & Putri, 2016). Organisasjoner har derfor begynt å se på egne strategier for å takle eierskapskonfliktene som kan oppstå i kontekster der ansatte har med personlig eide enheter med på jobben(Harris, Ives & Junglas, 2012).

Tiltak for å løse risikoen

Artiklene fra søket foreslår fem generelle tiltak for å minske sikkerhetsrisikoene med mobile enheter:

- Opplæring og sikkerhetskampanjer (9*)
- Tekniske sikkerhetskontroller og -applikasjoner (16*)
- Organisatoriske regler og standarder (9*)
- Kunnskapsdeling og samarbeid (5*)
- Toppledelsens engasjement (5*)

** Tallet i parentes representerer antallet artikler som tok for seg tiltaket.*

Opplæring og sikkerhetskampanjer

Opplæring og sikkerhetskampanjer er en av de viktigste måtene å rette opp mangelen på sikkerhetsbevissthet i en virksomhet (Chin et al., 2012; Das & Khan, 2016). Opplæring blir også sett på som en effektiv måte å utvikle et godt BYOD-styringssystem ved å forme brukernes sikkerhetsholdninger på en positiv måte og eliminere negative oppfatninger (Bello et al., 2017; Markelj & Bernik, 2015).

Organisasjoner bør passe på at ansatte får den tiden de trenger for å sette seg inn i og bli flinkere med sikkerhet. Det er ikke noe nytt at mennesker ser på forandringer som stress. Opplæringen bør være atskilt fra hverdagslige oppgaver, for å gi ansatte spillerom til å fullføre kurset i eget tempo. Det holder ikke kun å utføre et opplæringskurs eller en sikkerhetskampanje. Det er viktig at det er en kontinuerlig prosess i virksomheten for å holde sikkerhetsbevisstheten til de ansatte på topp (McGill & Thompson, 2017).

For å få best mulig effekt ut av sikkerhetsopplæringen bør organisasjoner skreddersy programmet, slik at alle ansatte forstår innholdet og viktigheten av det. Sikkerheten i virksomheten må ikke bli sett på som en byrde, men som en del av hverdagen (Thompson et al., 2017).

Tekniske sikkerhetskontroller og -applikasjoner

Tekniske sikkerhetskontroller og -applikasjoner er de tiltakene som er foreslått av flest forfatterne i denne studien. Sikkerhetskontroller kan forklares som alle de tekniske tiltak en organisasjon eller en bruker innfører for å minske risikoen for sikkerhetsbrudd. Innenfor de mange sikkerhetskontrollene finner man tekniske tiltak på enheten, fra automatiske oppdateringer og fjerntjenester (tjenester for å slette innhold eller finne en tapt enhet utenfra) til virksomhetsstyrte tiltak for eksempel enhetsstyring. For å få brukere til å ta i bruk tekniske sikkerhetskontroller og -applikasjoner, må brukervennlighet vektlegges. Årsaken er at brukerne ofte ikke ønsker å bruke masse tid på å lære seg å forstå kompliserte programmer, bare for å sikre noe de i utgangspunktet tror er sikkert (Alsaleh et al., 2017; Chin et al., 2012; Gkioulos et al., 2017; Hovav & Putri, 2016).

Ifølge Harris og Patten (2014), Zhang et al. (2017) og Shih et al. (2008) bør det installeres sikkerhetsapplikasjoner på mobile enheter på lik linje med andre datamaskiner. Om mulig bør det også benyttes *Virtuelt Privat Nettverk* (VPN) for en sikrere tilkobling på internett. Et annet viktig sikkerhetsaspekt er å ha kontroll over alle enheter som er i virksomhetens nettverk, med muligheten til å fjernslette enheter som ikke er lenger i bruk.

Store virksomheter bør også vurdere to-faktor autentisering for ekstern tilgang. Kombinasjonen av enheten og personlig passord er en god måte å øke sikkerheten i virksomheten. Dersom virksomheten har ekstra god råd bør det innføres enhetsstyringssystemer og virtualisering. Enhetsstyringssystemer for mobile enheter kalles «*Mobile Device Management*» (MDM) og gir virksomheten full kontroll over hvilke enheter som blir benyttet innad i virksomheten. I større virksomheter har dette blitt vanligere å ha, og ansatte blir tvunget til å koble enheten til systemet før de får tilgang på virksomhetens informasjon. Med virtualisering logger man inn via en tynnklient til en annen maskin, noe som sikrer at informasjon aldri ligger på selve enheten (Hovav & Putri, 2016).

Organisatoriske regler og standarder

Virksomhetene bør sikre seg et omfattende og tilstrekkelig sett med informasjonssikkerhetskomponenter for mobile enheter. Det vil si at virksomheten selv må passe på at de ikke har hull eller mangler innen informasjonssikkerhet. Ledelsen bør arbeide tett med informasjonssikkerhetssjefen og gå sammen gjennom alle sikkerhetstiltakene. Det er spesielt viktig at informasjonssikkerhetsreglene dekker alt relevant, og at ansatte har muligheten til å lese reglementet når de ønsker (Bello et al., 2017; Markelj & Bernik, 2015).

Goode (2010) skriver at virksomheter bør bruke en kravspesifikasjon ved innkjøp av mobile enheter. Mobile enheter med lavere sikkerhet vil da bli utelukket, og sikkerhetsrisikoene knyttet til brukerfeil vil også reduseres.

Kunnskapsdeling og samarbeid

Kunnskapsdeling er en viktig faktor for å få til informasjonssikkerhet. Ansatte som diskuterer og deler sikkerhetskunnskap og -erfaringer skaper en positiv effekt på hvordan de håndterer sikkerheten (Alsaleh et al., 2017; McGill & Thompson, 2017). Virksomheter som ikke har kjøpekraft til enhetsstyringssystemer og enheter til sine ansatte, bør sikre at de ansatte har en god plattform for å dele kunnskap (Harris & Patten, 2014).

Toppledelsens engasjement

Kulturen blir ikke formet av hva ledelsen sier eller publiserer. Det er viktig at ledelsen ikke bare forutsetter at noe er viktig, men også konsekvent følger opp og støtter beslutningene som tas (Harris & Patten, 2014). Ledelsen bør stå frem og gjøre det klart at enheter som benyttes både i privat- og jobbsammenheng kan skape større sikkerhetsrisikoer for virksomheten (Goode, 2010), og at alle enheter kan bli utsatt for sikkerhetsbrudd (Shih et al., 2008; Tu et al., 2015).

2.1.5. Diskusjon og videre forskning

Under litteraturstudiet kom det frem noen spennende funn som utgjør grunnlag for diskusjon. *Tekniske sikkerhetskontroller og -applikasjoner* var tiltaket som ble nevnt flest ganger. Dette kan ved første øyekast virke selvforklarende. Tekniske sikkerhetskontroller og -applikasjoner er en god kombinasjon for å isolere de fleste sikkerhetstrusler. Det er imidlertid mennesker som utgjør den største informasjonssikkerhetsrisikoen, og det er begrenset hva de tekniske sikkerhetskontrollene strekker til ved menneskelig feil.

Diverse risikoer knyttet til brukeren av enheten kan løses ved *opplæring og sikkerhetskampanjer*. Opplæring og sikkerhetskampanjer er begge gode kombinasjoner for å øke ansattes bevissthet og kompetanse innen informasjonssikkerhet. Det er bevist ved flere anledninger at ansatte med høy sikkerhetsbevissthet (ISA) skaper en tryggere arbeidsplass ved at de ikke tar høyrisikoavgjørelser når det kommer til informasjonssikkerhet. Dessverre er det slik at organisasjoner ikke klarer å opprettholde en høy ISA over lengre tid. Mennesker har dårlig hukommelse og tar snarveier hvis de kan.

Et interessant funn er at litteratursøket kun identifiserte fem artikler som tar for seg *toppledelsens engasjement*. Toppledelsens engasjement, sammen med *opplæring og sikkerhetskampanjer,* blir beskrevet som en av de viktigste kildene til vedvarende kunnskap og motivasjon. Virksomheter som bruker mye ressurser på opplæring og sikkerhetskampanjer, risikerer at dette kan være forgjeves dersom de ansatte ikke er motiverte til å gjennomføre kursene. Forandringer og nye «ting» er sjeldent populært i virksomheter. Det er derfor ekstra viktig at lederne står frem som gode eksempler når de skal innføre nye sikkerhetstiltak.

Eierskap er diskutert mye frem og tilbake i litteraturen. Konseptet med personlige eide mobile enheter introduserer nye dilemmaer på arbeidsplassen og i hjemmet. På den ene siden er personlige eide enheter kjøpt og betalt av brukeren, og på den andre siden blir enheten benyttet i organisatoriske kontekster. Begge sidene føler et eierskap til enheten og har sine egne meninger om bruken av den (Hovav & Putri, 2016; McGill & Thompson, 2017). For eksempel er det blitt vanlig å jobbe på en personlig laptop hjemme. Det som skjer på denne maskinen har ikke virksomheten kontrollen over. Her må virksomheten selv foreslå noen strategier for å unngå slike dilemmaer (Harris et al., 2012).

Mislykkede forsøk på implementasjon av informasjonssikkerhet kan i mange tilfeller skyldes virksomheten selv. For å kunne oppnå best mulig resultat av implementasjonen, kreves det organisatorisk støtte på tvers av linjene. Når organisasjoner går frem for å innføre nye mobile sikkerhetstiltak, har de en tendens til å fokusere på tekniske tiltak. Det var overraskende mange artikler som tok for seg tiltak for å forhindre virus og skadevare på enheten. Det kan argumenteres for at fokuset i større grad bør bli rettet mot proaktive sikkerhetstiltak, som organisatoriske standarder og kunnskapsdelingsplattformer, istedenfor reaktive sikkerhetstiltak som bruk av antivirusprogramvare.

I litteraturen blir det skrevet om gode tekniske *informasjonssikkerhetssystemer* (ISS) for å håndtere de mobile enhetene. Disse systemene koster mye penger og er sjeldent å finne i små og mellomstore virksomheter. Ingen av disse systemene blir beskrevet som et

rapporteringssystem, et system for å rapportere inn sikkerhetsproblemer som har oppstått – for eksempel hvis man som ansatt har mistet enheten sin. Dette er problematisk. Virksomheter sliter med å få ansatte til å innrømme sine feil, noe som kan vokse til et større problem over tid.

Et ISS bør fungere som et oppslagsverk hvor den enkelte ansatte kan få en oversikt over alle regler, hvilke kurs han eller hun har gjennomført og viktige meldinger fra ledelsen. Det kan muligens være en fordel å kombinere et belønningssystem med ISS for å øke motivasjonen til de ansatte. Dette kan være så enkelt at en ansatt får en belønning for å rapportere noe som er brudd på sikkerhetsreglene, eller for å gjennomføre et nytt sikkerhetskurs.

Det finnes også en bemerkelsesverdig forskjell på operativsystemene og hvilke sikkerhetsrisikoer de innehar. Virksomheter med lite «mobilkyndige» ansatte bør gå til innkjøp av iOS-enheter (Harris & Patten, 2014). iOS-enheter forhindrer flere brukerfeil ved at det ligger strenge restriksjoner som standard i operativsystemet, i motsetning til andre operativsystemer. Det er også viktig å finne et balansepunkt mellom brukervennlighet og sikkerhet, slik at brukeren trives med det valgte operativsystemet (Harris et al., 2012).

Diskusjon av sikkerhetstiltak

Ledelsen i virksomheter må minne ansatte om at informasjonssikkerhetsbrudd kan skje og at disse truslene kan gi store konsekvenser for organisasjonens ressurser. Toppledelsen bør være involvert i å utforme og distribuere disse beskjedene.

Basert på denne litteraturstudien er det laget en liste med sikkerhetstiltak for å skjerpe informasjonssikkerheten med mobile enheter i virksomheter:

Kategori	Sikkerhetstiltak
Passord	Ha et sterkt passord som ikke assosieres med brukeren selv
	Lås enheten dersom den forlates
	Bruk automatisk lås på enheter som støtter det
	Ikke lagre passord på enheten (for eksempel i nettleseren)
	Ikke bruk samme passord på forskjellige applikasjoner
Applikasjoner og filer	Logg ut av applikasjoner som ikke brukes
	Sjekk hvilke tilganger applikasjonen krever
	Installer antivirusprogram dersom enheten støtter dette
	Aktiver fjernsletting og fjernsporing dersom enheten støtter dette
	Last kun ned applikasjoner fra det offisielle biblioteket
	Ikke klikk på filer fra ukjente avsendere
	Ikke tukle med operativsystemet (Jailbreak / Rooting)
	Ta jevnlige sikkerhetskopier av enheten
Internett	Ikke koble til offentlige nettverk
	Bruk VPN hvis du har muligheten
	Ikke koble privat enhet til virksomhetens nettverk
	Pass på at internettrafikken er kryptert (se etter HTTPS)
Ansatt	Ikke skriv / chat med fremmede
	Ikke lån bort enheten til fremmede
	Spør om hjelp hvis du er i tvil

	Ta regelmessige sikkerhetskurs for å holde deg oppdatert
Enhet	Hold enheten oppdatert – både applikasjoner og operativsystem
	Skru av Bluetooth og WiFi når det ikke brukes
	Dekk til kameraet når det ikke brukes
	Slett informasjon på enheten før den kastet / selges
	Aldri ha konfidensiell informasjon på enheten
Ledelse	Vurder heller å kjøpe IOS-enheter enn Android-enheter
	Åpne for et mobilt arbeidsrom (virtualisering av maskinen gjennom tynnklient)
	Bruk to-faktor autentisering der det er mulig

Tabell 5 – Utvalgte sikkerhetstiltak fra litteratur

Samtidig med litteraturstudien ble det rekruttert virksomheter til undersøkelsen. Underveis i rekrutteringen sa seks ledere fra IT-sikkerhetsmiljøet seg villige til å diskutere undersøkelsen og tiltakslisten. Diskusjonene foregikk over e-post og telefon.

Elementene på sikkerhetstiltakslisten ble revidert av sikkerhetsledere slik at de skulle ha høy relevans og forståelige beskrivelser før undersøkelsen begynte. Noen elementer, for eksempel «dekk til kameraet når det ikke brukes» og «vurder å kjøpe iOS-enheter ovenfor Android-enheter», var det enighet om at var for rigide tiltak å nevne i en normal sikkerhetssammenheng. Det ble også påpekt at det var normalt å råde ansatte til å rapportere sikkerhetshendelser eller mistanke om avvik, under sikkerhetsopplæringen.

Et forhold pekte seg spesielt ut. Det er mange store virksomheter i Norge i dag benytter seg av MDM-løsninger. Dette betyr i praksis at brukerne eier den mobile enheten selv, og hvis de skal ha tilgang til bedriftsdata, må de installere MDM-løsningen på enheten sin. MDM-løsninger, ofte i en container-basert variant (jobbrelatert innhold holdes separat fra annet innhold på enheten), sørger for at sikkerhetsinnstillingene (f.eks. skjermlås, VPN, osv.) settes automatisk på brukerens enhet, slik at firmaspesifikk informasjon (f.eks. e-post, kalender og filer) holdes separat fra øvrig innhold på enheten. Dette gjør at enheten kan fjernslettes/deaktiveres, dersom den kommer på avveie.

Brukeren kan ha noe uklart forhold til hva som menes med «å innføre sikkerhetstiltak på enheten» og vil dermed ha utfordringer med å svare kvantitativt på en del spørsmål rundt dette. En mulig løsning vil være å plukke ut en del håndfaste eksempler på sikkerhetstiltak brukeren selv har mulighet til å påvirke (f.eks. bryte eller suboptimere). Det er også viktig å påpeke at noen brukere vil mene at informasjonssikkerhet er noe som blir ordnet i virksomheten, og at det er ingenting de kan gjøre for å påvirke det. En slik oppfatning av kontroll vil være svært viktig å få med i undersøkelsen.

En rekke av tiltakene på listen er heller ikke forventet i den ansattes arbeidssituasjon, men heller påtvunget av organisasjonen selv. Mange virksomheter implementerer sikkerhetstiltak den ansatte må forholde seg til og ikke kan velge bort. Hvis enheten ikke registreres i MDM-systemet, vil brukeren heller ikke få tilgang på e-post eller andre bedriftsinterne data.

Tiltakslisten kunne forklart bedre hvordan sikkerhetsarbeid gjennomføres i praksis dersom den ble delt opp i andre kategorier, for eksempel «forventes av den ansatte» og «implementert av organisasjonen». Slik tiltakslisten er satt opp nå, er det vanskelig å vise forskjeller på hva som er implementert av tekniske tiltak og hva sikkerhetskulturen sørger for. En god kombinasjon av tekniske tiltak og årvåkne medarbeidere, må til for å sikre enhver bedrifts informasjonsverdier. Det er stor forskjell på oppfatningen av hva som er en optimal situasjon for en sikkerhetssjef, og slik den arter seg i hverdagen til en ansatt.

Figur 5 – Tekniske og sosiale aspekter ved informasjonssikkerhet

Videre forskning

Forskning rundt sikkerhetsatferd omhandler i mange tilfeller modeller fra kjente atferdsteorier. Innen sikkerhetskonteksten er det spesielt en modell som stikker seg ut, nemlig «*Protection Motivation Theory*» (PMT). PMT er en modell som fungerer svært godt til å forklare beskyttende atferd. Beskyttende atferd betyr at individuelle tar frivillige handlinger for å redusere risikoer som direkte omhandler dem selv (for eksempel å bruke kodelås på smarttelefonen for å forhindre innsyn av en tredjepart). Innen sikkerhetsatferd finnes det ikke bare beskyttende atferd. Eksempelvis kan det hende en bruker velger å gjøre uheldige ting fordi han eller hun ikke vet bedre. Videre forskning innen sikkerhetsatferd bør dermed fokusere på forskjellige varianter av atferdsteori og sammenhenger.

Det ville også vært interessant å fortsette arbeidet på listen med sikkerhetstiltak. Dette kunne passet godt som en delfi-studie, hvor sikkerhetseksperter fra forskjellige virksomheter diskuterer listen i et ekspertpanel og kommer frem til hvilke sikkerhetstiltak som er de mest kritiske.

Ansattes opprettholdelse av sikkerhetsregler og -policy har fått mye oppmerksomhet innen forskningsverdenen. Innen konteksten av mobile enheter er dette et mangelfullt område. Videre er det ikke avdekt hvilke sikkerhetstiltak ansatte vurderer som gode eller dårlige samt hvilke faktorer som kan forklare dette.

2.2. Teori til modellbygging

Vi har til nå beskrevet litteratur om informasjonssikkerhet på mobile enheter. Bruken av mobile enheter i forskjellige situasjoner og hvordan de håndterer sikkerhetstiltak har blitt en viktig faktor i en informasjonssikkerhetskontekst. Forskning på informasjonssikkerhet ved mobile enheter har stort sett fokusert på tekniske og organisatoriske perspektiver, et fagfelt som nå er veldokumentert (se **Litteraturstudie 2.1**). Dette fokusområdet har ført til at den individuelle brukeren av enheten har fått lite oppmerksomhet i tidligere forskning. Videre i rapporten skal vi beskrive teorier om menneskelig atferd som kan belyse sikkerhetsatferden til ansatte når de er ute på farten.

Forfatterne av den kjente atferdsteorien «*Theory of Planned Behavior*», Fishbein og Ajzen (1975), anerkjente at det finnes andre eksterne faktorer som påvirker teorien. Blant disse faktorene ble personlighet nevnt som en individuell forskjell som kan indirekte påvirke atferd. Integrasjon av personlighetstrekk i atferdsmodeller er et relativt nytt område innen IS-forskning, og vi har kun funnet et fåtall studier som har undersøkt denne sammenhengen (se Devaraj, Easley og Crant (2008); Nov og Ye (2008); Svendsen et al. (2013); Uffen, Kaemmerer og Breitner (2013)).

Denne studien forsøker dermed å fylle dette forskningsgapet ved å belyse hvordan personlighetstrekk og atferdsmessige kognitive faktorer kan påvirke brukerens holdninger til bruk av sikkerhetstiltak på mobile enheter. Slike studier er fåtallige i tidligere IS-forskning.

2.2.1. Atferdsteori

Forskning rundt individuelle forskjeller er svært utbredt i IS-forskning. Forskere har satt sammen kognitive variabler i forskjellige modeller for å kunne forutsi og forklare faktisk atferd. For å forstå koblingen mellom en mobilbrukers personlighetstrekk og i hvilken grad disse faktorene påvirker faktisk atferd av sikkerhetstiltak, må kognitive prosesser betraktes. Kognitiv psykologi handler om å se på de prosessene som ligger til grunn for oppfattelse, tenking og kunnskapservervelse (erkjennelse). Ifølge Teigen og Svartdal (2016) består disse prosessene av persepsjon (sanseoppfatning), oppmerksomhet, forestillingsvirksomhet, hukommelse, begrepsdanning, bedømming, resonnering og problemløsning.

Innenfor dette område finnes det flere kjente teorier som vil bli gått igjennom i de neste avsnittene.

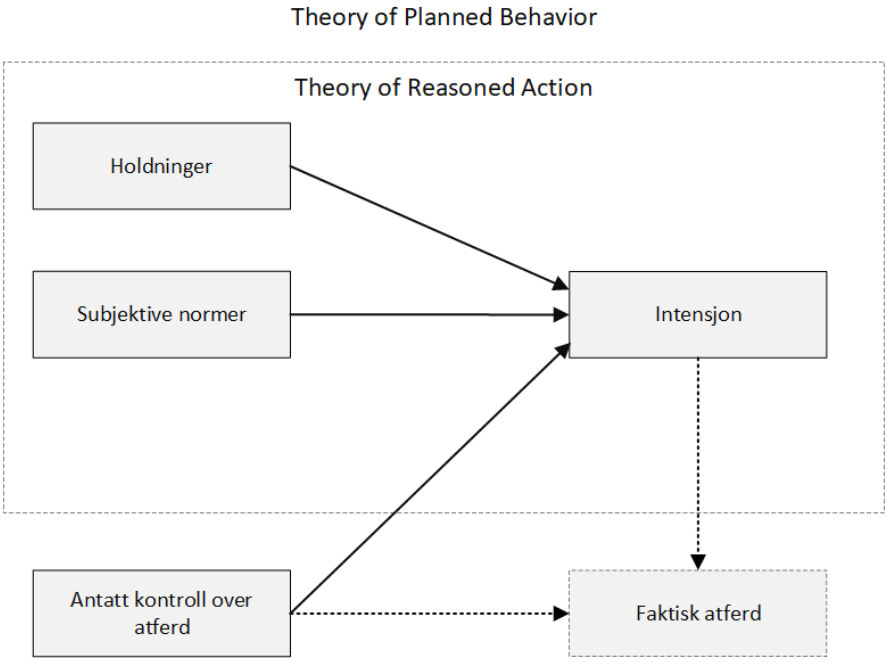
Theory of Planned Behavior og Technology Acceptance Model

For å forstå hvorfor en bruker bestemmer seg for å ta i bruk ulike sikkerhetsmekanismer, kan to velkjente atferdsteorier være til hjelp: «*Theory of Planned Behavior*» (TPB) (Ajzen, 1991) og «*Technology Acceptance Model*» (TAM) (Davis, 1989). Begge modellene er utvidelser av «*Theory of Reasoned Action*» (TRA) (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975) og er mye brukt innen IS-forskning. TPB hevder at en persons atferd er bestemt av brukerens intensjon om å utføre en gitt aktivitet. Denne intensjonen for å utføre aktiviteten kan bli forutsett ut fra tre faktorer:

- holdningen mot aktiviteten,
- subjektive normer
- oppfattet kontroll over aktiviteten

Holdningen mot aktiviteten refererer til personens tro på om aktiviteten er positiv eller negativ. En positiv holdning vil trolig oppmuntre personen til å utføre aktiviteten. Subjektive normer er personens antakelse av det sosiale presset til å utføre eller ikke utføre aktiviteten, for eksempel om personer av betydning (venner, kollegaer, familie, osv. snakker godt eller vondt om aktiviteten (Ajzen, 1991). Oppfattet kontroll over aktiviteten er den «lettheten» eller «vanskeligheten» av å utføre en aktivitet, samt en personlig følelse av kontroll over situasjonen. Denne faktoren sies å kunne forklare både intensjonen og den faktiske atferden (Ajzen, 1991), noe som ble mye debattert i sosial-psykologi litteraturen (Pavlou & Fygenson, 2006).

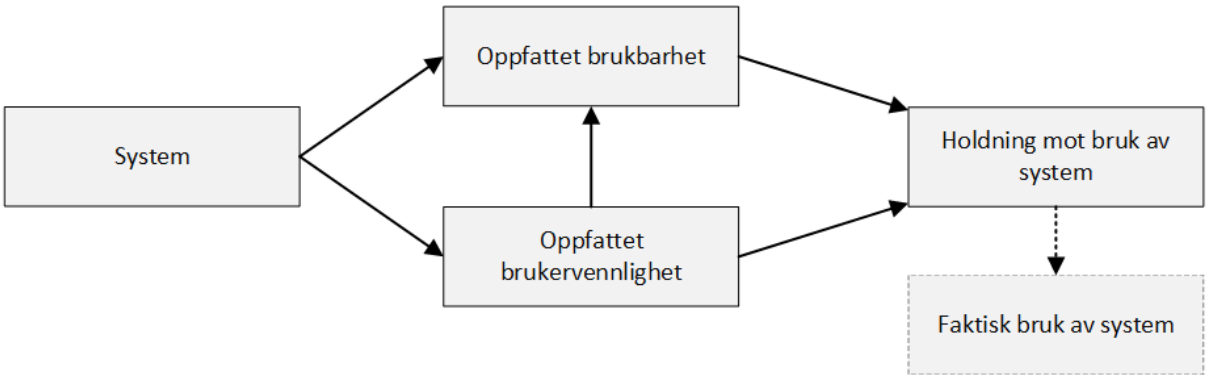
Ajzen foreslo senere at faktoren «oppfattet kontroll over aktiviteten» inneholdt to separate komponenter: Tro på egen mestringsevne («*self-efficacy*») og kontrollerbarhet (Ajzen, 2002). Tro på egen mestringsevne er definert som individets bedømmelse av hans eller hennes ferdigheter og evner til å utføre aktiviteten (Dinev & Hu, 2007). Kontrollerbarhet er definert som individets vurdering av tilgjengeligheten av ressurser og muligheten til å utføre aktiviteten (Ajzen, 2002; Pavlou & Fygenson, 2006). Det er vanlig å se på «tro på egen mestringsevne» som en refleksjon av personlige faktorer og «kontrollerbarhet» som å reflektere eksterne faktorer og ressurser (Dinev & Hu, 2007). Til tross for at flere forskere har valgt å benytte seg av TPB (se for eksempel Bulgurcu et al. (2010); Dinev og Hu (2007); Pavlou og Fygenson (2006)) er fortsatt bruken av den noe omdiskutert fordi den gir varierte resultater (Sommestad & Hallberg, 2013; Thompson et al., 2017).



Figur 6 – Theory of Planned Behavior & Theory of Reasoned Action

Noen år senere forklarte Taylor og Todd (1995) at for å kunne bedre forstå hvordan forholdene i TPB utartet seg til intensjon, måtte man bryte ned holdningsoppfattelsene i teorien. De baserte seg på innovasjonsteorien (Rogers, 1983) hvor holdninger er delt opp i tre egenskaper: «relativ fordel», «kompleksitet» og «kompatibilitet». Denne teorien er kalt «*Decomposed Theory of Planned Behavior*» (D-TPB) og viser til bedre forklaringsevner enn rene TPB- og TRA-modeller (Taylor & Todd, 1995).

På grunn av manglende forklaringsfaktorer i «*Theory of Reasoned Action*» (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975) for hvordan forutse brukeraksept i ny teknologi, utviklet Davis (1989) «*Technology Acceptance Model*» som en utvidelse av TRA. Likt som i TRA og TPB, så mener TAM at holdninger mot ny teknologi er en faktor i teknologi-adopsjon og -bruk. Modellen fremhever to viktige faktorer ved brukeraksept til ny teknologi: «oppfattet brukervennlighet» og «oppfattet brukbarhet (nyttevedi)». Oppfattet brukervennlighet er definert som i hvilken grad bruken av ny teknologi vil være enkel. Oppfattet brukbarhet er definert som i hvilken grad den nye teknologien vil forbedre arbeidsprestasjonen i en jobbsetting (Davis, 1989; Dinev & Hu, 2007). Gjennom tidene har TAM fått mye oppmerksomhet. Det er blant annet utviklet en TAM2 (Venkatesh, 2000; Venkatesh & Davis, 2000), en «universell teori for aksept og bruk av teknologi» (Venkatesh et al., 2003) og TAM har blitt brukt som forklaringsindikatorer i D-TPB (Taylor & Todd, 1995).



Figur 7 – Technology Acceptance Model

Protection Motivation Theory

«*Protection Motivation Theory*» (PMT) (Rogers, 1975; Rogers, Cacioppo & Petty, 1983) ble utviklet for å forklare hvordan man kan påvirke risikabel oppførsel og for å forklare hvilke komponenter en oversivende beskjed bør inneholde (Rogers, 1975). PMT er basert på teorien rundt fryktbaserte argumenter og forklarer at handlingen til en individuell blir påvirket av to vurderinger:

- trusselvurdering (hvor risikabel, alvorlig og sannsynlig en uønsket konsekvens er)
- håndteringsvurdering (hvor effektivt, håndterbar og kostbar den risikoreduserende handlingen er)

Et fryktinnledende argument («*fear appeal*») er et begrep som beskriver en strategi for å motivere til å gjøre en spesiell handling, følge en spesiell regel, eller kjøpe et spesielt produkt ved å bruke frykt (Maddux & Rogers, 1983).

Forklart med andre ord, mener PMT at en persons handlinger blir formet av en kost/nytte-analyse, hvor risikoen assosiert med handlingen er sammenlignet med kostnaden av å prøve å redusere eller eliminere risikoen. Denne tankegangen er sammenliknet med måten å tenke på i ulike sikkerhetsstandarder, som for eksempel ISO 27000 , hvor utvelgelsesprosessen fokuserer på kostnadseffektive løsninger (Sommestad, Karlzén & Hallberg, 2015).

Da Rogers (1975) formulerte den første versjonen av PMT i 1975, var variablene annerledes enn de er i dag. Variablene for å måle motivasjon for risikoreduserende atferd var: Alvorlighetsgrad av en hendelse, sannsynligheten for at hendelsen skjer dersom ingen risikoreduserende atferd blir gjort, og effektiviteten av den risikoreduserende handlingen. Ifølge den originale teorien, får kognitive prosesser disse variablene til å «mediere» hverandre, for eksempel er sannsynligheten for at hendelsen skjer irrelevant hvis oppfattet trussel også er lav.

Noen år senere ble teorien revidert for bedre å kunne forklare opphavet til handlingen. Teorien ble presentert som en mer generell teori om «overbevisende kommunikasjon», hvor variabler som personlighet og tidligere erfaring indirekte påvirket de kognitive prosessene. I tillegg ble teorien utvidet ytterligere med nye forklaringer som påvirker de kognitive prosessene (Maddux & Rogers, 1983; Rogers et al., 1983).

Nåværende PMT (revidert 1983) antyder at handlingen til et individ, når de står ovenfor en risiko, bestemmes av to vurderinger: En trussel- og en håndteringsvurdering. Trusselvurderingen er prosessen med å vurdere en frykt som oppstår på grunn av individets oppfatning av hvor truet han eller hun føler seg i en viss situasjon, samt hvilke belønninger eller sanksjoner handlingen fører til. Det finnes to trusselfaktorer: Oppfattet sårbarhet (hvordan et individ føler at noe negativt vil skje dersom det ikke gjøres noen tiltak) og oppfattet alvorlighetsgrad (graden av fysiske eller psykiske konsekvenser trusselen ser ut til å forårsake). Hvis en trusselvurdering har en høy grad av oppfattet sårbarhet og alvorlighetsgrad, samtidig som belønningene er lave, vil et individ vise en høy intensjon til å utføre risikoreduserende atferd. For eksempel individer som har intensjon om å slutte å røyke:

> Å røyke kan gi lungekreft (oppfattet alvorlighet), og jeg som røyker har større sannsynlighet enn en ikke-røyker til å få lungekreft (oppfattet sårbarhet), dessuten er sigaretter dyrt, og det er ingen andre som røyker lengre (lite eller ingen belønninger for å fortsette å røyke).

Håndteringsvurderingen er satt sammen av tro på egen mestringsevne («*self-efficacy*»), responsevne («*response-efficacy*») og responskostnad («*response cost*»). Tro på egen mestringsevne er troen på at egne ferdigheter kan utføre den beskyttende handlingen. Responsevne er troen på effektiviteten av den beskyttende handlingen. Responskostnad er alle antakelser om kostnader assosiert med den beskyttende handlingen. I en informasjonssikkerhetskontekst, er denne kostnaden ikke alltid reflektert i materielle

kostnader (penger). Den kan også bli sett på som den tiden en aktivitet tar, eller hvor mye ekstra arbeid som må legges inn for å få utført handlingen. Hvis en person tror at den beskyttende handlingen er effektiv (løser problemet), og at det ikke medfører alt for mye ekstra arbeid, og at de evner å gjøre det som skal til, vil sannsynligheten for at de gjør den beskyttende handlingen være høy.

PMT var opprinnelig utviklet for helsesituasjoner hvor individer burde bli overbevist om å ta frivillige handlinger for å redusere risikoer som direkte omhandler dem selv (overførbare sykdommer, røyking, o.l.). Til tross for dette har teorien vist seg å være brukbar innen forsking på andre typer risikoer, særlig innen informasjonssikkerhetsmiljøet (Hovav & Putri, 2016; McGill & Thompson, 2017; Sommestad et al., 2015; Thompson et al., 2017; Vance, Siponen & Pahnila, 2012).

Social Cognitive Theory

Hvordan man lærer fra det sosiale miljøet har vært et spennende tema innen sosialpsykologi-forskningen siden Bandura (1977) fremmet fenomenet «tro på egen mestringsevne» («*self-efficacy*»). En gjennomgående tråd i forskningen er at læring fra det sosiale miljøet kan påvirke de kognitive prosessene, noe som kan drive en forandring i atferd. Sagt på en annen måte kan det du lærer fra andre i det sosiale miljøet (venner, familie, kollegaer) ha en påvirkning på hva du faktisk gjør.

Bandura's teori, «*Social Cognitive Theory*» (SCT), (Bandura, 1977, 1986) beskriver menneskelige handlinger i form av en slags kontinuerlig gjensidig interaksjon mellom kognitive, atferdsmessige og kontekstrelaterte faktorer. Teorien legger vekt på at selvrefleksjon motiverer og styrer atferd. I hovedsak betyr dette at selvobservasjoner og tilbakemeldinger danner grunnlaget for hvilke vurderinger man gjør i gitte situasjoner. Denne vurderingen vil videre påvirke intensjonen om å utføre handlingen (Tu et al., 2015). Eksempelvis vil valget av hårfrisyre være styrt av egne meninger om frisyren og hva slags frisyre vennene dine syntes er stilig.

SCT er delt opp i flere komponenter. I dette studiet blir «*Social Learning Theory*» (SLT) tatt i bruk, som er en underliggende teori i SCT. SLT påstår at læring skjer i sosiale miljøer og blir skildret som et dynamisk samspill mellom personen, konteksten og atferden. Å lære fra det sosiale miljøet kan enten skje direkte (erfaring) eller indirekte (ved observasjon) (Bandura, 1977). Teorien kan dermed forklare hvordan mennesker lærer og hvordan det påvirker valgene de tar (Tu et al., 2015). Denne teorien har blitt brukt i flere studier angående IS-opplæring (Compeau & Higgins, 1995; Karjalainen & Siponen, 2011) og IS-adopsjon (Hong et al., 2011), men har også blitt brukt innen IS-sikkerhetskonteksten (Pahnila, Siponen & Mahmood, 2007; Tu et al., 2015; Warkentin, Johnston & Shropshire, 2011).

Denne studien antar at disse sosiale læringsmekanismene også gjelder for intensjonen av å innføre sikkerhetstiltak. For eksempel vil folk motta informasjon angående tiltaket og trusselen fra forskjellige kilder. De blir også påvirket av personlige erfaringer, som for eksempel hvis de selv eller andre (for eksempel kollegaer), har opplevd motstand mot sikkerhetstiltaket tidligere eller blitt utsatt for et virus. Teorien er brukt i tilnærmende studier (Pahnila et al., 2007; Tu et al., 2015).

D&M Model of IS-Success

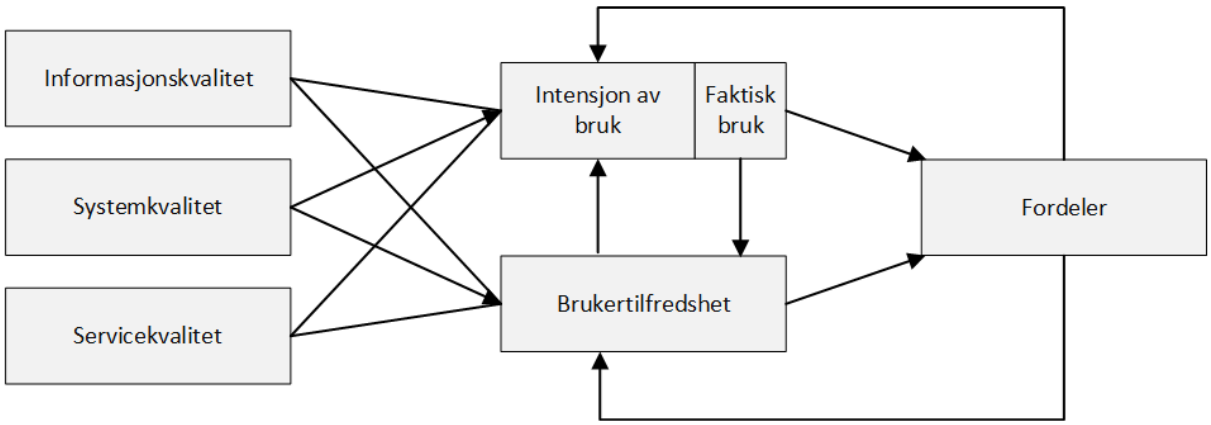
Det er utarbeidet flere modeller for å måle suksess og hvordan ulike faktorer påvirker hverandre. Blant disse suksessmodellene er det én modell som stikker seg ut, nemlig suksessmodellen «*D&M IS-Success Model*» (D&M-ISSM) av DeLone og McLean (1992). Hensikten med modellen var å samordne tidligere kunnskap om, og foreslå en ny fremgangsmåte for å måle ytelse av informasjonssystemer. D&S-ISSM (1992) inneholder variabler for å måle i hvilken grad man kan forvente individuelle og organisatoriske gevinster fra informasjonssystemet.

Modellen ble hyppig referert, noe som førte til at forfatterne reviderte modellen i 2003. Den nye og oppdaterte modellen er basert på empiriske og teoretiske bidrag fra andre forskere som har benyttet modellen i sin egen forskning (DeLone & McLean, 2003). Den nye D&M-ISSM (2003) inneholder seks sammenhengende dimensjoner: Systemkvalitet, informasjonskvalitet, servicekvalitet, bruk, brukertilfredshet og netto ytelse.

Fra den tidligere modellen (1992) til den nye (2003) er det gjort to nevneverdige forandringer:

- Servicekvalitet er lagt til som en variabel i modellen for å gjenspeile betydningen av service og støtte i suksessfulle informasjonssystemer.
- Individuelle og organisatoriske gevinster er slått sammen inn til en mer forklarende variabel, «netto ytelse».

I den originale D&S-ISSM (1992) inngikk de to dimensjonene informasjonskvalitet og systemkvalitet for å fange opp det essensielle i et informasjonssystem. Ettersom årene gikk, dukket også behovet opp for å måle en tredje dimensjon, nemlig servicekvalitet. Gjennom årene har informasjonssystemer blitt mer kompleks og det har dukket opp nye forretningsmuligheter takket være teknologi. Servicekvalitet er den overordnede støtten levert av tjenesteleverandøren og gjelder uansett om støtten leveres av IT-avdelingen eller blir outsourcet til en tredjepart. Denne dimensjonen har blitt veldig viktig i dag, også innen informasjonssikkerhet. Brukerne i et informasjonssikkerhetsmiljø er avhengige av god hjelp og støtte. Dårlig opplæring og mangel på sikkerhetsreglement vil resultere i tapt informasjonssikkerhet i virksomheten.



Figur 8 – D&M Model of IS-Success

2.2.2. Personlighetsteori

Personlighetspsykologi er studien av hele mennesket som individ. Mange tenker på personlighet som forskjeller mellom mennesker, for eksempel mennesketyper og egenskaper. Karakteristikken til personer kan variere og er en viktig del av personlighetspsykologi.

Denne studien har valgt å studere personlighetens struktur. Personlighetens struktur, *personlighetstrekk,* er oppbygning og indre sammenheng mellom ulike trekk eller «deler» av personligheten (Teigen & Skre, 2016). For å undersøke dette temaet, blir to av de mest benyttede personlighetsteoriene presentert: «*Five-Factor Model*» og «*Myers-Briggs Type Indicator*».

Five-Factor Model (FFM)

«*Five-Factor Model*» (FFM), ofte referert til som «*The Big Five*», er en omfattende psykologisk teori som tar for seg personlighetstrekk (Judge & Bono, 2000). Tupes og Christal (1992) har ofte blitt kreditert for å ha funnet opp «The *Big Five*», men modellen stammer egentlig fra en tidligere forsker ved navn Raymond Cattell (Goldberg, 1990).

FFM er en hierarkisk organisering av ulike personlige egenskaper bestående av fem grunnleggende dimensjoner: åpenhet, planmessighet, ekstroversjon, medgjørlighet og nevrotisme. Hver bipolar faktor (eks. ekstroversjon versus introversjon) oppsummerer flere spesifikke fasetter (eks. sosialitet), som igjen utgjør et stort antall spesifikke trekk (eks. pratsom & utadvendt) (Costa Jr & McCrae, 1992).

Flere måleinstrumenter har blitt utviklet for å måle «*Big-Five*» dimensjonene. De mest kjente er Costa og McCrae, som lagde et måleinstrument kalt NEO («*Neuroticism-Extroversion-Openness*»), med en fullversjon på hele 240 spørsmål («*The revised NEO Personality Inventory*» = NEO-PI-R) og en kortversjon på kun 60 spørsmål («*NEO-Five Factor Inventory*» = NEO-FFI). Behovet for kortere måleinstrumenter økte med årene, og gjorde at John, Donahue og Kentle (1991) utviklet ett sett med 44 spørsmål («*Big Five Instrument*» = BFI). Målet var å produsere en kort liste, som ville gjøre det mer fleksibelt og effektivt å evaluere de fem dimensjonene når det ikke er behov for flere differensierte målinger og individuelle fasetter (John & Srivastava, 1999). I senere tid har Rammstedt og John (2007) kommet med et forenklet måleinstrument med kun ti spørsmål («*10-Item Big Five Inventory*» = BFI-10). BFI-10 har tatt ut to spørsmål per dimensjon, hvor hver dimensjon har et positivt og et negativt spørsmål.

McAdams (1992) nevner to grunnleggende svakheter med FFM. For det første har modellen lite å tilby med hensyn til årsakene til personligheten. For det andre er modellen basert på typisk oppførsel, og man kan ikke regne med unntak fra disse generelle trekkene. Andre kritikere (Block, 1995; Loevinger, 1994), har uttrykt tvil om at en modell basert på kun fem uavhengige dimensjoner vil ha noe som helst viktig å si om personlighetsutvikling.

Tabell 6 – Dimensjoner i FFM oppsummerer de ulike dimensjonene i FFM.

Faktor	Generell beskrivelse	Beskrivelse for lav skår	Beskrivelse for høy skår
Ekstroversjon	Forklarer om personen er påståelig, dominerende, energisk, aktiv, snakkesalig, entusiastisk	Reservert, stille, nøktern	Munter, liker mennesker og store grupper, søker spenning og stimulering
Medgjørlighet	Vurderer personens samarbeidsverdier og menneskelige forhold	Manipulerende, selvsentrert, mistenkelig, hensynsløs	Tillit, tilgivende, omsorgsfull, godtroende
Nevrotisme	Forklarer personens individuelle forskjeller innen emosjonell stabilitet	Selvsikker, rolig, avslappet	Negative følelser, angst, fiendtlighet, depresjon, selvbevissthet, impulsivitet, sårbarhet
Planmessighet	Forklarer i hvilken grad personen er organisert og oppfyller sine plikter og ansvar	Upålitelig, lat, uorganisert	Travel, grundig, effektiv, pålitelig
Åpenhet	Karakteriserer om personen er intellektuelt nysgjerrig og har tendens til å søke nye erfaringer og utforske nye ideer	Konvensjonell, få interesser, ikke analytisk	Kreativ, innovativ, fantasifull, reflekterende, utradisjonell

Tabell 6 – Dimensjoner i FFM (adoptert fra: McCrae & John, 1992; Zhao & Seibert, 2006)

Myers-Briggs Type Indicator (MBTI)

Psykologisk personlighetsteori ble først utviklet av den sveitsiske psykologen Carl Jung, som foreslo at individuelle forskjeller i menneskeheten er forutsigbare og konsistente gjennom hele livsløpet. Dette ble basert på varige («*endurige*») egenskaper som sterkt påvirker personlighet og grunnleggende mentale funksjoner (Kitzrow, 2002). Jung foreslo å dele mennesket inn i to deler: Ekstroverte og introverte. Han kom også med at personligheten var delt i fire (tanke/følelse og intuisjon/sansing), strukturert som bipolare par. Dette var fordi han mente mennesket har en funksjon de er bevisst og best på, og en funksjon som er underutviklet og ubevisst (Rzadkowska, 2016).

Senere utviklet to amerikanske kvinner, Katherine Briggs og hennes datter, Isabel Briggs Myers, «*Myers-Briggs Type Indicator*» (MBTI)**.** MBTI er et selvrapporterende spørsmålsskjema, basert på Jungs teori om psykologiske typeforskjeller, som bestemmer en persons psykologiske type. Denne modellen identifiserer 16 psykologiske typer basert på fire bipolare skalaer (Kitzrow, 2002):

- Ekstrovert/Introvert
- Sansende/Intuitiv
- Tenkende/Følgende
- Avgjørende/Oppfattende

Ekstrovert (E) eller Introvert (I) handler om hvor et individ foretrekker å gi hans eller hennes oppmerksomhet og hvordan individet får sin energi. Ekstrovert fokuserer på å samle energi fra den ytre verden av mennesker og aktiviteter, mens Introvert fokuserer på å få sin energi fra den indre verden av tanker og følelser (Kitzrow, 2002).

Sansende (S) eller Intuitiv (N) handler om hvordan et individ foretrekker å samle og behandle informasjon, og hva slags informasjon de gir oppmerksomhet til. Personer med preferanse for Sansende fokuserer på informasjonen de mottar gjennom deres sanser og er interessert i fakta, detaljer og praktiske egenskaper. Personer med en preferanse for Intuitiv er mindre interessert i fakta, og foretrekker å fokusere på teorier, mønstre, forbindelser og muligheter (Kitzrow, 2002).

Tenkende (T) eller Følende (F) handler om hvordan den enkelte tar avgjørelser. Personer med en preferanse for Tenkende tar beslutninger basert på logikk og fakta, mens personer med preferanse for Følende tar beslutninger basert på personlige og subjektive verdier, og virkningen disse beslutningene har på andre (Kitzrow, 2002).

Avgjørende (J) eller Oppfattende (P) handler om hvordan hvert enkelt individ liker å leve livet sitt og håndtere den ytre verden. Enkeltpersoner med en preferanse for Avgjørende foretrekker å planlegge og organisere tiden og livet sitt på en strukturert måte. Personer som er Oppfattende foretrekker en fleksibel og spontan tilnærming til livet. De liker å holde sine muligheter åpne og kan føle seg begrenset dersom det blir satt beslutninger (Kitzrow, 2002).

I tabellen under er de ulike personlighetstypene fra MBTI oppsummert.

ISTJ	**ISFJ**	**INFJ**	**INTJ**
Tradisjonalister 13,7 %	**Beskyttere 12,7 %**	**Guider 1,7 %**	**Visjonærer 1,4 %**
Pliktoppfyllende	Pliktoppfyllende	Hengiven	Selvstendig
Praktiske	Praktiske	Innovative	Innovative
Logiske	Støttende	Idealistisk	Analytiske
Metodiske	Nitidige	Medfølende	Målrettet
ISTP	**ISFP**	**INFP**	**INTP**
Problemløsere 6,4 %	**Harmoniserere 6,1 %**	**Humanister 3,2 %**	**Konseptualiserere 2,4 %**
Hensiktsmessig	Tolerant	Innsiktsfull	Spørrende
Praktiske	Realistisk	innovativ	Innovative
Objektive	Harmonisk	Idealistisk	Objektive
Tilpasningsdyktig	Tilpasningsdyktig	Tilpasningsdyktig	Abstrakt
ESTP	**ESFP**	**ENFP**	**ENTP**
Aktivister 5,8 %	**Fun-lovers 8,7 %**	**Entusiaster 6,3 %**	**Entreprenører 2,8 %**
Energisk	Spontan	Optimistisk	Risikovillig
Praktisk	Praktisk	Innovative	Innovative
Pragmatisk	Vennlig	Medfølende	Utadvendt
Spontan	Harmonisk	Allsidig	Tilpasningsdyktig
ESTJ	**ESFJ**	**ENFJ**	**ENTJ**
Koordinatorer 10,4 %	**Supportere 12,6 %**	**Utviklere 2,8 %**	**Reformatorer 2,9 %**
Organisert	Vennlig	Vennlig	Bestemt
Praktisk	Praktisk	Innovative	Innovative
Logisk	Lojal	Støttende	Strategisk
Utadvendt	Organisert	Idealist	Utadvendt

Tabell 7 – De 16 personlighetstypene i MBTI (Busch & Moen, 2014; Myers et al., 1998)

2.3. Oppsummering og diskusjon av teori

Denne delen har rapportert fra en kort litteraturstudie med hensikt å identifisere vanlige sikkerhetsrisikoer og -tiltak, og det er nevnt tidligere forskning innen atferds- og personlighetspsykologiteorier. Videre i rapporten blir det valgt ut elementer fra teoriene. Disse elementene blir brukt til å bygge en teoretisk modell for å belyse problemstillingen.

2.3.1. Diskusjon og valg av atferdsteori

Innen forskning på sikkerhetsatferd er det hovedsakelig benyttet to «konkurrerende» teorier: «*Theory of Planned Behavior*» (TPB) og «*Protetion Motivation Theory*» (PMT). Begge teoriene gir gode resultater og er brukt i tilsvarende studiekontekster (se for eksempel: Bulgurcu et al. (2010); Johnston og Warkentin (2010)). I denne studien argumenteres det for at TPB er et bedre valg enn PMT.

Hvorfor mennesker bestemmer seg for å innføre ulike sikkerhetstiltak er mye forsket på. Selv om teknologiadapsjonsteorier, som «*Technology Acceptance Model*» (TAM) (Davis, 1989), «*Unified Theory of Acceptance and Use of Technology*» (UTAUT) (Venkatesh et al., 2003), med flere, er gode på å forutse teknologiaksept og bruk, er disse ofte begrenset til produktivitetsbaserte applikasjoner. At personer tar i bruk sikkerhetstiltak er ofte forbundet med en frykt for at noe skal skje, noe som nødvendigvis ikke vil øke ytelsen på arbeidsplassen (Johnston & Warkentin, 2010). Dette er hovedgrunnen til at mange argumenterer for at PMT, en teori som bygger på frykt, er en god teori å benytte for å forklare sikkerhetsintensjon og -atferd.

I situasjoner der trusselen har en opplevd moderat-til høy grad, vil individer gjøre tiltak for å redusere denne trusselen. Disse tiltakene kan føre til positive resultater, som for eksempel å innføre et sikkerhetstiltak, og er ofte den responsen IT-ledere ønsker å oppnå når de bruker frykt i en sikkerhetssammenheng (Johnston & Warkentin, 2010). Kort oppsummert fungerer denne teorien godt, dersom brukerne er klar over de sikkerhetstruslene som eksisterer.

Basert på resultatene fra tidligere forskning, er det klart at teorien klarer å forklare en god del av intensjonene relatert til sikker atferd innen informasjonssikkerhet. Til tross for dette, finnes det gode grunner til å anta at nøyaktigheten til teorien avhenger av hvilken type sikkerhetsatferd den blir benyttet mot. For det første ble PMT utviklet til å forklare hvordan frykt påvirker frivillige atferdsintensjoner relatert til helse. I IS-sikkerhetskonteksten har teorien blitt brukt til å forklare overholdelse av sikkerhetsregler og annen obligatorisk oppførsel (Ifinedo, 2012; Siponen et al., 2014). For det andre ble teorien utviklet for å forklare hvordan kognitive prosesser relaterer seg til bestemte trusler (for eksempel HIV) og spesifikke håndteringsmetoder (for eksempel beskyttet samleie). Teorien er imidlertid blitt brukt til IS-sikkerhetsatferd som er kompleks eller abstrakt, som for eksempel å «oppføre seg sikkert» (Johnston & Warkentin, 2010; Thompson et al., 2017). For det tredje ble teorien utviklet for helsetrusler mot individuelle, og ikke mot organisasjonen eller andre.

Ifinedo (2012) brukte variabler fra både PMT og TPB i sin studie om overholdelse av sikkerhetsreglene i virksomheter. Resultatene fra denne studien er i favør av TPB, hvor alle variablene ble støttet. Generelt sett klarer PMT å forklare mellom 0.34 og 0.5 av variansen i

den studerte populasjonen (Sommestad et al., 2015), hvor TPB forklarer 0.42 innen samme kontekst (Sommestad & Hallberg, 2013).

Denne studien har som hensikt å analysere ansattes holdninger til bruk og faktisk bruk av sikkerhetstiltak med mobile enheter ute på farten. Basert på litteraturstudien, er brukere lite opplyst om hvilke sikkerhetsrisikoer som finnes, og at mange ikke frykter sikkerhetsbrudd på enheten deres. Ifølge Sommestad, Karlzén og Hallberg's (2015) META-analyse gir PMT best resultater dersom trusselen og håndteringsmetoden er spesifikk, relaterer seg til individet personlig (ikke til organisasjonen) og er frivillig. Denne studien relaterer seg til hverken en spesifikk trussel eller håndteringsmetode og vil være i en obligatorisk (tvunget) organisatorisk kontekst. Basert på disse argumentene, faller valget på den mer generelle atferdsteorien TPB for å forklare sikkerhetsatferd.

2.3.2. Diskusjon og valg av personlighetsteori

«Myers-Briggs Type Indicator» (MBTI) er mye brukt i alt fra konsulentfirmaer til opplæringsfirmaer, og er veldokumentert og testet for validitet og reliabilitet (Burisch, 1984). En av ulempene med MBTI er at den er ganske så kostbar å benytte. Det finnes imidlertid flere gratisversjoner på internett. Problemet med disse er at de hverken er dokumentert eller testet for validitet og reliabilitet. Ved å gå for en slik gratis test er sannsynligheten større for å samle inn feil type data (McDonald & Edwards, 2007).

Det har også kommet mye kritikk mot MBTI. Dette er i hovedsak forskere som benytter FFM i sin forskning som kommer med denne kritikken. McCrae og Costa (1989) er ganske kritiske til MBTI fordi den utelater Nevrotisme, noe som alle seriøse teoretikere og psykometrikere mener er en fundamental dimensjon av personlighet. De nevner også at MBTI ikke gir like omfattende informasjon på alle skalaene, slik som NEO-PI er i stand til å gjøre. De tror at dette er svært viktig for å forstå personene som skårer i midten på skalaen og konkluderer dermed med:

> *«If the MBTI is used, evidence to date suggests that it may be better to abandon the Jungian framework and reinterpret the MBTI in terms of the five factor model»* (McCrae & Costa, 1989, s. 37).

Furnham (1996) mener det er helt klart at de psykometriske egenskapene, spesielt da konstruksjonen og de prediktive validitetskriteriene til NEO-PI er overlegne over MBTI. I tillegg til at de fem dimensjonene sannsynligvis er mer nyttig i det anvendte feltet ved å gå mer i detalj på faktorene.

FFM har også sine svakheter. Block (1995) har kommentert mye rundt FFM og skissert flere utfordringer med modellen. Andre utfordringer knyttet til FFM er at de ulike måleinstrumentene kan gi forskjellige resultater (Feldt et al., 2008).

Til tross for kritikk faller valget på FFM. FFM gir gode resultater både innen reliabilitet og validitet gjennom flere empiriske forsøk. De fleste måleinstrumentene for FFM ligger tilgjengelig for de som ønsker å bruke instrumentene og er godt dokumentert. FFM er i tillegg gratis, i motsetning til MBTI.

BFI-10 - måleinstrument for Five Factor Model

I en ideell verden ville personlighetsforskere ha tilstrekkelig tid og ressurser for å få en høy innholdsvaliditet og pålitelighet fra veletablerte instrumenter. Dessverre er slike forhold sjeldne, noe som fører til at forskere ofte står overfor valget mellom å bruke et kort instrument eller ikke bruke noe instrument i det hele tatt.

En internettbasert studie brukte for eksempel ett spørsmål for å skaffe seg en vurdering av selvtillit fra deltakerne. Svarresponsen fra denne undersøkelsen var stor, og forskeren påstår selv at responsen neppe ville vært like stor dersom det var mange spørsmål respondenten måtte forholde seg til (Robins et al., 2002).

I denne studien ble det valgt å bruke BFI-10 (Rammstedt & John, 2007) for å måle personlighetstrekkene til respondentene. Formålet med studien er å se etter sammenhenger mellom personlighetstrekk og holdninger til bruk. Det vil ikke være behov for en dyp og gjennomgående personlighetsstudie for å finne ut om denne sammenhengen er relevant. Dersom det skulle bli relevant med en dypere studie senere, bør det utføres en utdypet studie med et større måleinstrument.

BFI-10 inneholder ti spørsmål og tar svært kort tid for respondenten å gjennomføre. Fordelen med slike korte instrumenter er at man eliminerer redundansen i spørsmålene, noe Burisch argumenterer for:

> *«Short scales not only save testing time, but also avoid subject boredom and fatigue...there are subjects...from whom you won't get any response if the test looks too long. There is, by the way, the likelihood that a long scale will actually be less valid than a short one.»* - Burisch (1984, s. 219)

Reliabilitet og validitet av BFI-10

Rammstedt og John (2007) opprettet BFI-10 fordi de mente tiden hadde forandret seg. De tidligere instrumentene på 40-60 spørsmål, som virket korte da, ser nå ut til å ta alt for lang tid for den gjennomsnittlige respondenten. De så en økende trend mot kortere personlighetsinstrumenter, samtidig som forskere ønsket et kortere instrument.

BFI-10 har vist seg å kunne forklare nesten 70% av variansen til BFI-44 fullskalaen (Freudenthaler, Spinath & Neubauer, 2008). Den har også blitt brukt i flere tidligere studier (Guido et al., 2015; Karwowski et al., 2013; Küfner et al., 2010; Lechner & Rammstedt, 2015), der BFI-10 har vist overkommelig reliabilitet og validitet.

2.3.3. Oppsummering av teori og valg

Innledningsvis i teoridelen ble det foretatt en litteraturstudie for å kartlegge hvilke risikoer og tiltak som finnes ved bruk av mobile enheter. Denne litteraturstudien ga innblikk i hvilke sikkerhetsrisikoer som kan oppstå med mobile enheter, samt en liste over sikkerhetstiltak som kunne bli brukt videre i studien.

For å etablere eksisterende teori innen forskningsområdet, ble det gjennomgått tidligere forskning innen atferds- og personlighetsteori. Under atferdsteori er det generelt to teorier som har blitt mye benyttet for sikkerhetsatferd: TPB og PMT. Ettersom teoriene måler atferd på to forskjellige måter, ble det gjort en vurdering av hvilken atferdsteori som passet best til denne studien. TPB ble det endelige valget.

Under personlighetsteori ble MBTI og FFM beskrevet. MBTI og FFM er de mest kjente personlighetsrammeverkene benyttet i dag. FFM ble valgt hovedsakelig fordi den er godt dokumentert og tilbyr et gratis måleinstrument.

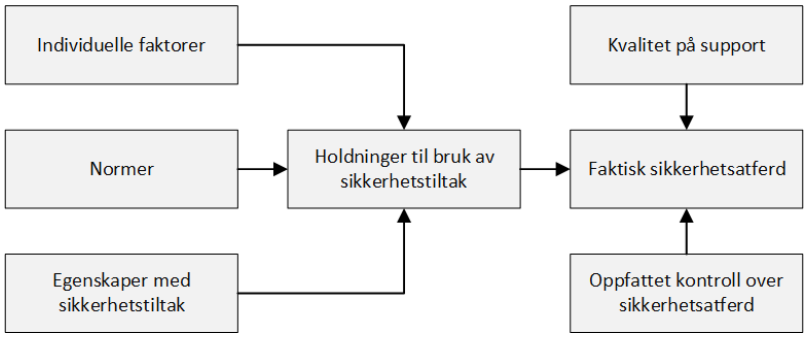
3. Forskningsmodell og hypoteser

Utviklingen av forskningsmodellen og hypoteser har foregått ved en deduktiv teoretisk tilnærming. Tidligere litteratur har blitt brukt til å besvare problemstillingen i studien. Forskningsmodellen er en konseptuell modell som forsøker å analysere ansattes holdning til bruk av sikkerhetstiltak og deres faktiske sikkerhetsoppførsel. Modellen låner variabler fra TPB (Ajzen, 1991), SCT (Bandura, 1977), TAM (Davis, 1989), D&M-ISSM (DeLone & McLean, 2003) og FFM.

Under utviklingen av modellen ble det gjort noen valg. Begrunnelsen for disse valgene finnes i **2.2 - Teori til modellbygging**. Kort oppsummert ble det argumentert for at TPB var den beste modellen for denne studien og blir derfor brukt som base for å måle sikkerhetsatferd. Personlighetstrekk i modellen blir studert som en individuell faktor og målt ved hjelp av FFM.

Først i kapitlet er det presentert en konseptuell forskningsmodell. Denne modellen beskriver hvilke faktorer som kan forklare holdninger til bruk, og faktisk bruk av, sikkerhetstiltak. Videre er det presentert og diskutert hypoteser basert på tidligere forskningslitteratur. Til slutt illustreres den endelige forskningsmodellen med tilhørende hypoteser.

3.1. Konseptuell forskningsmodell



Figur 9 – Konseptuell forskningsmodell

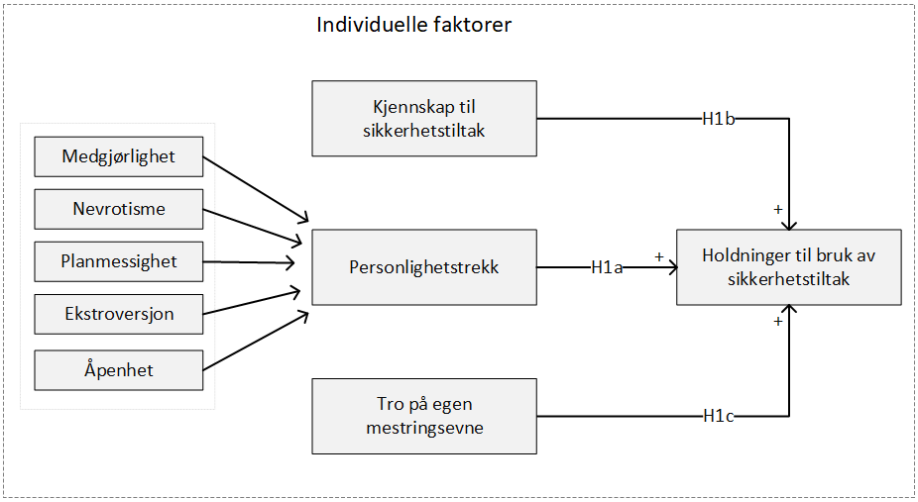
Vi valgte å inkludere tre generelle faktorer som kan forklare holdninger til bruk av sikkerhetstiltak basert på tidligere litteratur. Holdningene til bruk av sikkerhetstiltak blir påvirket av individuelle faktorer, normer og egenskaper ved sikkerhetstiltak. Videre blir holdningene overført til faktisk sikkerhetsatferd. Denne sikkerhetsatferden blir igjen påvirket av i hvilken grad sikkerhetstiltakene blir støttet i virksomheten (opplæring, kurs, osv.) og hvilken kontroll brukeren har over atferden.

Som et forsøk å forenkle modellen, er atferdsintensjon droppet ved å la holdninger til bruk av sikkerhetstiltak peke direkte mot faktisk atferd. Intensjon er antatt til å være en umiddelbar forutsetning for atferd og er en indikasjon på individets samlede vurdering mot en gitt handling. Dersom individer har en positiv intensjon mot en handling, vil det være svært sannsynlig at individet faktisk utfører handlingen.

3.2. Hypoteser

Videre i dette kapittelet blir hypotesene introdusert og diskutert individuelt. Underkapitlene er delt opp basert på den konseptuelle forskningsmodellen.

3.2.1. Individuelle faktorer



Figur 10 – Individuelle faktorer

Individuelle faktorer kan variere på mange måter. Man kan blant annet se forskjeller mellom mennesker på det fysiske, psykiske, personlighetsmessige, kunnskapsmessige og deres erfaringer. I denne studien vil individuelle faktorer bli belyst både i form av personlighetstrekk, deres kjennskap til informasjonssikkerhetstiltak og tro på egen mestringsevne.

Personlighetstrekk

Personlighetstrekk er personens karakteristiske mellommenneskelige egenskaper og er beskrevet av de som har sett personen i en rekke situasjoner. Eksempelvis kan man se forskjell på festens midtpunkt og en som er veldig tilbaketrukket. Dette er også forklart som personens rykte (Hogan, Hogan & Roberts, 1996).

FFM er laget for å måle personlighetstrekk i fem ulike dimensjoner. Vi har valgt å adoptere modellen med alle dimensjonene: Ekstroversjon, Nevrotisme, Medgjørlighet, Planmessighet og Åpenhet. På denne måten kan vi se om det finnes noen konkrete underliggende forhold i de forskjellige dimensjonene som faktisk gjør at personlighetstrekk får forklaringskraft mot holdning til bruk av sikkerhetstiltak.

Gjennom en internettundersøkelse kom Pattinson et al. (2015) frem til at åpenhet, medgjørlighet og planmessighet var positivt assosiert til selvrapportert informasjonssikkerhetsatferd. Medgjørlighet og planmessighet ble også rapportert som en viktig faktor for å forklare brukernes intensjon om å ta i bruk sikkerhetsapplikasjoner (Shropshire, Warkentin & Sharma, 2015).

Med dette kommer følgende hypotese:

> *H1a: Det er en positiv sammenheng mellom personlighetstrekk og holdninger til bruk av sikkerhetstiltak.*

Illustrert i **Figur 10 – Individuelle faktorer.**

Kjennskap til sikkerhetstiltak

Kjennskap til sikkerhetstiltak bygger på bevisstheten til personen. Bevissthet er menneskets evne til å oppleve, registrere og sanse hva som hender i ens omgivelser og med en selv (Hansen, 2018). Innen informasjonssikkerhet har bevissthet fått mye oppmerksomhet (se for eksempel: Bulgurcu et al. (2010); Zhang et al. (2017)) og blir ofte brukt som en forklaringsfaktor for menneskelig feil. I denne studien defineres sikkerhetsbevissthet som i hvilken grad den ansatte er opplyst over hvilke sikkerhetstiltak som eksisterer i ens arbeidssituasjon. Dersom en ansatt ikke er klar over at det finnes sikkerhetstiltak, vil heller ikke den ansatte danne holdninger til bruk av sikkerhetstiltak(ene).

Ifølge TPB er det sannsynlig at høyere bevissthet kan føre til positive holdninger. Ajzen (1991) skriver videre at individer som er bevisst og har kunnskap om aktiviteten, vil ha flere positive assosiasjoner til kontrollerende faktorer rundt aktiviteten. Dermed vil et individ som er klar over de sikkerhetstiltakene som finnes i virksomheten, antakeligvis være klar over hvilke interesser organisasjonen og personer i ens sosiale miljø, har om ulike sikkerhetstiltak.

Med dette kommer følgende hypotese:

> *H1b: Det er en positiv sammenheng mellom kjennskap til sikkerhetstiltak og holdninger til bruk av sikkerhetstiltak.*

Illustrert i **Figur 10 – Individuelle faktorer.**

Tro på egen mestringsevne

Tro på egen mestringsevne, fra SCT (Bandura, 1977), er definert som troen på at man er kapabel til å kontrollere ens egen utføring av en bestemt oppgave. I denne studien dreier dette seg om ansattes vurdering av egne ferdigheter og evner til å innføre sikkerhetstiltaket.

I TPB er tro på egen mestringsevne med på å forklare et individs oppfattet kontroll over atferd. Teorien bygger på at en vurdering av egne evner samt kontroll over situasjonen bestemmer om man har mulighet til å gjennomføre handlingen. Det er grunn til å tro at holdninger mot bruken av sikkerhetstiltak kan formes uavhengig om individet har kontroll på handlingen. Hvis du som ansatt ikke evner å innføre sikkerhetstiltak, vil trolig holdningene til bruken av dem bli påvirket av dette, uansett om du har kontroll over tiltakene eller ikke.

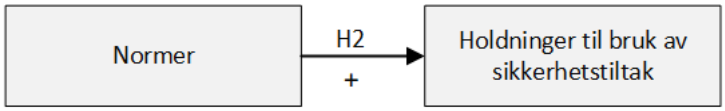
I denne studien vektlegges Bandura (1977) ved å benytte tro på egen mestringsevne som en egen variabel, og antar med dette at variabelen kan påvirke holdninger til bruk av sikkerhetstiltak. Dersom individet mener at egne ferdigheter er tilstede, vil holdninger til bruk av sikkerhetstiltak bli mer positiv.

Med dette kommer følgende hypotese:

> *H1c: Det er en positiv sammenheng mellom tro på egen mestringsevne og holdninger til bruk av sikkerhetstiltak.*

Illustrert i **Figur 10 – Individuelle faktorer.**

3.2.2. Normer



Figur 11 – Normer

Konseptet sosial innflytelse er mye diskutert i IS-litteraturen. I TPB og TRA er sosial innflytelse definert som individets oppfatninger av hvorvidt det er forventet fra familie, venner og samfunn å utføre den gitte handlingen. TAM tok ikke med sosial innflytelse i modellen. De argumenterte for at sosial innflytelse var uklart definert og manglet empirisk støtte.

Konformitet betyr at individer oppfører seg i tråd med gjeldende normer, enten om det er innenfor en bestemt gruppe eller mer generelt (Store Norske Leksikon, 2017). De fleste mennesker ønsker å oppføre seg i tråd med sosiale normer, enten det er i frykt om å ikke passe inn i den sosiale gruppen eller andre ting. Å ikke følge sosiale normer kan også komme med sanksjoner, noe som er sjeldent ønskelig.

Bulgurcu et al. (2010) studerte ansattes intensjoner til å følge sikkerhetsreglene i virksomheten. Sosiale normer var en av variablene som signifikant påvirket ansattes intensjon om å følge sikkerhetsretningslinjene i virksomheten. At ansatte bestemmer seg for å bruke sikkerhetstiltak, synes dermed å være tett knyttet til sikkerhetsretningslinjene og forventninger fra personene rundt dem.

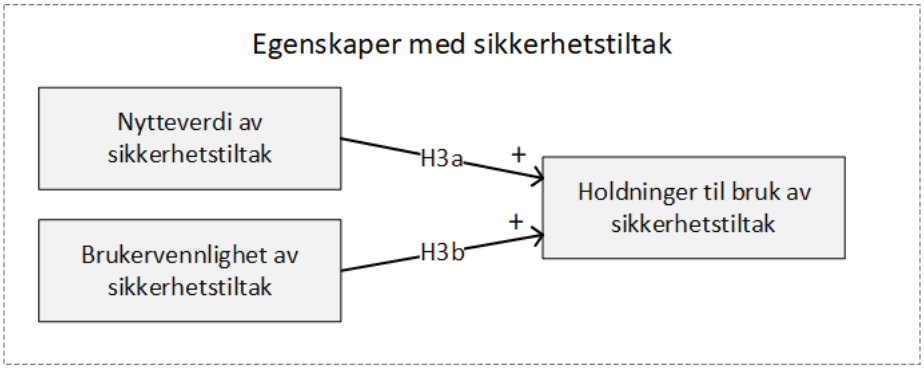
I denne studien fokuserte vi på vanlige brukere av mobile enheter. Med dette menes det at personene forholder seg til normer fra ledelsen, uttrykt som forventninger (retningslinjer) til bruk av sikkerhetstiltak.

Med dette kommer følgende hypotese:

> *H2: Det er en positiv sammenheng mellom normer og holdninger til bruk av sikkerhetstiltak.*

Illustrert i **Figur 11 – Normer.**

3.2.3. Egenskaper med sikkerhetstiltak



Figur 12 – Egenskaper med sikkerhetstiltak

TAM er skreddersydd for å måle brukeraksept ved IS. I likhet med IS, kan oppfattelsen av suksess ved sikkerhetstiltakene bli oppfattet forskjellig. Slik som i D-TPB (Taylor & Todd, 1995), velger vi å adoptere oppfattet brukbarhet og oppfattet brukervennlighet som variabler for å forklare sikkerhetstiltakenes påvirkningskraft mot holdninger til bruk.

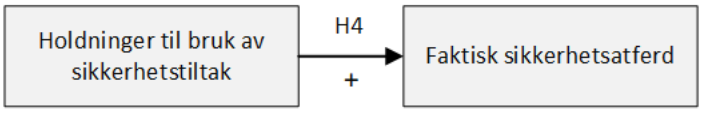
Nærmere bestemt kan oppfattet nytteverdi forklare i hvilken grad en bruker tror at sikkerhetstiltaket vil øke sikkerheten på hans eller hennes enhet. Den andre variabelen fra TAM, oppfattet brukervennlighet, beskriver i hvilken grad en bruker tror at det å gjennomføre sikkerhetstiltaket vil være enkelt og problemfritt.

Med dette kommer følgende hypoteser:

> *H3a: Det er en positiv sammenheng mellom oppfattet nytteverdi av sikkerhetstiltak og holdninger til bruk av sikkerhetstiltak.*
>
> *H3b: Det er en positiv sammenheng mellom brukervennlighet av sikkerhetstiltak og holdninger til bruk av sikkerhetstiltak.*

Illustrert i **Figur 12 – Egenskaper med sikkerhetstiltak.**

3.2.4. Holdninger til bruk av sikkerhetstiltak



Figur 13 – Holdninger til bruk av sikkerhetstiltak

Holdning betyr innstilling (Teigen, 2016) og oppfører seg som en positiv eller negativ følelse mot en handling. Generelt sett forklarer holdninger den individuelles samlede vurdering av konsekvensene av en spesiell handling. I denne studien utgjør positive holdninger en persons tro på at å ta i bruk sikkerhetstiltak vil bidra til å øke beskyttelsen av mobile enheter.

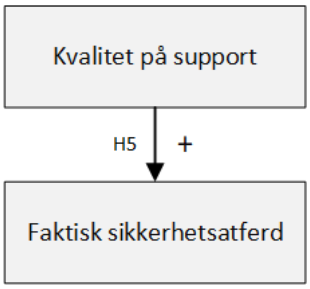
Hvis brukeren oppfatter resultatet av en viss handling som positiv, i dette tilfellet sikkerhetstiltak, vil han eller hun danne positive holdninger til bruken av sikkerhetstiltak. Dersom en har gode holdninger overfor en atferd, vil det være stor sannsynlighet for at handlingen trer i kraft.

Med dette kommer følgende hypotese:

> *H4: Det er en positiv sammenheng mellom holdninger til bruk av sikkerhetstiltak og faktisk sikkerhetsatferd*

Illustrert i **Figur 13 – Holdninger til bruk av sikkerhetstiltak**.

3.2.5. Kvalitet på support



Figur 14 – Kvalitet på support

For at ansatte skal ha mulighet til å innføre sikkerhetstiltak på enheten, er det viktig at virksomheten bidrar med assistanse og tilrettelegging. I D&M ISSM (DeLone & McLean, 2003), er servicekvalitet definert som den overordnede støtten levert av tjenesteleverandøren og gjelder uansett om støtten leveres av IT-avdelingen eller blir outsourcet til en tredjepart. For å forklare hvilken opplæring og support virksomheten selv tilbyr den ansatte i bruken av sikkerhetstiltak, brukes variabelen servicekvalitet. I denne studien blir servicekvalitet uttrykt som kvalitet på support.

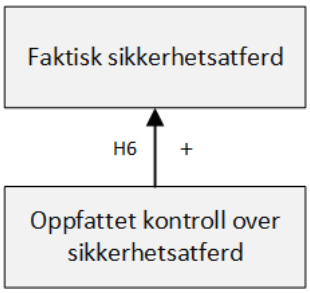
Dersom virksomheten tilbyr god opplæring og tilrettelegging for sikkerhetstiltak, vil trolig den ansatte føle seg kompetent nok til å bruke sikkerhetstiltak på enheten.

Med dette kommer følgende hypotese:

> *H5: Det er en positiv sammenheng mellom kvalitet på support og faktisk sikkerhetsatferd.*

Illustrert i **Figur 14 – Kvalitet på support**.

3.2.6. Oppfattet kontroll over sikkerhetsatferd



Figur 15 – Oppfattet kontroll over sikkerhetsatferd

Antatt kontroll over atferd reflekterer den ansattes følelse av kontroll over en handling. Ifølge TPB og Bandura (1977) sin teori om sosial læring, er et individs antatte kontroll over atferd styrt av troen på tilgang til de ressursene som trengs for å utføre handlingen. Dersom individet mener at egne ferdigheter og ressursene er tilstede for å innføre sikkerhetstiltaket, vil det være større sannsynlighet for at atferden blir gjennomført.

Litteraturen gjør et poeng av at holdninger må reflektere noe som har fått tid til å utvikle seg før man spør om dem. Holdninger som ikke er forankret i erfaringer om en bestemt atferd, vil ha mindre prediksjonskraft på intensjon og faktisk atferd. Atferd som et individ ikke har innflytelse over vil dermed føre til mindre sterke og tydelige holdninger.

Når det kommer til innføring av sikkerhetstiltak, er det ikke sikkert at dette er frivillig, og det er grunnen til at oppfattet kontroll over atferd påvirker faktisk sikkerhetsatferd. Noen sikkerhetstiltak kan være utenfor individets kontroll (for eksempel tvunget VPN for å lese jobb e-post), eller det kan være sanksjoner for å ikke følge ulike retningslinjer (å miste jobben dersom man ikke innfører et sikkerhetstiltak).

Med dette kommer følgende hypotese:

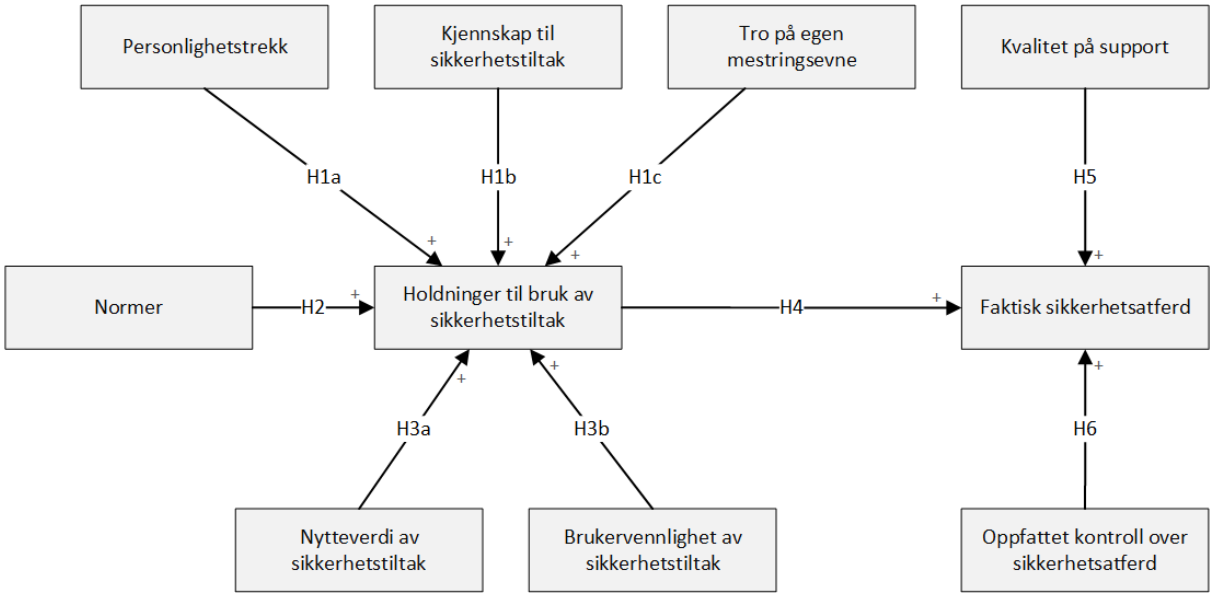
> *H6: Det er en positiv sammenheng mellom oppfattet kontroll atferd og faktisk sikkerhetsatferd.*

Illustrert i **Figur 15 – Oppfattet kontroll over sikkerhetsatferd**.

3.2.7. Oppsummering av hypoteser og forskningsmodell

Den endelige forskningsmodellen med tilhørende hypoteser er illustrert i **Figur 16 – Forskningsmodell med hypoteser**.

Alle hypotesene antar at det er en positiv sammenheng i den retningen pilen peker.



Figur 16 – Forskningsmodell med hypoteser

4. Metode

I denne studien har vi valgt en spørreundersøkelse som kvantitativ metodisk tilnærming. I kvantitative undersøkelser blir de som undersøkes kalt enheter, og det som undersøkes blir kalt variabler. Studien ønsker å finne frem til et mønster av forklaringer, beskrevet av modeller og hypoteser, som gjelder for utvalget og som muligens kan generaliseres til en større populasjon. Det ble i tillegg benyttet en kvalitativ metode for å kvalitetssikre sikkerhetstiltak mot eksperter på området. Dermed kan man si at studien har en positivistisk tilnærming, men med en kvalitativ sjekk av relevansen til faktorene som studeres (Kristoffersen, Tufte & Johannessen, 2011).

4.1. Forskningstilnærming

Meningen med studien er å oppnå bred forståelse av hvilke faktorer som påvirker ansattes holdninger til bruk og faktisk bruk av sikkerhetstiltak ute på farten. Målet med studien blir dermed å innhente informasjon som tillater en test av hypotesene og gjennom dette belyse problemstillingen.

Bevissthet om ens underliggende filosofiske perspektiv vil hjelpe å skape en klarere formening om hvordan og hva man kan lære gjennom studien. Innenfor den underliggende filosofien skilles det mellom ontologiske og epistemologiske teorier (Oates, 2006).

> «Ontologiske teorier dreier seg om grunnleggende antakelser om hvordan den sosiale verdenen ser ut, mens epistemologiske teorier er ulike oppfatninger om hvordan man kan skaffe seg kunnskaper om denne verdenen.» (Kristoffersen et al., 2011, s. 58).

Denne studien utføres med et positivistisk syn. Positivismen oppfatter at verden kan beskrives og generaliseres med forhold som er kausalt bundet til hverandre. Ved å ha et positivistisk filosofisk perspektiv på forskningen, vil forskeren og samfunnet være to separate elementer, og dermed kan samfunnet kartlegges på en så objektiv måte som mulig (Jacobsen, 2015).

4.1.1. Strategi & Design

En forskningsstrategi er den overordnede fremgangsmåten for å besvare forskningsspørsmålet (Oates, 2006). Problemstillingen til studien er: «Hvilke faktorer kan forklare ansattes bruk av sikkerhetstiltak på mobile enheter når de er ute på farten?» og det må dermed velges en forskningsstrategi som egner seg til å besvare problemstillingen.

For å kunne besvare problemstillingen, brukes en kvantitativ tilnærming basert på data fra ett bestemt tidspunkt. En slik undersøkelse fokuserer på bredde istedenfor dybde og gir et øyeblikksbilde av det fenomenet som skal studeres (Kristoffersen et al., 2011). Hypotesene i studien er basert på teoretisk kunnskap fra litteraturen, og studien blir dermed sett på som deduktiv.

Forskningsdesignet viser planen for å samle inn og behandle data, slik at man kan svare på forskningsspørsmålet. Som illustrert i **Figur 17 – Forskningsdesign**, kan modellen deles opp i to faser og ni deler.

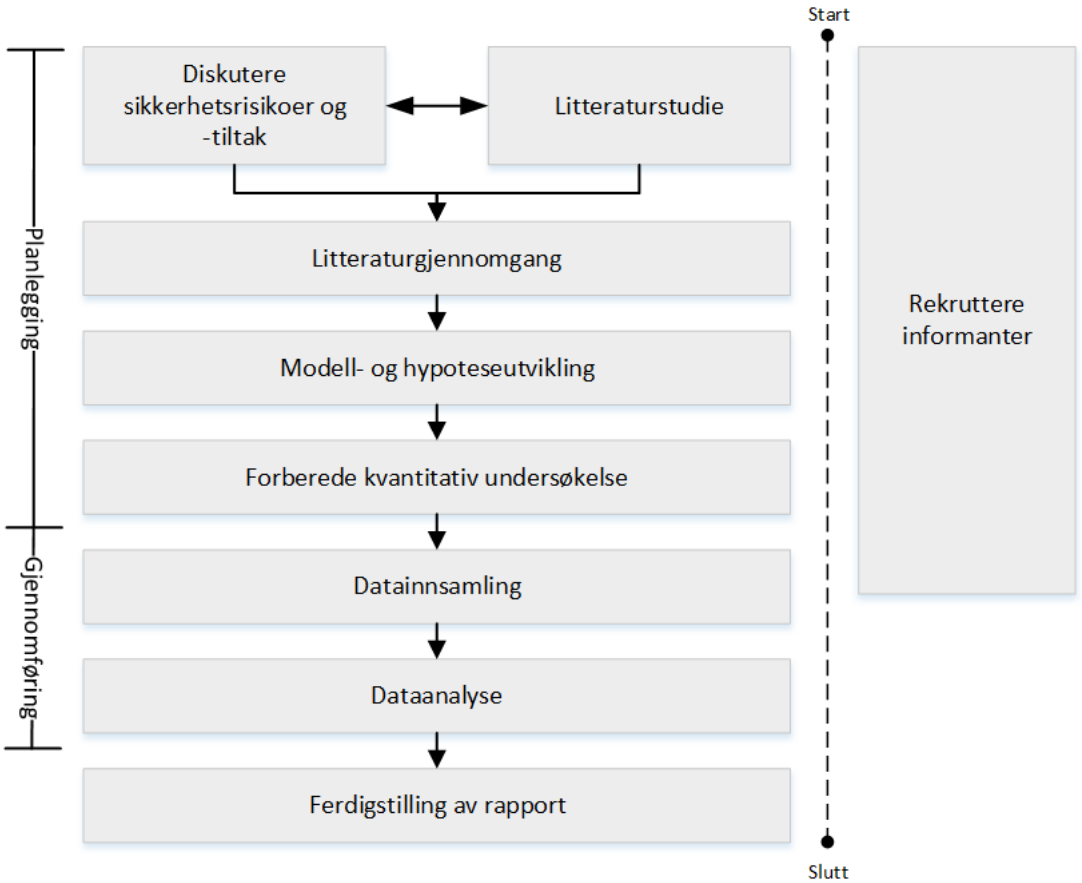
Planleggingsfasen bestod av:

- diskusjon av sikkerhetsrisikoer og -tiltak
- litteraturstudie
- litteraturgjennomgang
- modell- og hypoteseutvikling
- forberede den kvantitative undersøkelsen

Den neste fasen var gjennomføring som bestod av:

- datainnsamling
- dataanalyse

Da spørreundersøkelsen ble sendt ut, var det ikke lenger mulig å endre skjemaet. Det var viktig at arbeidet i planleggingsfasen var grundig, slik at det var mulig å måle det som faktisk skulle måles. For å kunne oppnå et stort nok utvalg, har vi gjennom begge fasene rekruttert respondenter til undersøkelsen.



Figur 17 – Forskningsdesign

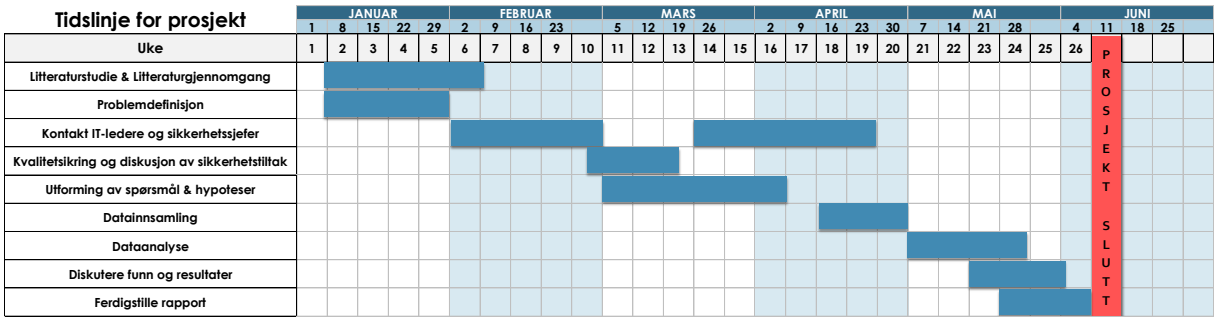
4.1.2. Etiske utfordringer

Det kan argumenteres for at resultatene fra personlighetstesten kan kobles til personlige og/eller faglige interesser. En ansatt er nok ikke interessert i at personlighetstrekkene, sammen med deres holdninger til bruk av sikkerhetstiltak, skal bli kjent for arbeidsgiver. Det ble tatt høyde for dette og dermed ble samme anonyme undersøkelse distribuert over internett til alle deltakende virksomheter. Med tanke på at samme undersøkelse ble distribuert til flere ulike virksomheter, vil det være nærmest umulig å identifisere enkeltpersoner eller virksomheter i undersøkelsen.

I et forsøk på å minske eventuelle misforståelser, ble det sendt ut et skriv til virksomhetene. Dette skrivet forklarte hvem som kunne få tilgang til dataene, hva dataene skulle brukes til, og at det ikke ville være mulig å spore svarene tilbake til respondenten.

4.1.3. Tidsplan

I figuren under er tidsplanen for prosjektet illustrert.



Figur 18 – Tidsplan for prosjektet

For å sikre god progresjon i prosjektet var det nyttig å ha en tidsplan. Det var viktig å holde tidsplanen kontinuerlig oppdatert, for å følge med på store tidtakere i prosjektet, samtidig som vi var oppdatert med hvilke oppgaver som måtte gjøres frem mot innlevering.

4.2. Operasjonalisering og måling av variabler

Operasjonalisering dreier seg om å utvikle et sett med spørsmål som kan brukes til å måle nivået på variablene i forskningsmodellen. Det er vanlig å utvikle et sett med spørsmål (indikatorer) som dekker innholdet til hver bestemt variabel. For eksempel kan ansattes kjennskap til sikkerhetstiltak deles opp i flere forskjellige sikkerhetstiltak.

Vi har valgt å bruke rangordning/ordinalnivå som målenivå for svaralternativene. Ordninalnivå betyr at verdiene kan sorteres etter naturlig størrelse, for eksempel «Jeg følger sikkerhetsreglene i bedriften» kan rangeres på en Likert-skala (Skala 1 = Helt uenig -> 5 = Helt enig). Her kan man bruke svarene til å gruppere enhetene, samt si noe om forholdet mellom kategoriene (Jacobsen, 2015; Kristoffersen et al., 2011).

Et spørsmål med målbare svaralternativer ser omtrent slik ut:

Sikkerhetsråd ute på farten er enkle å forstå

Helt uenig 1 2 3 4 5 Helt enig

For å kunne fange opp holdninger til bruk av sikkerhetstiltak, er det viktig å forstå hvilke situasjoner hvor det er opp til brukeren selv å bestemme om han eller hun vil bruke sikkerhetstiltak. Det er først når den enkelte ansatte er alene og utenfor organisatorisk kontekst at han eller hun har fullstendig kontroll over egne valg. Spørsmålene i studien fokuserer dermed på når den ansatte er «ute på farten». «På farten» handler om de gangene den ansatte bruker mobilen, nettbrettet eller laptop'en på steder utenfor virksomheten.

Eksempler på farten:

- Jobbe på kafé eller andre offentlige steder
- Ute på forretningsreise
- Sjekke e-post eller kalender på vei til jobb

4.2.1. Operasjonalisering av variabler

Litteraturen inneholdt mange gode eksempler på tidligere, godt testet operasjonaliseringer av de ulike variablene. Vi laget dermed et sett med kvantitativt målbare indikatorer for hver variabel i modellen basert på tidligere formuleringer i litteraturen.

Personlighetstrekk

Personlighetstrekk i studien bruker instrumentet BFI-10 av Rammstedt og John (2007). Denne variabelen måler personlighetstrekk med ti indikatorer, med to bipolare indikatorer per personlighetstrekk.

Indikatorene som er reverserte er markert med en (**R**). Skåren fra reverserte indikatorer må snus i dataanalysen (for eksempel lav skår på indikator *ekstroversjon_r* betyr at man ville skåret høyt på ekstroversjon).

- **Skala:**
  1 = Helt uenig --> 5 = Helt enig

Indikator	**Operasjonalisert ved følgende spørsmål**
Jeg ser på meg selv som …	
ekstroversjon	… utadvendt og sosial
ekstroversjon_r	… reservert (**R**)
medgjorlig	… generelt tillitsfull
medgjorlig_r	… finner lett feil ved andre (**R**)
planmessighet	… gjør en godt gjennomført jobb
planmessighet_r	… tendens til å være lat (**R**)
nevrotisme	… lett nervøs
nevrotisme_r	… avslappet og håndterer stress bra (**R**)
apenhet	… har en livlig fantasi
apenhet_r	… lite kunstnerisk interesse (**R**)

Tabell 8 – Operasjonalisering av personlighetstrekk

Kjennskap til sikkerhetstiltak

Kjennskap til sikkerhetstiltak er basert på Bulgurcu et al. (2010) og Dinev og Hu (2007). Denne variabelen har to indikatorer for å måle kjennskap til sikkerhetstiltak:

- **Skala:**
  1 = Helt uenig --> 5 = Helt enig

Indikatorer	**Operasjonalisert ved følgende spørsmål**
isa _1	Generelt sett er jeg godt kjent med virksomhetens sikkerhetsrutiner når jeg er ute på farten
isa_2	Jeg har satt meg godt inn i hvilke sikkerhetsrutiner som gjelder når jeg er ute på farten

Tabell 9 – Operasjonalisering av kjennskap til sikkerhetstiltak

Tro på egen mestringsevne

Tro på egen mestringsevne i studien er basert på Bulgurcu et al. (2010) og Eikebrokk et al. (2011). Denne variabelen måler tro på egen mestringsevne med tre indikatorer:

- **Skala:**
  1 = Helt uenig --> 5 = Helt enig

Indikatorer	Operasjonalisert ved følgende spørsmål
Når jeg ute er på farten …	
se_1	... har jeg de ferdighetene og kunnskapen som trengs for å følge anbefalte sikkerhetsråd
se_2	... klarer jeg å følge anbefalte sikkerhetsrutiner uten hjelp fra andre
se_3	... hjelper jeg andre med anbefalte sikkerhetsrutiner

Tabell 10 – Operasjonalisering av tro på egen mestringsevne

Normer

Normer i studien er identifisert ut ifra den tiltakslisten som ble opprettet i litteraturstudien (se **2.1 Litteraturstudie**). Denne variabelen måler normer med 18 indikatorer. Indikatorene er delt inn i to kategorier basert på hva slags tiltak det er: *situasjonsbestemte* og *tekniske*. De situasjonsbestemte tiltakene er noe brukeren må gjøre når han eller hun kommer i en viss situasjon. De tekniske tiltakene er noe som må aktiveres eller installeres på enheten for at de skal fungere.

- **Skala:**
  1 = Ikke viktig -> 5 = Svært viktig, Vet ikke/ Ikke relevant

Indikator	Operasjonalisert ved følgende spørsmål
Hvor viktig er det at du følger disse sikkerhetsrutinene ute på farten?	
n_situasjon_1	Ikke klikk på filer fra ukjente avsendere
n_situasjon_2	Ikke etterlat enheten uovervåket
n_situasjon_3	Ikke lån bort enheten til fremmede
n_situasjon_4	Ikke bruk samme passord flere steder
n_situasjon_5	Ikke koble til usikrede trådløse nettverk
n_situasjon_6	Ikke bruk ukjent eller uklarert utstyr (f.eks minnepenn)
n_situasjon_7	Ikke skriv ned eller lagre passord (f.eks på gule lapper)
n_situasjon_8	Ikke modifiser (endre) operativsystemet (Jailbreak / Rooting)
n_situasjon_9	Meld fra om sikkerhetshendelser eller mistanke om avvik
n_teknisk_1	Aktivere automatisk lås
n_teknisk_2	Installere antivirusprogram
n_teknisk_3	Aktivere fjernsletting & fjernsporing
n_teknisk_4	Ta jevnlig sikkerhetskopi
n_teknisk_5	Bruk VPN (Virtuelt Privat Nettverk)

n_teknisk_6	Pass på at internettrafikken er kryptert (HTTPS)
n_teknisk_7	Krypter informasjon på enheten
n_teknisk_8	Legg enheten i låsbart skap når den ikke brukes
n_teknisk_9	Skru av Bluetooth & WiFi når det ikke brukes

Tabell 11 – Operasjonalisering av normer

Oppfattet nytteverdi med sikkerhetstiltak

Oppfattet nytteverdi med sikkerhetstiltak er basert på Davis (1989), Dinev og Hu (2007) og Uffen et al. (2013). Denne variabelen måler nytteverdi med tre indikatorer.

Indikator	**Operasjonalisert ved følgende spørsmål**
Ta stilling til følgende påstander om sikkerhetstiltak på farten:	
pu_1	Å følge anbefalte sikkerhetsråd når jeg er ute på farten bidrar til å holde virksomheten trygg
pu_2	Å følge anbefalte sikkerhetsråd når jeg er ute på farten bidrar til å holde informasjon på enheten trygg
pu_3	Å følge anbefalte sikkerhetsråd når jeg er ute på farten har flere fordeler enn ulemper

Tabell 12 – Operasjonalisering av oppfattet nytteverdi med sikkerhetstiltak

Oppfattet brukervennlighet med sikkerhetstiltak

Oppfattet brukervennlighet med sikkerhetstiltak er basert på Davis (1989), Dinev og Hu (2007) og Uffen et al. (2013). Denne variabelen måler brukervennlighet med tre indikatorer.

Indikator	**Operasjonalisert ved følgende spørsmål**
Ta stilling til følgende påstander om sikkerhetstiltak på farten:	
eu_1	Jeg tror de fleste klarer å følge anbefalte sikkerhetsråd når de er ute på farten
eu_2	Det er enkelt å følge anbefalte sikkerhetsråd når man er ute på farten
eu_3	Sikkerhetsråd ute på farten er enkle å forstå

Tabell 13 – Operasjonalisering av oppfattet brukervennlighet med sikkerhetstiltak

Holdninger til bruk av sikkerhetstiltak

Holdninger til bruk av sikkerhetstiltak er basert på Dinev og Hu (2007), Eikebrokk et al. (2011) og Ifinedo (2012). Denne variabelen måler holdninger til bruk med 16 indikatorer. En holdning er ikke entydig, å gjennomføre en holdningsmåling krever dermed at man deler spørsmålet opp i flere skalaer. For eksempel kan en holdning til bruk av et sikkerhetstiltak være positiv og fornuftig, men samtidig tidskrevende.

Holdningsmålinger (semantiske differensialer) lot seg ikke gjennomføre i datainnsamlingsverktøyet SurveyXact. Vi måtte dermed omgjøre spørsmålene til en Likert-skala. Reverserte indikatorer er markert med en (**R**). Skåren fra reverserte indikatorer må snus i dataanalysen på samme måte som personlighetstrekk.

I tillegg til to generelle spørsmål til holdning til bruk, har studien inkludert to scenarioliknende spørsmål. Disse scenarioene er laget ut ifra tiltakslisten. Scenarioene er ment til å dekke to negative handlinger innen informasjonssikkerhet:

- Koble til åpent trådløst nettverk på café
- Gå fra enheten ubevoktet

- **Skala:**
  1 = Helt uenig --> 5 = Helt enig

Indikator	**Operasjonalisert ved følgende spørsmål**
Generelt sett, mener jeg sikkerhet på mobile enheter ute på farten er ...	
att_positiv_r1	... negativt (**R**)
att_fornuftig_1	... fornuftig
att_nyttig_1	... nyttig
att_tid_r1	... tidskrevende (**R**)
For meg, er det å følge virksomhetens retningslinjer for sikkerhet ute på farten ...	
att_positivt_r2	... negativt (**R**)
att_fornuftig_2	... fornuftig
att_nyttig_2	... nyttig
att_tid_r2	... tidskrevende (**R**)
For meg, vil det å koble seg til et åpent trådløst nettverk på café være ...	
att_positivt_1	... negativt
att_fornuftig_r1	... fornuftig (**R**)
att_nyttig_r1	... nyttig (**R**)
att_tid_1	... tidsbesparende
For meg, vil det å gå fra enheten ubevoktet være ...	
att_positivt_2	... negativt
att_fornuftig_r2	... fornuftig (**R**)
att_nyttig_r2	... nyttig (**R**)
att_tid_2	... tidsbesparende

Tabell 14 – Operasjonalisering av holdninger til bruk av sikkerhetstiltak

Kvalitet på support

Kvalitet på support er basert på DeLone og McLean (2003). Denne variabelen måler supportkvalitet tre indikatorer.

- **Skala:**
  1 = Helt uenig --> 5 = Helt enig

Indikatorer	Operasjonalisert ved følgende spørsmål
sq_1	IT-hjelp har gitt meg god opplæring og trening i bruk av sikkerhetsrutiner
sq_2	IT-hjelp gir rask bistand på sikkerhetsrutiner når jeg trenger det
sq_3	IT-hjelp er lett tilgjengelige når jeg trenger assistanse med sikkerhetsrutiner

Tabell 15 – Operasjonalisering av kvalitet på support

Oppfattet kontroll over sikkerhetsatferd

Oppfattet kontroll over sikkerhetsatferd er basert på Eikebrokk et al. (2011). Denne variabelen måler oppfattet kontroll over sikkerhetsatferd med én indikator:

- **Skala:**
  1 = Helt uenig --> 5 = Helt enig

Indikatorer	Operasjonalisert ved følgende spørsmål
Når jeg ute er på farten …	
pbc_1	... er det opp til meg selv å bestemme om jeg skal følge anbefalte sikkerhetsrutiner

Tabell 16 – Operasjonalisering av oppfattet kontroll over sikkerhetsatferd

Faktisk sikkerhetsatferd

Faktisk sikkerhetsatferd er basert på Ajzen (2006). Denne variabelen måler faktisk sikkerhetsatferd med to indikatorer:

- **Skala:**
  1 = Helt uenig --> 5 = Helt enig

Indikatorer	Operasjonalisert ved følgende spørsmål
ab_1	Totalt sett, følger jeg anbefalte sikkerhetsrutiner ute på farten
ab_2	Jeg tenker mye på å holde den mobile enheten trygg ute på farten

Tabell 17 – Operasjonalisering av faktisk sikkerhetsatferd

4.2.2. Operasjonalisering av kontrollspørsmål

I tillegg til spørsmålene knyttet til variablene, ble det laget et par introduksjonsspørsmål. Disse spørsmålene var med i undersøkelsen for å samle inn tilleggsinformasjon til analysen, men også for å ufarliggjøre undersøkelsen for respondenten ved å gi dem noen enkle spørsmål om dem selv.

Først ble det spurt om ulike demografiske forhold. Dette innebar alder, kjønn, utdanning og ansiennitet. Videre ble det spurt om hvilke enheter de selv brukte i en jobbsammenheng. Dette var viktig å avdekke tidlig, slik at respondenten ikke ble sittende å gjennomføre en undersøkelse som ikke var ment for han eller hun. Dersom respondenten mente han eller hun brukte en annen mobil enhet enn det som stod listet opp, fikk respondenten muligheten til å skrive inn i feltet «annet».

Det ble også spurt om respondenten tidligere hadde blitt utsatt for en sikkerhetshendelse og om den mobile enheten hadde blitt konfigurert for å fungere i virksomheten. Tanken bak disse spørsmålene var for å kunne gruppere datasettet i flere deler dersom man fikk nok respondenter.

Til slutt fikk respondenten muligheten til å skrive egne kommentarer til undersøkelsen.

Variabel	Operasjonalisert ved følgende spørsmål	Skala
Alder	Alder Ca. år ____	Respondenten fyller selv ut et tall
Kjønn	Kvinne / Mann	Kvinne <> Mann
Utdanning	Anslå antall år etter grunnskole Ca. år ___	Respondenten fyller selv ut et tall
Ansiennitet	Hvor lenge har du vært ansatt i virksomheten? Ca. år ___	Respondenten fyller selv ut et tall
Mobile enheter	Hvilke(n) mobil(e) enhet(er) bruker du i jobbsammenheng? - Smarttelefon - Nettbrett - Bærbar datamaskin / laptop - Annet	Respondenten velger en eller flere mobile enheter. Dersom «*Annet*» kan respondenten skrive i tekstfelt
Mobile Device Management	Har din(e) mobil(e) enhet(er) blitt konfigurert for å fungere i virksomheten?	Ja, Nei, Vet ikke
Tidligere utsatt for sikkerhetshendelser	Har du tidligere blitt utsatt for en sikkerhetshendelse?	Ja, Nei, Vet ikke

Tabell 18 – Operasjonalisering av kontrollvariabler

4.3. Metode for datainnsamling

Når man skal gå frem for å samle inn data til en kvantitativ undersøkelse, er det flere forhold man bør planlegge. Dette kapitlet inneholder beskrivelser av hvordan datainnsamlingen ble planlagt og gjennomført i studien.

4.3.1. Utvalg og avgrensning

Som problemstillingen antyder, er virksomheter med potensielt mye sensitiv eller konkurransedyktig data interessante for studien. Relevante respondenter for undersøkelsen er ansatte som bruker mobile enheter ute på reise, eller på andre måter befinner seg ute i det offentlige rom. Dette er et relativt stort omfang. For å holde studien innenfor en geografisk ramme, er studien begrenset til Norge og norsktalende personer.

Den opprinnelige planen var å utføre en sannsynlighetsutvelgelse, men dette lot seg ikke gjøre ettersom det var tilnærmet umulig å identifisere en populasjonsliste for utvalget. Det finnes andre former for utvalg som avviker fra sannsynlighetsutvalgene. Disse utvalgene kan gi et systematisk skjevt utvalg, noe som betyr at enkelte relevante grupper kan risikere å ikke bli med i det hele tatt. Til tross for risikoene knyttet til ikke-sannsynlighetsutvelgelser, valgte vi å gjennomføre et skjønnsmessig utvalg etterfulgt av snøballmetoden (Oates, 2006).

I flere tidligere studier om informasjonssikkerhet er det brukt studenter istedenfor ansatte, men det kan diskuteres hvor like disse gruppene egentlig er. Det stilles høyere krav til ansatte fordi de blant annet har signert en arbeidskontrakt. Studien endte dermed med å rekruttere ansatte i virksomheter som banker, advokatfirmaer, forsikringsselskaper, konsulentfirmaer, m.fl. fordi dette var virksomheter med potensielt mange forretningshemmeligheter som kan medføre en sikkerhetsrisiko på reise.

4.3.2. Antall respondenter og tiltak for utvelgelse

For å kunne være i stand til å gjøre en god statistisk analyse av dataene, var det viktig å få tak på nok respondenter. Antallet anbefalte respondenter varierer med hvilken analysemetode som blir brukt. For denne studien falt valget på «*Structural Equation Modelling*» (SEM), mer spesifikt «*Partial Least Squares*-SEM» (PLS-SEM) som blir forklart nærmere i kapittelet **4.4 Metode for dataanalyse**.

I PLS-SEM er det anbefalt å ha et utvalg som er likt eller større enn ett av disse to kriteriene (Hair Jr et al., 2014):

1. Ti ganger større enn antallet formative indikatorer brukt til å måle en enkel variabel
2. Ti ganger større enn antallet strukturelle veier rettet mot en bestemt variabel i den strukturelle modellen

Dette betyr at man må telle antallet variabler i forskningsmodellen for å få et ca. tall på hvor stort utvalget bør være. Forskningsmodellen i denne studien fordeles slik:

- Individuelle faktorer (3 variabler)
- Normer (1 variabel)
- Egenskaper med sikkerhetstiltak (2 variabler)
- Holdninger (1 variabel)
- Kvalitet på support (1 variabel)
- Oppfattet kontroll over sikkerhetsatferd (1 variabel)
- Faktisk sikkerhetsatferd (1 variabel)

Til sammen blir dette ti variabler, som betyr at man bør ha et utvalg på minst 100 respondenter (10*10 = 100). Denne tommelfingerregelen er det samme som å si at størrelsen på utvalget bør være ti ganger antallet piler pekende mot variablene i strukturmodellen (PLS) (Hair Jr et al., 2014).

Først ble det laget en liste over virksomheter med de rette kvalifikasjonene. Listen ble laget først og fremst ut ifra forskernes kunnskap og tidligere jobbsøking, men også ved å bruke plattformer for jobbsøking.

LinkedIn, et sosialt nettverk, ble benyttet for å komme i kontakt med utvalgte virksomheter. Plattformen tillater gratismedlemmer å teste deres «Premium Recruiter» i 30-dager kostnadsfritt. Denne funksjonaliteten gir deg blant annet muligheten å sende mail til andre medlemmer av LinkedIn, uten å være i samme nettverk.

Søkefunksjonen til LinkedIn ble brukt for å finne viktige nøkkelpersoner (CISO, CIO, CEO) i de tiltenkte virksomhetene. Nesten alle virksomhetene på listen var representert på LinkedIn, noe som gjorde denne prosessen relativt enkel. Personer som virket interessert i informasjonssikkerhet, og som forhåpentligvis hadde nok ansvar og interesse for å dele undersøkelsen internt i virksomheten, ble kontaktet. De interessante personene fikk tilsendt en e-post med informasjon om undersøkelsen.

Videre ble snøballmetoden benyttet for å få tak i flere respondenter. De fikk et spørsmål om det var mye reisevirksomhet innad i virksomheten, og om personen var interessert i å dele undersøkelsen internt hos seg til relevante ansatte. Ulempen med dette var at ingen hadde direkte kontroll over hvor mange eller hvilke respondenter som mottok skjemaet.

Dette var en kontinuerlig prosess som varte helt til datainnsamlingen nærmet seg slutten. Da gratisperioden for LinkedIn var over, fortsatte rekrutteringen med tradisjonell e-post. Her ble det anvendt ulike jobbsøkerportaler og virksomhetenes egne hjemmesider.

Totalt ble det sendt ut ca. 150 forespørsler til virksomheter. Prosessen var svært tidskrevende som gjorde at vi måtte svare på spørsmål og kommentarer vedrørende undersøkelsen daglig. Det kan argumenteres for at det kunne blitt gjort flere grep for å sikre en høyere svarprosent. Deler av kommunikasjonen kunne for eksempel blitt overført til telefon. Fordelen med e-post var at vi fikk kommunisert med flere virksomheter på samme tid. Det var også enighet om å ikke sende mer enn én e-epost per virksomhet, fordi flere e-poster og telefonsamtaler kan virke masete, og dermed sette universitetets navn og rykte på spill.

4.3.3. Pre-test

Undersøkelsen ble pre-testet før den ble sendt ut. Pre-testingen ble gjort for å finne eventuelle utydelige formuleringer og annet som kan føre til forvirring hos respondenten. Til sammen deltok åtte personer på pre-testingen, hvorav fire medstudenter, to ansatte fra ulike virksomheter og to sikkerhetssjefer (CISO) i større virksomheter.

Pre-testen ble hovedsakelig gjennomført ved at en av forskerne satt ved siden av respondenten under utfyllingen av spørreskjemaet. Dersom dette ikke lot seg gjøre, ble pre-testen tatt over telefon. Under pre-testingen ble respondenten oppfordret til å tenke høyt. På denne måten fikk man raskt informasjon om spørsmålet ble tolket riktig, samt et visuelt inntrykk av reaksjonene på spørsmålet.

Erfaringer fra pre-testen var svært verdifull. Gjennom pre-testingen kom det frem at ikke alle hadde lik oppfatning av at ordene «innfører», «følger» og «bruker» har samme betydning. Eksempelvis kan det hende at man innfører et tiltak (for eksempel få IT til å legge inn kryptering/en app) som deretter fjerner rollen av å «følge noe» eller bestemme om en vil «bruke» en funksjonalitet/et sikkerhetsråd. Hvem er det da som har innført tiltaket? IT-avdelingen eller personen? Hva måler man da etterpå?

Det var enighet om at formuleringen «å bruke sikkerhetstiltak» ble for uklart for en vanlig respondent. Dersom man bruker et sikkerhetstiltak, følger man jo implisitt virksomhetens krav (normer) om informasjonssikkerhet. Dermed ble det valgt å bruke andre ord enn «sikkerhetstiltak» i undersøkelsen, for eksempel «å følge virksomhetens krav til informasjonssikkerhet» og «følge sikkerhetsråd», noe som gir en mer forståelig beskrivelse for en vanlig ansatt.

Pre-testingen hjalp å gruppere, fjerne og endre spørsmål. En respondent påpekte at han eller hun satt igjen med følelsen av at spørsmålene ble gjentatt flere ganger. Basert på dette ble spørsmålene gruppert ut ifra hva det ble spurt om, istedenfor basert fra variabler og indikatorer (slik det var tidligere), slik at gjennomføringen av undersøkelsen skulle føles naturlig.

4.3.4. Gjennomføring av datainnsamling

Spørreskjemaet ble formidlet og samlet inn over internett ved hjelp av en hyperlenke fra SurveyXact. Denne lenken ble sendt ut til kontaktpersonen i virksomheten, som deretter distribuerte lenken med spørreskjemaet til relevante ansatte. Det ble også laget et skriv, som et forslag til intranettartikkel og e-postoppsett, for å rekruttere flest mulig respondenter i de virksomhetene som hadde takket ja. Dette var for å forenkle den interne rekrutteringsjobben for kontaktpersonen.

Spørreundersøkelsen var delt inn i fem deler:

- Del 1 inneholdt bakgrunnsinformasjon om respondenten. Dette var kjønn, alder, utdanning, hvilke mobile enheter som brukes i jobbsammenheng, m.m.
- Del 2 inneholdt personlighetstrekk fra BFI-10
- Del 3 inneholdt normer fra ledelsen. Dette var en liste over sikkerhetstiltak der respondenten skulle ta stilling til viktighet av normer ute på farten (sikkerhetstiltak)
- Del 4 inneholdt spørsmål knyttet til holdninger til bruk av sikkerhetstiltak, individuelle faktorer og egenskaper med sikkerhetstiltakene.
- Del 5 inneholdt spørsmål knyttet til virksomhetens IT-hjelp. Disse spørsmålene handlet om ulike faktorer knyttet til kvalitet på support i virksomheten.

Hele undersøkelsen inneholdt til sammen 74 spørsmål. Spørsmålene ble gruppert sammen med spørsmål som virket like og passet sammen. Dette var for å skape en bedre flyt og fjerne eventuelle misforståelser om at respondenten har svart på spørsmålet tidligere.

Etter at en respondent hadde gjennomført undersøkelsen, ble dataene sendt automatisk til SurveyXact sin database. Her hadde man kontroll over hvor mange respondenter som hadde gjennomført hele undersøkelsen og hvor mange som hadde svart på deler av den / droppet ut.

Spørreundersøkelsen ble utstedt onsdag den 11.04.2018. Det ble sendt ut purringer kamuflert som takkemeldinger. Purringen inneholdt en takk for vel gjennomført undersøkelse, men også en påminnelse til de som enda ikke hadde deltatt. Dette viste seg å være en effektiv måte å få respondenter til å svare på undersøkelsen.

- Ingen purring: 89 respondenter
- Første purring: 160 respondenter
- Andre purring: 210 respondenter

4.3.5. Reliabilitet og validitet

Reliabilitet og validitet er viktig i forskning. Reliabilitet handler om hvor pålitelige dataene i undersøkelsen er. Dette dreier seg om nøyaktigheten av undersøkelsens data, hvilke data som benyttes, måten data blir samlet inn på og prosesseres (Kristoffersen et al., 2011).

Validitet handler om i hvilken grad undersøkelsen er egnet til å gi gyldige svar på det man ønsker å undersøke. En undersøkelse som skal måle faktisk atferd, men som måler motivasjon, vil for eksempel ikke være valid.

Tiltakene som ble brukt for å sikre validitet og reliabilitet i studien, er listet opp i tabellen under.

Reliabilitet	**Intern validitet**	**Ekstern validitet**
• Undersøkelsen ble pre-testet av åtte forsøkspersoner • Bruk av anerkjente operasjonaliseringer fra tidligere forskningslitteratur (TPB, BFI-10, TAM, D&M ISSM). • Dokumentere de ulike stegene i forskningsprosessen	Innholdsvaliditet • Undersøkelsen ble pre-testet av åtte forsøkspersoner Begrepsvaliditet • Undersøkelsen ble pre-testet av åtte forsøkspersoner	• Bredt utvalg • Bruk av profesjonelle IT-ledere

Tabell 19 – Tiltak for å sikre reliabilitet og validitet

4.3.6. Begrensninger med spørreundersøkelser

Det er begrensninger ved bruk av et spørreskjema. Et spørreskjema går ikke i dybden og i detaljene på forskningsemnet, men fokuserer på bredden og omfanget. Man kan dermed ikke kunne trekke ut respondentenes grunner og følelser til hvorfor de svarer slik de gjør. Respondenten blir også påtvunget spesielle meninger, siden både spørsmålene og svaralternativene er standardisert (Jacobsen, 2015).

4.4. Metode for dataanalyse

Univariate og bivariate analyser har lenge vært populære statistiske metoder å studere data og dens korrelasjoner (Kristoffersen et al., 2011), men takket vært teknologiske verktøy er det nå mulig å finne mer komplekse forhold i dataen (Hair Jr et al., 2014).

I denne studien er det benyttet en avansert datanalysemetode kalt «*Partial Least Squares*» (PLS) – «*Structural Equation Modelling*» (SEM). Denne analysemetoden er en av de to vanlige tilnærmingene til SEM. Den andre, kalt «*Covariance-based*-SEM» (CB-SEM), blir hovedsakelig brukt for å teste etablerte teorier. PLS-SEM, på den andre siden, er foreslått i de situasjoner hvor den strukturelle modellen er kompleks, og det finnes mindre eller lite teori om sammenhengene (Hair Jr et al., 2014).

Dataanalyseprogrammet SmartPLS (Ringle, Wende & Becker, 2015) ble brukt for å gjennomføre dataanalysen. Dette programmet tillater å lage en visuell sti-modell (path-model) som passer forskningsmodellen og tilhørende variabler og hypoteser. Før det var mulig å gjøre en analyse, måtte det gjennomføres noen manuelle steg med dataene.

Det første som ble gjort var å ekskludere respondenter som ikke hadde fullført hele spørreskjemaet. Mange respondenter falt av da de skulle besvare sikkerhetsnormer på farten (del 3) og grunnen til dette er noe uvisst. For å spekulere, kan det hende at:

- Respondenten ikke var på farten i det hele tatt og var dermed irrelevant for undersøkelsen
- Respondenten hadde dårlig tid og/eller syntes det var mange spørsmål på en side

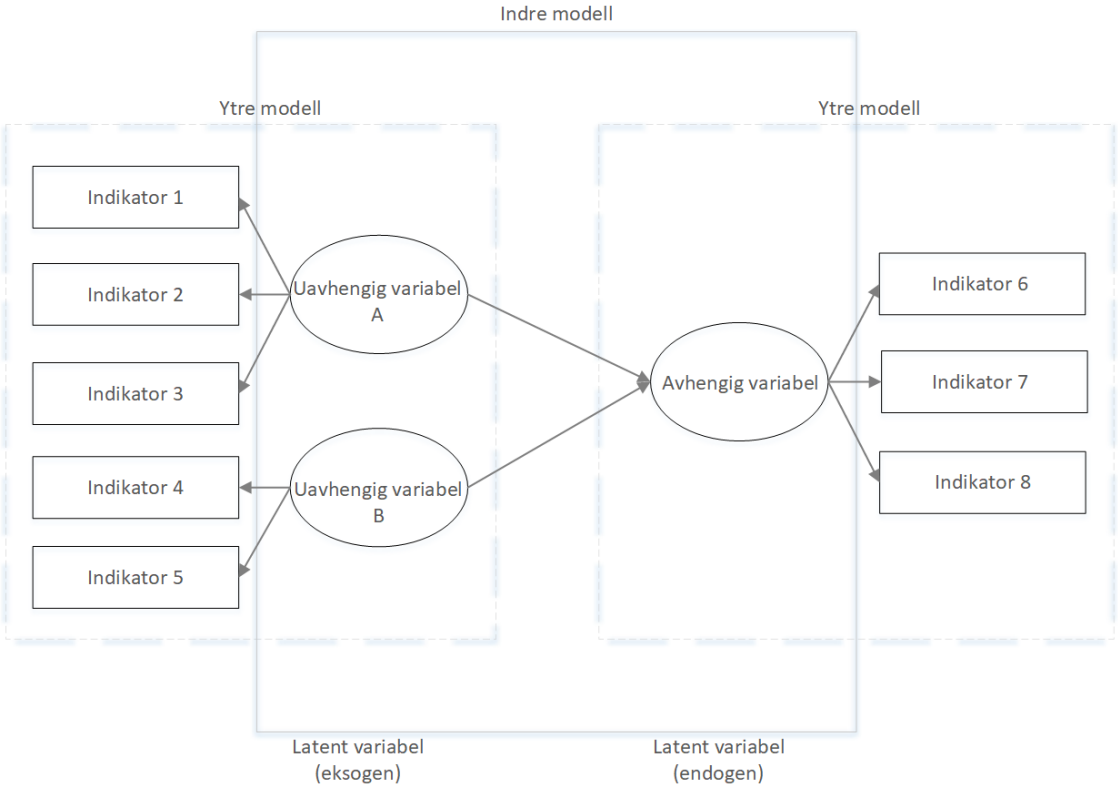
Alle reverserte indikatorer måtte bli snudd manuelt før de ble importert til SmartPLS. De reverserte indikatorene ble snudd ved å ta øverste skala pluss en, deretter subtrahere verdien (Reversert Likert-skala = (Høyeste skalaverdi + 1) – Respondentens svar). Filtreringsprosessen endte med 210 brukbare svar som ble importert til SmartPLS.

I SmartPLS kan man bestemme hva som skal gjøres med tomme felter. Datasettet inneholdt 333 tomme felter, som utgjorde omtrent 2% av totalt utfylte felter (333 av 15207). Disse tomme feltene kommer fra spørsmål om normer i virksomheten. Dersom feltet var tomt, hadde ikke respondenten mulighet til å svare fornuftig på normen, og man kan dermed påstå at normen ikke er tilstede i virksomheten til respondenten.

Det ble brukt «*Pairwise deletion*» for analysen. Dette sørget for at mest mulig av datasettet faktisk ble benyttet i dataanalysen. Dette er det mest fornuftige. «*Mean values replacement*» ville gitt respondenter formening om normer som ikke var tilstede i deres arbeidssituasjon, og «*Case wise deletion*» ville fjernet respondenter som ikke hadde absolutt alle sikkerhetsnormer i virksomheten.

4.4.1 Indre og ytre modell

SEM modellen deles opp i to mindre modeller som vist i **Figur 19 – Indre og ytre modell.** Den indre modellen spesifiserer forholdet mellom de antatt avhengige og uavhengige latente variablene, mens den ytre modellen spesifiserer forholdet mellom de latente variablene og deres tilhørende indikatorer. Variablene i denne SEM modellen deles opp i eksogen og endogen. En eksogen variabel har en eller flere piler pekende mot andre variabler og ingen mot seg selv. En endogen variabel må ha minimum en pil pekende mot seg og presenterer effekten fra variablene som peker mot den (Wong, 2013).



Figur 19 – Indre og ytre modell

4.4.2 Formative og refleksive modeller

Det finnes formative og refleksive indikatorer, og disse kan spesifiseres i SEM. De fleste variablene og medfølgende indikatorer er refleksive i denne studien, men basert på kriteriene til Jarvis, MacKenzie og Podsakoff (2003) og Coltman et al. (2008) (se **Tabell 20 – Forskjeller med refleksive og formative modeller**) argumenteres det for at variablene *Normer* og *Personlighetstrekk* er formative.

I studien kartlegger vi ledelsens normer «nedenfra og opp». Normene framtrer som et resultat av reaksjonen på de tiltakene som representeres. Det vil si at holdningene til bruk av sikkerhetstiltak blir utrykt gjennom hvor viktig man opplever at konkrete tiltak er, og dermed *formativt.* Ledelsens generelle holdning til sikkerhet er uberørt av om ett spesifikt tiltak er relevant eller ikke. Dessuten er det slik at ikke alle konkrete tiltak er tilstede hos alle virksomheter, og dermed blir normene etablert av de tiltakene som finnes hos respondenten.

Hvis vi derimot hadde målt ledelsens generelle holdninger til bruk av sikkerhetstiltak, og bedt respondentene om å utrykke enighet til indikatorer som forklarer denne generelle holdningen, ville normene vært *refleksive*.

Personlighetstrekk måles også formativt. FFM består av fem dimensjoner som ikke kan endres uten at definisjonen til begrepet blir forandret, dermed *formativt*.

Formativ modell	**Refleksiv modell**
Retningen av kausalitet er fra indikatorene til variablene	Retningen av kausalitet er fra variablene til indikatorene
Indikatorene definerer egenskapene til variabelen	Indikatorene er forekomster av variabelen
Endringer i indikatorene bør skape endringer i variabelen	Endringer i indikatoren bør **ikke** skape endringer i variabelen
Endringer i variabelen skaper **ikke** endringer i indikatorene	Endringer i variabelen skaper endringer i indikatorene
Indikatorene må **ikke** være utskiftbare	Indikatorene bør være utskiftbare
Indikatorene må **ikke** ha liknende innhold eller dele et felles tema	Indikatorene bør ha liknende innhold eller dele et felles tema
Å droppe en indikator kan endre det konseptuelle domene av variabelen	Å droppe en indikator bør **ikke** endre det konseptuelle domene av variabelen

Tabell 20 – Forskjeller med refleksive og formative modeller

4.4.3 Sikre god målekvalitet

Det ble gjort flere steg for å sikre reliabilitet og validitet i studien. PLS-SEM er en relativt ny og omfattende analysemetode som har fått mye ris og ros i forskningen. Forskere bytter stadig fokus på hva som bør rapporteres av reliabilitets- og validitetstester, og man trenger ikke lete lenge før en forstår at forskningsfeltet er under utvikling. For eksempel har *Goodness of Fit* (GoF)-indeksen lenge blitt rapportert som en universell måte å validere PLS-SEM modeller, men det tok ikke lang tid før GoF ble kritisert for å gi feil resultater (Hair et al., 2017; Hair Jr et al., 2016).

For å sikre høy målekvalitet (reliabilitet og validitet i PLS-SEM) fulgte vi veletablerte råd og prosedyrer (Hair et al., 2017; Hair Jr et al., 2014; Wong, 2013). I et forsøk på å holde tritt med de råd og anbefalinger som gjelder for PLS-SEM, har vi fulgt rådene i boksamlingen til Hair Jr et al. (2014, 2016). Hair Jr. er en anerkjent forfatter innenfor forskningsmetode, og bøkene hans har blitt sitert over 5000 ganger (sjekket 14.05.18). Bøkene argumenterer godt for hva og hvorfor man skal rapportere med PLS-SEM.

I den ytre modellen varierer stegene ut ifra hvilke indikatorer som blir brukt (refleksive/formative). Denne studien benytter både refleksive og formative indikatorer, og det er dermed naturlig å følge de anbefalte rådene for begge. Rådene for å sikre god målekvalitet i studien er skissert i **Tabell 21 – Tiltak for å sikre god målekvalitet**. Detaljer for gjennomføring finnes i **5. Resultater**.

			Hva er OK?
Ytre modell	Refleksive indikatorer	Indikator Reliabilitet (*Indicator Reliability*)	Hver indikator bør ha en ytre ladning (*outer loading*) på minst **0.70**
		Intern Konsistens (*Internal Consistency Reliability*)	Cronbachs alfa har en del begrensninger (Hair Jr et al., 2014), dermed bruker man kompositt reliabilitet (*composite reliability*). Kompositt reliabilitet bør være minst **0.70**. Hvis det er en utforskende studie aksepteres verdier på minst **0.60**
		Konvergent Validitet (*Convergent Validity*)	Gjennomsnittlig varians (AVE) bør være minst **0.50**
		Diskriminant Validitet (*Discriminant Validity*)	Fornell & Larcker foreslår at kvadratroten til AVE på hver variabel må være større enn korrelasjonen mellom variablene (Hair Jr et al., 2014). Heterotrait-Monotrait (HTMT) bør være mindre enn **0.85 - 0.90** for konseptuelle indikatorer (Hair et al., 2017).
	Formative indikatorer	Indikatorvekt og bidrag	Rapporter t-verdier og f-verdier. Rapporter indikatorvekter og ladninger, se etter signifikante bidrag
		Kollinearitet	Variation Inflation Factor (VIF) mindre enn **5.0**
		Konvergent validitet	Gjennomfør en redundantanalyse
Indre modell		Kollinearitet	VIF mindre enn **5.00**
		Forklart varians	R^2 varierer mellom 0 – 1. **0.25** = svak **0.50** = moderat **0.75** = sterk
		Prediktiv relevans	Q^2 større enn **0.00**
		Effektstørrelse	Effektstørrelse (f^2 & q^2) **0.02** = svak **0.15** = moderat **0.35** = sterk

Tabell 21 – Tiltak for å sikre god målekvalitet

4.5. Ytre modell

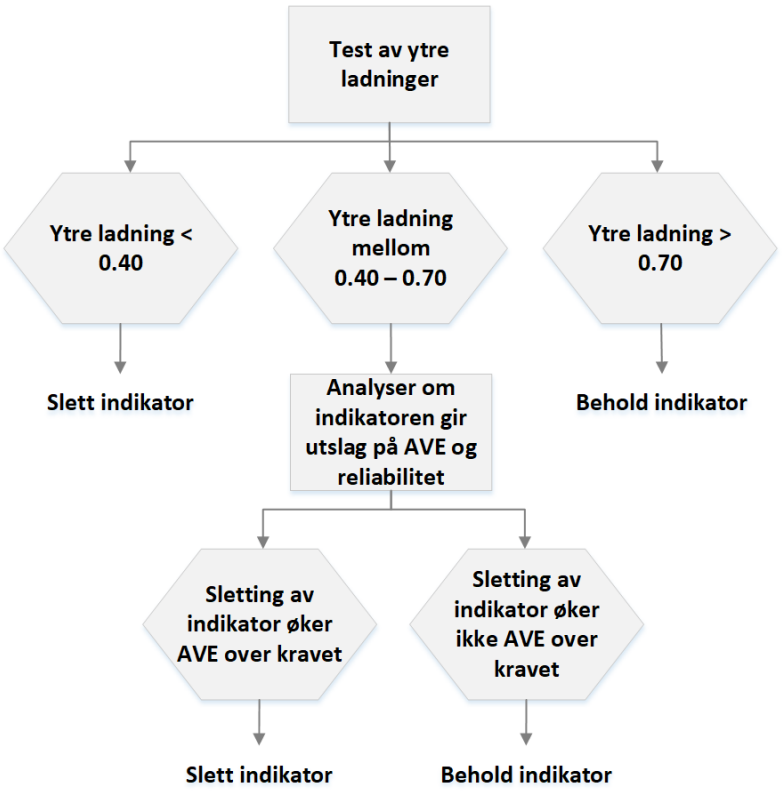
Dette kapitlet går i dybden på reliabilitet og validitet i den ytre modellen. Den ytre modellen forklarer indikatorenes forklaringskraft på variablene. Videre blir de refleksive og formative indikatorene presentert hver for seg, ettersom de har forskjellige krav for reliabilitet og validitet.

4.5.1. Refleksive indikatorer

For å evaluere reliabiliteten og validiteten til refleksive indikatorer må man ta høyde for indikator reliabilitet, intern konsistens, konvergent validitet og diskriminant validitet (se **Tabell 21 – Tiltak for å sikre god målekvalitet**). Disse blir presentert hver for seg.

Reliabilitet - Indikator og intern konsistens

Tradisjonelt sett er «Cronbachs alpha» brukt til å måle intern konsistens. Cronbachs alpha gir et estimat av reliabiliteten basert på korrelasjonen mellom de observerte indikatorene (Hair Jr et al., 2014), men har vist seg å gi en konservativ måling i PLS-SEM (Hair et al., 2017; Wong, 2013). Forskningslitteratur foreslår å erstatte Cronbachs alpha med kompositt reliabilitet (Hair et al., 2017; Wong, 2013). Kompositt reliabilitet tar høyde for den ytre ladningen og måler hvorvidt indikatorene måler samme fenomen. Dersom en indikator har en ladning som er mindre enn 0.40, bør indikatoren slettes. I noen tilfeller kan indikatoren ligge mellom 0.40 og 0.70, men da må man analysere hvorvidt den gjennomsnittlige variansen (AVE) blir påvirket positivt eller negativt dersom indikatoren slettes (Hair Jr et al., 2014).



Figur 20 – Vurderingsprosess for refleksive indikatorer (Hair Jr et al., 2014)

Validitet – Konvergent og diskriminant

Konvergent validitet uttrykker i hvilken grad en måling korrelerer positivt med en alternativ måling av samme variabel. Refleksive indikatorer er forskjellige måter å måle samme fenomen på, dermed bør indikatorene konvergere eller dele en høy varians (Hair Jr et al., 2014). For å sjekke konvergent validitet regner man ut hver variabels gjennomsnittlige varians (AVE). Dersom AVE er minst 0.50, er konvergent validitet tilstede.

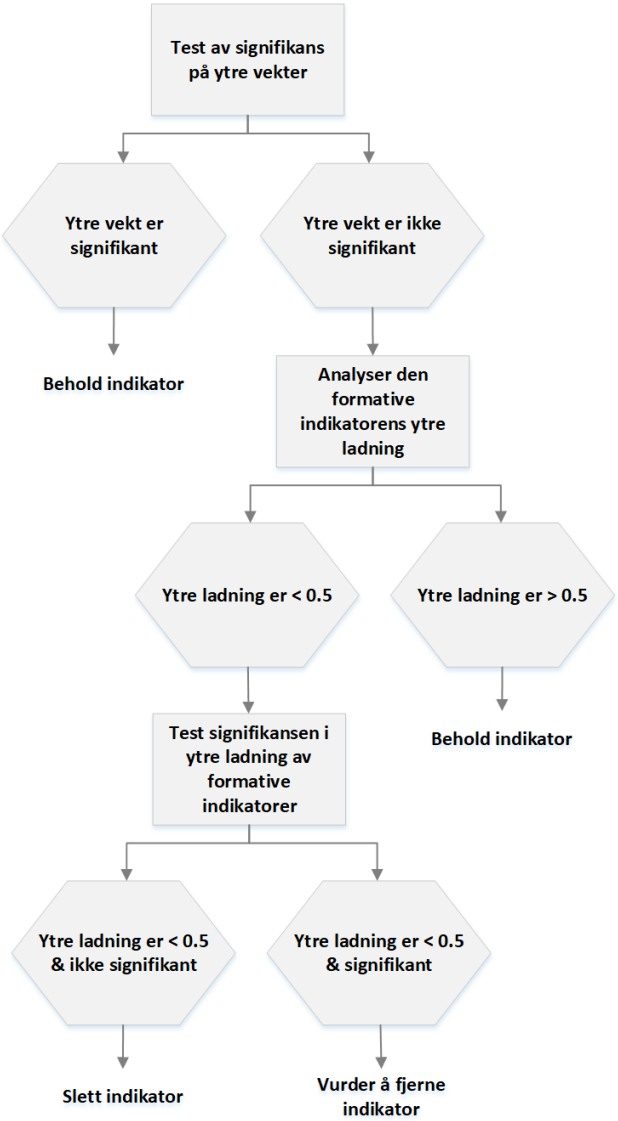
Diskriminant validitet beskriver i hvilken grad en variabel eller indikator er distinkt forskjellig fra de andre variablene eller indikatorene. Forklart med andre ord, en indikator eller variabel som har diskriminant validitet er unik i å fange opp fenomenet den representerer (Hair Jr et al., 2014). I denne utredningen benyttes både Fornell-Larcker-kriteriene og Heterotrait-Monotrait (HTMT) for å måle diskriminant validitet. Fornell-Larcker-kriteriene sammenlikner kvadratroten til en variabels AVE med dens korrelasjoner til andre variabler. Mer spesifikt, må kvadratroten til hver variabels AVE være høyere enn dens høyeste korrelasjon til andre variabler. Logikken bak denne metoden er basert på ideen at en variabel bør ha høyere varians i egne indikatorer enn med andre variabler (Hair Jr et al., 2014).

Fornell-Larcker-kriteriene har mottatt kritikk for, i noen tilfeller, å gi unøyaktige målinger og bruker for mye plass i en utredning. Den siste tiden har det blitt vanligere å bruke HTMT, en mer nøyaktig og plasseffektiv metode (Hair et al., 2017; Henseler, Ringle & Sarstedt, 2015), for å måle diskriminant validitet. En HTMT-måling som er minst 0.85 – 0.90 viser diskriminant validitet (Hair et al., 2017).

4.5.2. Formative indikatorer

For å evaluere reliabiliteten og validiteten til formative indikatorer vil vi se på relevansen og signifikansen til ytre vekter. Først undersøker vi om modellen inneholder kollinearitetsproblemer. Dersom indikatorene har en variansinflasjonsfaktor (VIF) > 5.0 må det gjøres grep for å fjerne multikollinearitet i indikatorene (Hair Jr et al., 2014).

Videre skal t-verdier og p-verdier rapporteres for å se hvilke indikatorer som er signifikante. Ifølge Hair Jr et al. (2014) bør man være forsiktig når man vurderer å slette en formativ indikator. I **Figur 21** er det skissert hva som bør vurderes før man sletter en formativ indikator.



Figur 21 – Vurderingsprosess for formative indikatorer (Hair Jr et al., 2014)

Hair Jr et al. (2014) foreslår også at man skal gjennomføre en redundansanalyse for å måle konvergent validitet. En slik analyse krever at man har en eller flere refleksive indikatorer for å måle samme variabel. Dette må tas hensyn til under datainnsamlingen, noe denne undersøkelsen ikke har gjort.

4.6. Indre modell

Resultatene fra den indre modellen gjør at en kan vurdere hvor godt de empiriske dataene støtter teorien. Før en kan sjekke signifikansen og relevansen av stikoeffisientene i modellen, og dermed beholde eller forkaste hypoteser i studien, må det også kontrolleres for reliabilitet og validitet i indre modell.

4.6.1. Reliabilitet og validitet

Å analysere validitet og reliabilitet i indre modell innebærer å studere modellens prediktive evner og forholdene mellom variablene. Stegene for dette kan oppsummeres slik:

- Analysere om modellen har kollinearitetsproblemer
- Analysere forklart varians (R^2-verdier) og effektstørrelser (f^2-verdier)
- Analyser prediktiv relevans (Q^2-verdier) og effektstørrelser (q^2-verdier)

Det første steget er å måle kollinearitet i modellen. Kollinearitet måles likt som i den ytre modellen ved å sjekke variansinflasjonsfaktoren (VIF) (Hair Jr et al., 2014). VIF bør være < 5.00.

Videre i neste steg rapporteres forklart varians, (R^2). Verdiene varierer fra 0 – 1, der høye verdier indikerer at modellen har høy prediksjonskraft. R^2 uttrykker modellens prediktive kraft og representerer de eksogene latente variablenes kombinerte effekt på den endogene latente variabelen (Hair Jr et al., 2014). Det er vanskelig å si hva som er en akseptabel R^2-verdi, fordi verdiene avhenger av hvor kompleks modellen er, i hvilket forskningsområde man er i, samt hvor langt teoretiseringen har kommet på det aktuelle feltet. Denne studien følger Hair et al. (2017)'s tommelfingerregel, og dermed gir R^2-verdier på 0.75 høy, 0.50 moderat og 0.25 svak prediksjonskraft.

I tillegg til å rapportere R^2, er det også interessant å analysere forandring i R^2 dersom man fjerner en eksogen latent variabel fra modellen. Dette kalles effektstørrelser f^2. Effektstørrelsene (f^2) går ut på å se etter endringer i R^2-verdien når en eksogen variabel utelates fra modellen. Dette gjøres for å vurdere om variabelen har en innvirkning på den endogene (avhengige) variabelen. f^2-verdier indikerer at den eksogene variabelen har en liten (< 0.02), mellomstor (< 0.15) eller stor (< 0.35) effekt på den endogene variabelen (Hair Jr et al., 2014).

Det siste steget er å analysere Stone-Geisser's Q^2-verdi, omtalt som prediktiv relevans (Q^2-verdier), og deretter regne ut effektstørrelser (q^2-verdier). Q^2 måler hvor bra den refleksive modellen kan forklare originale observerte verdier. Q^2-prosedyren gjelder ikke for formative modeller, og dermed blir normer og personlighetstrekk utelukket fra denne beregningen. Q^2-verdier større enn 0 indikerer at modellen har prediktiv relevans (Hair Jr et al., 2014). Effektstørrelsen til Q^2 (q^2) utregnes på samme måte som effektstørrelsen f^2 og viser endringer i prediksjonskraft ved å utelate variabler fra modellen.

4.6.2. Stikoeffisienter

For å bekrefte eller avkrefte hypoteser i studien, analyserer vi signifikansen og relevansen til stikoeffisientene i modellen. Et estimat av stikoeffisientene representerer de antatte forholdene mellom variablene. Stikoeffisientene har standardiserte verdier mellom -1 og +1, der verdier nærmere +1 representerer sterke positive forhold som nesten alltid er statistisk signifikant. Tall som er nærmere 0 representerer svake forhold og verdier nærmere -1 representerer sterke negative forhold.

Stikoeffisient	**Styrke**
0.00 - 0.29	Svak
0.30 - 0.49	Lav
0.50 - 0.69	Moderat
0.70 - 0.89	Sterk
0.90 - 1.0	Veldig sterk

Tabell 22 – Tommelfingerregel for evaluering av styrken til stikoeffisienter (adoptert fra: Pett, Lackey & Sullivan, 2003)

Om en koeffisient er signifikant, avhenger av dens standardavvik. Standardavviket åpner opp muligheten til å regne ut den empiriske t-verdien. Hvis den empiriske t-verdien er større enn den kritiske verdien, kan man si at koeffisienten er signifikant på et bestemt nivå (signifikansnivå). Vanlige kritiske verdier for en *to-halet* test er 1.65 (signifikansnivå = 10%), 1.96 (signifikansnivå = 5%) og 2.57 (signifikansnivå = 1%). Vanlige kritiske verdier for en *en-halet* test er 1.28 (signifikansnivå = 10%), 1.65 (signifikansnivå = 5%) og 2.33 (signifikansnivå = 1%). Valg av kritiske verdier avhenger av hva som er hensikten med studien (Hair Jr et al., 2016).

Dersom hypotesene er formulert slik at retningen er spesifisert, for eksempel slik at mer av en egenskap gir mer av noe annet, er hypotesen ensidig. På den andre siden sier ikke tosidig hypoteser (to-halet tester) noe om hvordan relasjonen er, men bare at det er en uspesifisert relasjon mellom en egenskap og noe annet. Denne studien har hypoteser som sier at det er positive eller negative sammenhenger i dataen og opererer dermed med ensidige hypoteser (en-haletester).

Sammen med t-verdier, er det også vanlig å rapportere p-verdier. p-verdier representerer sannsynligheten for feilaktig vurdering av nullhypotesen. Jo lavere p-verdi desto sterkere bevis mot nullhypotesen. I samfunnsforskning er det vanlig å ha et signifikansnivå på 0.05 eller 0.01 (Jacobsen, 2015). Stikoeffisienter som ligger under dette nivået ($p \leq 0.05 \mid p \leq 0.01$) blir regnet som signifikante.

5. Resultater

I dette kapitlet rapporteres resultatene fra dataanalysen. Under dataanalysen er det brukt forkortelser og disse er oppsummert i tabellen under (**Tabell 23**).

Forklaring	Forkortelse
Personlighetstrekk	P
Kjennskap til sikkerhetstiltak (Information System Awareness)	ISA
Oppfattet brukervennlighet (Perceived Usefulness)	PU
Oppfattet brukbarhet (Ease of Use)	EU
Holdninger til bruk av sikkerhetstiltak (Attitude)	ATT
Normer (Norms)	N
Tro på egen mestringsevne (Self-Efficacy)	SE
Oppfattet kontroll over sikkerhetsatferd (Perceived Behavior Control)	PBC
Supportkvalitet (Support Quality)	SQ
Faktisk sikkerhetsatferd (Actual behavior)	AB

Tabell 23 – Viktige forkortelser brukt i dataanalysen

5.1. Deskriptiv statistikk

I tabellen under (**Tabell 24**) presenteres deskriptiv statistikk fra respondentene

Kategori	**Verdier**
Antall respondenter	210
Alder	Min = 20 Max = 65 Gj.snitt = 40,2 Std.avvik = 10,9
Kjønn	Menn = 121 (57,6%) Kvinner = 89 (42,4%)
Utdanning (Antall år etter grunnskole) *Grunnskole er den 10-årige (tidl. 9 år) obligatoriske skolen for barn og ungdom i alderen 6-16 år*	Min = 0 Max = 12 Gj.snitt = 6,1 Std.avvik = 0,5
Ansiennitet	Min = 0 Max = 38 Gj.snitt = 8 Std.avvik = 7,8
Mobile enheter	Laptop = 202 Smarttelefon = 202 Nettbrett = 42 Annet = 3 (Smartklokker)
Enhet konfigurert for å fungere i virksomheten	Ja = 175 (83%) Nei = 40 (10%) Vet ikke = 15 (7%)
Tidligere utsatt	Ja = 64 (30%) Nei = 136 (65%) Vet ikke = 10 (5%)

Tabell 24 – Deskriptiv statistikk om respondentene fra undersøkelsen

5.2. Ytre modell

Her blir resultatene fra den ytre modellen rapportert. Først presenteres målinger fra de refleksive modellene, etterfulgt av målinger fra de formative modellene.

5.2.1. Måling av refleksive modeller

Etter noen grep hadde de refleksive indikatorene både god reliabilitet og validitet. Det ble målt kompositt reliabilitet og indikatorenes ytre ladning ved å kjøre PLS-beregningen i SmartPLS. Indikatorer som ikke oppfylte kriteriene for reliabilitet ble fjernet.

Å måle en holdning krever at en deler spørsmålet opp i flere skalaer fordi en holdning nødvendigvis ikke er entydig. For eksempel kan «Holdning mot trening» være gunstig og positivt, men samtidig strevsomt og tidskrevende. Slike semantiske differensialer (holdningsmåling) viste seg å være umulig å gjennomføre i verktøyet SurveyXact.

For å sikre gode verdier i refleksive modeller ble det slettet elleve indikatorer knyttet til holdninger. Alle spørsmålene var hentet fra tidligere formuleringer i litteraturen, men spørsmålene ble omgjort til en Likert-skala for å fungere i SurveyXact. Dette kan forklare hvorfor man fikk lave verdier. Til slutt satt man igjen med fem indikatorer med gode verdier, noe som bør være nok til å fange opp holdningene.

Variabel	Indikator	Ytre ladning	Kompositt reliabilitet	Gjennomsnittlig varians (AVE)
Faktisk sikkerhetsatferd	ab_1	0.897	0.872	0.773
	ab_2	0.861		
Holdninger til bruk av sikkerhetstiltak	att_fornuftig_1	0.752	0.889	0.617
	att_fornuftig_2	0.829		
	att_nyttig_1	0.761		
	att_nyttig_2	0.857		
	att_positivt_r2	0.721		
Brukervennlighet med sikkerhetstiltak	eu_1	0.823	0.891	0.732
	eu_2	0.900		
	eu_3	0.842		
Kjennskap til sikkerhetstiltak	isa_1	0.946	0.948	0.901
	isa_2	0.952		
Oppfattet kontroll over sikkerhetsatferd	pbc_1	1.000	1.000	1.000
Nytteverdi med sikkerhetstiltak	pu_1	0.902	0.905	0.761
	pu_2	0.908		
	pu_3	0.803		
Tro på egen mestringsevne	se_1	0.930	0.879	0.711
	se_2	0.871		
	se_3	0.712		
Kvalitet på support	sq_1	0.837	0.940	0.796
	sq_2	0.908		
	sq_3	0.923		
	sq_4	0.900		

Tabell 25 – Reliabilitet og intern konsistens av refleksive indikatorer

Fornell-Larcker-kriteriene og HTMT ble beregnet i SmartPLS med PLS-algoritmen. Resultatene er i tabellene under (**Tabell 26** og **Tabell 27**).

	1. AB	2. ATT	3. EU	4. ISA	5. PBC	6. PU	7. SE	8. SQ
1. Faktisk sikkerhetsatferd	**0.879**							
2. Holdninger til bruk	0.375	**0.786**						
3. Brukervennlighet med sikkerhetstiltak	0.389	0.504	**0.855**					
4. Kjennskap til sikkerhetstiltak	0.672	0.281	0.396	**0.949**				
5. Oppfattet kontroll over atferd	-0.048	-0.259	-0.104	0.005	**1.000**			
6. Nytteverdi med sikkerhetstiltak	0.388	0.595	0.373	0.274	-0.302	**0.872**		
7. Tro på egen mestringsevne	0.481	0.188	0.393	0.651	0.020	0.193	**0.843**	
8. Kvalitet på support	0.351	0.364	0.267	0.256	-0.140	0.410	0.194	**0.892**

Tabell 26 – Validitet i ytre modell: Fornell-Larcker-kriterier

	1. AB	2. ATT	3. EU	4. ISA	5. PBC	6. PU	7. SE	8. SQ
1. Faktisk sikkerhetsatferd								
2. Holdninger til bruk	0.480							
3. Brukervennlighet med sikkerhetstiltak	0.505	0.604						
4. Kjennskap til sikkerhetstiltak	0.832	0.321	0.469					
5. Oppfattet kontroll over atferd	0.055	0.282	0.114	0.031				
6. Nytteverdi med sikkerhetstiltak	0.504	0.696	0.436	0.315	0.329			
7. Tro på egen mestringsevne	0.629	0.228	0.488	0.766	0.058	0.231		
8. Kvalitet på support	0.430	0.410	0.308	0.279	0.151	0.457	0.216	

Tabell 27 – Validitet i ytre modell: HTMT

5.2.2. Måling av formative modeller

Kollinearitetstatistikk kan leses av i SmartPLS ved å kjøre PLS-algoritmen. For å beregne t-verdier og p-verdier ble det kjørt en en-halet (*one-tailed*) bootstrapping i SmartPLS. Som illustrert i **Tabell 28 – Reliabilitet og validitet av formative indikatorer**, har ingen av indikatorene kollinearitetsproblemet (VIF større enn 5.0), men det er kun tre som har signifikant vekt: *n_teknisk*_2, *p_ekstroversjon* og *p_planmessighet_r* (p mindre enn 0.05). Basert på anbefalingene til Hair Jr et al. (2014), ble indikatorene analysert videre ved å se på ytre ladninger og signifikansen av dem. Dersom en ytre ladning var mindre enn 0.50 og ikke-signifikant var det rådet å fjerne indikatoren.

Variabel	Indikator	Vekt	T-verdi	P-verdi	VIF
Normer	n_situasjon_1	0.094	0.679	0.249	1.279
	n_situasjon_2	-0.124	0.645	0.259	1.837
	n_situasjon_3	0.010	0.056	0.478	1.829
	n_situasjon_4	0.150	0.893	0.186	1.831
	n_situasjon_5	-0.053	0.296	0.384	1.760
	n_situasjon_6	-0.041	0.219	0.413	1.656
	n_situasjon_7	0.145	1.094	0.137	1.228
	n_situasjon_8	0.297	1.029	0.152	2.022
	n_situasjon_9	0.105	0.577	0.282	1.568
	n_teknisk_1	0.185	0.891	0.186	1.612
	n_teknisk_2	0.475	2.540	**0.006**	1.859
	n_teknisk_3	0.107	0.430	0.334	2.231
	n_teknisk_4	0.003	0.016	0.494	2.100
	n_teknisk_5	0.020	0.089	0.464	1.702
	n_teknisk_6	0.261	1.228	0.110	1.936
	n_teknisk_7	-0.192	0.436	0.331	3.551
	n_teknisk_8	-0.096	0.522	0.301	2.032
	n_teknisk_9	0.243	1.404	0.080	1.831
Personlighetstrekk	p_apenhet	0.198	1.101	0.136	1.125
	p_apenhet_r	-0.307	1.313	0.095	1.110
	p_ekstroversjon	0.460	1.766	**0.039**	1.583
	p_ekstroversjon_r	-0.271	1.033	0.151	1.489
	p_medgjorlig	0.107	0.561	0.287	1.111
	p_medgjorlig_r	0.059	0.296	0.383	1.235
	p_nevrotisme	0.289	1.110	0.134	1.504
	p_nevrotisme_r	-0.384	1.393	0.082	1.345
	p_planmessighet	-0.087	0.406	0.342	1.186
	p_planmessighet_	0.787	2.353	**0.009**	1.271

Tabell 28 – Reliabilitet og validitet av formative indikatorer

Til tross for rådene til Hair Jr et al. (2014), kan man ikke bare fjerne en formativ indikator. Hovedforskjellen mellom refleksive og formative variabler er hva som skaper variansen. Refleksive variabler forårsaker varians i indikatorene, og motsatt skaper formative indikatorer varians i variabelen. Å fjerne en formativ indikator kan bety forskjellen på om variabelen blir forklart av indikatorene eller ikke. Dermed bør man være ekstra forsiktig med formative modeller.

Cenfetelli og Bassellier (2009) skriver at antallet indikatorer i en formativ modell har viktige implikasjoner for den statistiske signifikansen og vekten til indikatorene. Et større antall indikatorer resulterer ofte i at det er flere indikatorer med lav vekt, samt ikke-signifikante. Videre argumenterer Cenfetelli og Bassellier (2009) for at så lenge forskerne klarer å argumentere for viktigheten av indikatorene bør de beholdes.

For å ivareta hele bredden i det som studeres, valgte vi å beholde alle de formative indikatorene. I litteraturen diskuteres det mye rundt forskjellen mellom formative og refleksive målemodeller (Coltman et al., 2008; Jarvis et al., 2003). Ett argument for å bruke formative modeller er at en også vil oppdage konkrete underliggende forhold som faktisk gjør at den latente variabelen får forklaringskraft mot det andre begrepet. Hvis man i denne utredningen hadde fjernet noen indikatorer (for eksempel normer), ville det vært en undersøkelse med kun et utdrag av aktuelle sikkerhetstiltak i bedrifter. Dette ville vært problematisk.

5.3. Indre modell

Her blir resultatene fra den indre modellen rapportert. Først presenteres målinger fra reliabilitets- og validitetstester, deretter hypotesetesting, etterfulgt av *«model-fit»*.

5.3.1. Måling av reliabilitet og validitet

Resultatene fra reliabilitet og validitet kan leses i **Tabell 29 – Reliabilitet og validitet i indre modell**. Alle kollinearitetsmålinger ligger under kravet (VIF mindre enn 5.0), noe som betyr at den indre modellen ikke inneholder kollinearitetsproblemer/multikollinearitet.

Begge de endogene variablene i modellen (ATT og AB) karakteriseres av svak forklart varians (R^2 mindre enn 0.50). Sagt med andre ord, forklarer modellen 48% av variansen i «Holdninger til bruk (ATT)» og 20% i «Faktisk sikkerhetsatferd (AB)». Det er gjort få studier av individers sikkerhetsatferd ved mobile enheter, og derfor er forklart varians mindre viktig. Vi mener at rapportert R^2 er god for ATT, men moderat til svak for AB.

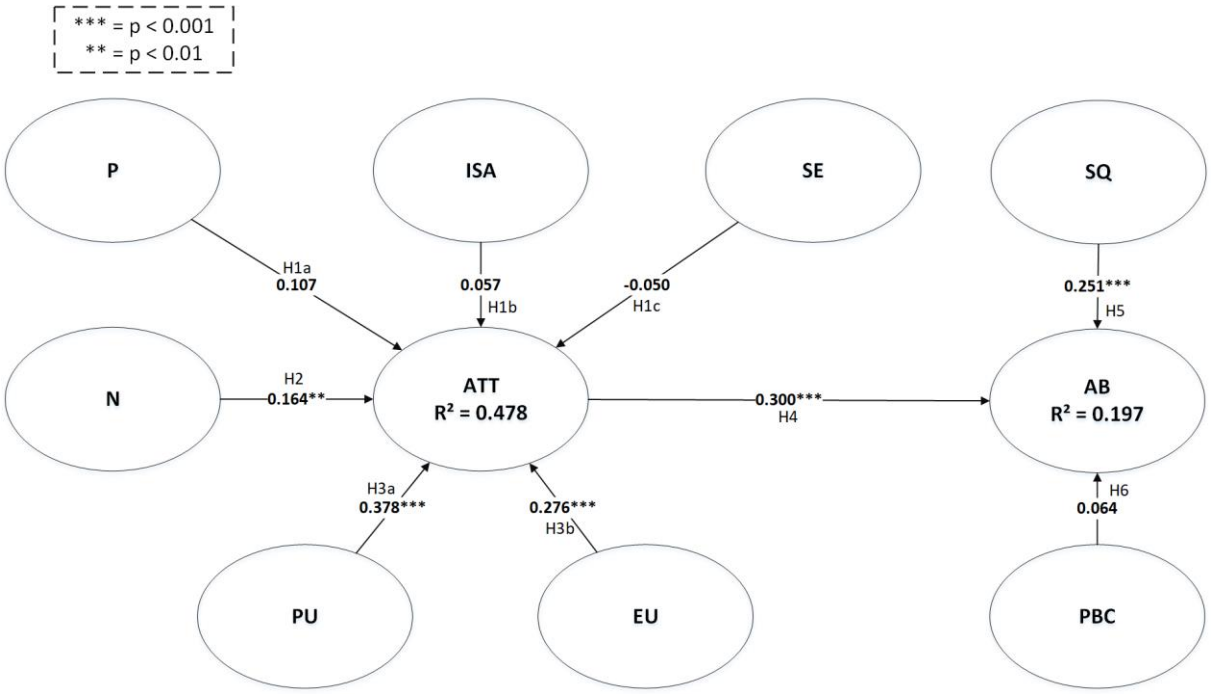
Modellen har prediktiv relevans med verdier betydelig over anbefalt minimumsverdi (Q^2 større enn 0.0).

Stien Nytteverdi -> Holdning til bruk (PU->ATT) har en mellomstor effektstørrelse (f^2 & q^2 større enn 0.15). De andre stiene i modellen har en lav effektstørrelse.

Endogen variabel	Sti	VIF	Forklart varians (R^2)	Effektstørrelse (f^2)	Prediktiv relevans (Q^2)	Effektstørrelse (q^2)
Holdninger til bruk	P -> ATT	1.107	0.478	0.020	0.263	0.005
	ISA -> ATT	1.860		0.003		0.001
	SE -> ATT	1.845		0.003		0.000
	N -> ATT	1.503		0.030		0.001
	PU -> ATT	1.519		0.181		0.184
	EU -> ATT	1.473		0.099		0.045
Faktisk sikkerhetsatferd	ATT -> AB	1.214	0.197		0.139	
	SQ -> AB	1.156		0.068		0.046
	PBC -> AB	1.074		0.005		0.002

Tabell 29 – Reliabilitet og validitet i indre modell

5.3.2. Hypotesetesting



Figur 22 – Resultater fra analyse av indre modell (stikoeffisienter & p-verdier)

P-verdiene viser sannsynligheten for at relasjonen (stikoeffisienten) som PLS har regnet ut, skyldes tilfeldigheter i materialet. Vi har utført testene med et signifikansnivå på 5%, dermed må p-verdien ligge under 0.05 for at målingen skal kunne være signifikant.

For å kalkulere stikoeffisientene i den indre modellen ble det kjørt en en-halet *Bootstrap* med 5000 grupper i SmartPLS. Denne algoritmen gav svar på t-verdier og p-verdier ved å teste datasettet mot 5000 utdrag av observasjoner fra datafila (Hair Jr et al., 2014). Tabellen under viser et forenklet bilde av resultatene fra analysen.

Endogen variabel	Sti & hypotese		Stikoeffisient	T-verdi	P-verdi	Signifikansnivå
Holdninger til bruk	P -> ATT	H1a	0.107	1.364	0.086	Ikke-signifikant
	ISA -> ATT	H1b	0.057	0.865	0.194	Ikke-signifikant
	SE -> ATT	H1c	-0.050	0.705	0.240	Ikke-signifikant
	N -> ATT	H2	0.164	2.389	0.008	p < 0.01
	PU -> ATT	H3a	0.378	5.264	0.000	p < 0.001
	EU -> ATT	H3b	0.276	4.215	0.000	p < 0.001
Faktisk sikkerhetsatferd	ATT -> AB	H4	0.300	4.000	0.000	p < 0.001
	SQ -> AB	H5	0.251	3.044	0.001	p < 0.001
	PBC -> AB	H6	0.064	1.061	0.144	Ikke-signifikant

Tabell 30 – Resultater fra indre modell

Hypotese H1a:
Det er en positiv sammenheng mellom personlighetstrekk og holdninger til bruk av sikkerhetstiltak.

Latent variabel	Stikoeffisient	T-verdi	P-verdi	Resultat
P -> ATT	0.107	1.364	0.086	Nær støttet.

Analysen av hypotesen viser en korrelasjon mellom personlighetstrekk og holdninger til bruk på 0.107. P-verdien på 0.086 viser at den empiriske støtten er nær signifikant. Dermed er denne hypotesen **nær støttet.**

Hypotese H1b:
Det er en positiv sammenheng mellom kjennskap til sikkerhetstiltak og holdninger til bruk av sikkerhetstiltak.

Latent variabel	Stikoeffisient	T-verdi	P-verdi	Resultat
ISA -> ATT	0.057	0.865	0.194	Ikke støttet.

Analysen av hypotesen viser en korrelasjon mellom kjennskap til sikkerhetstiltak og holdninger til bruk på 0.057. P-verdien på 0.194 viser at den empiriske støtten er ikke-signifikant. Dermed er denne hypotesen **ikke støttet**.

Hypotese H1c:
Det er en positiv sammenheng mellom tro på egen mestringsevne og holdninger til bruk av sikkerhetstiltak.

Latent variabel	Stikoeffisient	T-verdi	P-verdi	Resultat
SE -> ATT	-0.050	0.705	0.240	Ikke støttet.

Analysen av hypotesen viser en korrelasjon mellom tro på egen mestringsevne og holdninger til bruk på -0.050. P-verdien på 0.240 viser at den empiriske støtten er ikke-signifikant. Dermed er denne hypotesen **ikke støttet**.

Hypotese H2:
Det er en positiv sammenheng mellom normer og holdninger til bruk av sikkerhetstiltak.

Latent variabel	Stikoeffisient	T-verdi	P-verdi	Resultat
N -> ATT	0.164	2.389	0.008	Støttet.

Analysen av hypotesen viser en korrelasjon mellom normer og holdninger til bruk på 0.164. P-verdien på 0.008 viser at den empiriske støtten er sterkt signifikant. Dermed er denne hypotesen **støttet.**

Hypotese H3a:
Det er en positiv sammenheng mellom oppfattet nytteverdi av sikkerhetstiltak og holdninger til bruk av sikkerhetstiltak.

Latent variabel	Stikoeffisient	T-verdi	P-verdi	Resultat
PU -> ATT	0.378	5.264	0.000	Støttet.

Analysen av hypotesen viser en korrelasjon mellom nytteverdi og holdninger til bruk på 0.378. P-verdien på 0.000 viser at den empiriske støtten er sterkt signifikant. Dermed er denne hypotesen **støttet.**

Hypotese H3b:
Det er en positiv sammenheng mellom brukervennlighet av sikkerhetstiltak og holdninger til bruk av sikkerhetstiltak.

Latent variabel	Stikoeffisient	T-verdi	P-verdi	Resultat
EU -> ATT	0.276	4.215	0.000	Støttet.

Analysen av hypotesen viser en korrelasjon mellom brukervennlighet og holdninger til bruk på 0.276. P-verdien på 0.000 viser at den empiriske støtten er sterkt signifikant. Dermed er denne hypotesen **støttet.**

Hypotese H4:
Det er en positiv sammenheng mellom holdninger til bruk av sikkerhetstiltak og faktisk sikkerhetsatferd

Latent variabel	Stikoeffisient	T-verdi	P-verdi	Resultat
ATT -> AB	0.300	4.000	0.000	Støttet.

Analysen av hypotesen viser en korrelasjon mellom holdninger til bruk og faktisk sikkerhetsatferd på 0.300. P-verdien på 0.000 viser at den empiriske støtten er sterkt signifikant. Dermed er denne hypotesen **støttet.**

Hypotese H5:
Det er en positiv sammenheng mellom kvalitet på support og faktisk sikkerhetsatferd.

Latent variabel	Stikoeffisient	T-verdi	P-verdi	Resultat
SQ -> AB	0.251	3.044	0.001	Støttet.

Analysen av hypotesen viser en korrelasjon mellom supportkvalitet og faktisk sikkerhetsatferd på 0.251. P-verdien på 0.001 viser at den empiriske støtten er sterkt signifikant. Dermed er denne hypotesen **støttet.**

Hypotese H6:
Det er en positiv sammenheng mellom oppfattet kontroll over sikkerhetsatferd og faktisk sikkerhetsatferd.

Latent variabel	Stikoeffisient	T-verdi	P-verdi	Resultat
PBC -> AB	0.064	1.061	0.144	Ikke støttet.

Analysen av hypotesen viser en korrelasjon mellom oppfattet kontroll over sikkerhetsatferd og faktisk sikkerhetsatferd på 0.064. P-verdien på 0.144 viser at den empiriske støtten er ikke-signifikant. Dermed er denne hypotesen **ikke støttet**.

5.3.3. Model-fit

Basert på råd fra Hair Jr et al. (2016) blir det ikke rapportert «*Goodness-of-fit»* (GoF). For å vurdere hvorvidt modellen kan fange opp observert varians i vårt datamateriale, vil vi rapportere SRMR-verdier («*Standardized Root Mean Residual»).* SRMR er den standardiserte forskjellen mellom den observerte korrelasjonen i datamaterialet og den antatte korrelasjonen gitt modellens teoretiske relasjoner (Hair Jr et al., 2016). Denne metoden er ikke grundig testet i PLS-SEM og har derfor ikke fått noen standardiserte kriterier. Rapporten følger den konservative fremgangsmåten. SRMR-verdier mindre enn 0.08 betyr at modellen passer i forhold til korrelasjonsmønsteret som impliseres av teorien som brukes (Hair Jr et al., 2014, 2016).

	Saturated Model	**Estimated Model**
SRMR	0.070	0.079

Tabell 31 – Model-fit

Med SRMR-verdier på henholdsvis 0.070 og 0.079 kan det konkluderes med at modellen gir et godt samsvar mellom det observerte korrelasjonsmønsteret og mønsteret som følger av teorien som inkluderes i modellen.

6. Diskusjon

I dette kapittelet vil vi diskutere funnene opp mot hypotesene og tidligere litteratur. Studien har bygget en ny forskningsmodell vi ikke har sett i tidligere studier. Det ble funnet flere forklaringer både i tidligere forskningslitteratur og fra resultatene som kan forklare holdninger til bruk, og faktisk sikkerhetsatferd med mobile enheter.

Innledningsvis ble denne problemstillingen presentert:

> *Hvilke faktorer kan forklare ansattes bruk av sikkerhetstiltak på mobile enheter når de er ute på farten?*

Selv om informasjonssikkerhet på mobile enheter har blitt mye forsket på i tidligere IS-studier, har litteraturen vært dominert av et fokus på tekniske forhold der brukeren av løsningene i liten grad har blitt studert. Det har dermed vært spennende å bidra med aktuell forskning, sammenlikne resultater og følge med på utviklingen av forskningen innenfor dette feltet.

Diskusjonen videre deles inn i fem sentrale punkter:

- Oppsummering av studien med fokus på hvilke valg og utfordringer underveis
- Reliabilitet og validitet i studien
- Funn og svar på hypoteser
- Begrensinger med studien
- Implikasjoner for forskning og praksis

6.1. Oppsummering av studien

Studien begynte med en kort, men omfattende, systematisk litteraturstudie basert på Kitchenham (2004). Målet med litteraturstudien var å få innsikt i et lite utforsket og dermed relativt ukjent problemområde. Her ble det avdekket sentrale utfordringer samt løsninger med mobile enheter knyttet til brukeren, enheten og organisasjonen.

Under litteraturgjennomgangen var det planlagt å avholde intervjuer med sikkerhetseksperter på området. Generelt sett er informasjonssikkerhet et sensitivt område for virksomheter og krever involvering fra mange interne prosesser. Blant annet innebar dette godkjenning av flere nøkkelpersoner i hierarkiet.

Ettersom det tok svært lang tid for virksomheter å stille til intervju, ble det prioritert å fokusere på en omfattende litteraturstudie samtidig som man holdt dialogen gående med ulike virksomheter. Det endte med at sikkerhetstiltakene fra litteraturstudien ble kvalitativt kontrollert av sikkerhetseksperter via telefon og e-post. Dette var en viktig relevanssjekk som også tilførte detaljer til studien.

Rekruttering av respondenter var en kontinuerlig prosess gjennom hele studien. Man så hele tiden etter nye potensielle virksomheter og svarte på e-poster med spørsmål. Dette var mer tidskrevende enn først antatt. Det viste seg å være nærmest umulig, om ikke helt umulig, å kontakte respondenter direkte. Antakeligvis er dette et resultat av virksomheters gode innsats mot svindelforsøk. En ansatt er strengt opplært til å ikke svare eller klikke på lenker fra ukjente avsendere, noe som førte til at denne studien brukte et «toppen-og-ned» perspektiv for å rekruttere respondenter.

Det var 210 respondenter som svarte på studien, noe som er over kravet for å kunne gjøre en god PLS-SEM analyse. Verktøyet SmartPLS3 (Ringle et al., 2015), et intuitivt verktøy for å utføre PLS-SEM analyser, ble brukt for å kalkulere resultatene i studien. Studien rapporterte spennende resultater og totalt sett ble fem hypoteser støttet:

- Det er en positiv sammenheng mellom normer og holdninger til bruk av sikkerhetstiltak
- Det er en positiv sammenheng mellom oppfattet nytteverdi av sikkerhetstiltak og holdninger til bruk av sikkerhetstiltak
- Det er en positiv sammenheng mellom brukervennlighet av sikkerhetstiltak og holdninger til bruk av sikkerhetstiltak
- Det er en positiv sammenheng mellom holdninger til bruk av sikkerhetstiltak og faktisk sikkerhetsatferd
- Det er en positiv sammenheng mellom kvalitet på support og faktisk sikkerhetsatferd

6.2. Diskusjon av resultater

Denne studien gir et innblikk i hvordan ansatte i virksomheter forholder seg til informasjonssikkerhet, og slike studier er det få i av litteraturen (se **2.1.4 Datainnsamling og -analyse**). Begrepet «*ute på farten*» er et fenomen som ikke har fått mye oppmerksomhet i forskningen. Ettersom det stadig blir flere digitale nomader og ansatte som jobber der det måtte passe, vil det være rimelig å anta at begrepet snart kommer til å bli et populært forskningsemne. Det har derfor vært spennende å være noen av de første til å kaste lys over dette temaet og bidra til større innsikt i fenomenet.

For å strukturere funnene på en oversiktlig måte, er resultatene delt inn i underkapitler som representerer variablene i forskningsmodellen og blir diskutert individuelt.

6.2.1. Personlighetstrekk

Theory of Reasoned Action behandler personlighetstrekk som en ekstern effekt som kun kan påvirke atferd indirekte. Uttrykket *ekstern* ble brukt av Ajzen og Fishbein (1980) for å forklare muligheten for at andre eksterne faktorer kan påvirke forholdene i modellen. I vår studie antar vi at personlighetstrekk (FFM) påvirker holdninger til bruk av sikkerhetstiltak. FFM er ofte inkludert som en del av rekrutteringsfasen i virksomheter på grunnlag av at personlighetstrekk har direkte og indirekte sammenhenger med ytelse og andre jobbrelaterte atferder (Devaraj et al., 2008).

Analysen viste en nær signifikant (p mindre enn 0.1) stikoeffisient på 0.107 mot holdninger til bruk. Den positive korrelasjonen mellom personlighetstrekk og holdninger er i samsvar med studiens antakelser. Vanligvis er p større enn 0.05 ikke godtatt for å gi pålitelige funn, men det er imidlertid en mulighet for at personlighet kan påvirke holdninger til bruk allikevel. I utforskende studier, der det finnes lite eller ingen teori, argumenteres det for at p-verdier mindre enn 0.1 er godtatt. I denne studien var personlighetstrekk nær signifikant med to formative, signifikante indikatorer. Vektene av disse indikatorene viser at planmessighet og ekstroversjon bidro mest til at relasjonen ble signifikant.

Planmessighet er assosiert med indre motivasjon for å lykkes, være kunnskapsrik, stå for det en sier og være forsiktig. Forskning peker på dette personlighetstrekket som et av de viktigste innenfor informasjonssikkerhetsatferd. Planmessige personer har en tendens til å tenke fremover og er ekstra forsiktige når det kommer til informasjonssikkerhet (Uffen et al., 2013). Denne studien kan bekrefte at planmessighet bidrar mest til forholdet mellom personlighetstrekk og holdning til bruk av sikkerhetstiltak. Dette er et forventet resultat, ettersom personer med høye verdier av planmessighet er kjent for å ta mer ansvar (Uffen et al., 2013).

Personer som skårer høyt på ekstroversjon er karakterisert som muntre, energiske, ambisiøse og optimistiske. I tillegg liker de å utforske nye utfordringer og verdsetter mellommenneskelige forhold. Ekstroverte individer pleier å utføre det som er sett på som riktig atferd av andre. For eksempel vil ekstroverte individer bruke de sikkerhetstiltakene som er anbefalt og anerkjent av viktige nøkkelpersoner i virksomheten. I denne studien var ekstroversjon med på å gjøre forholdet mellom personlighetstrekk og holdninger til bruk signifikant. Tidligere forskningslitteratur har ikke fått støtte for dette.

Under pre-test av undersøkelsen kom det frem et poeng som er verdt å nevne. Det kan argumenteres for at svarene fra personlighetstrekkene ikke er helt nøyaktige. Mennesker liker å fremstille seg litt bedre enn de egentlig er, og dette kommer nok alltid til å være en begrensing i forskning, spesielt innen personlighetsforskning. I arbeidsmarkedet og generell jobbsøking er blitt vanlig å liste opp en del personlige egenskaper som ønskes for jobben. For eksempel blir disse egenskapene uttrykt som: *utadvendt, positiv, strukturert, nøyaktig* og *selvstendig.* Dersom man ser på BFI-10, instrumentet som ble brukt til å måle personlighetstrekk i studien, kan man forstå at det vil være fristende å gi seg selv litt høyere verdier. Man bør også tenke på i hvilken kontekst respondenten sitter i. Selv om undersøkelsen er anonym, har tross alt respondenten fått den tilsendt av sin overordnede. Hvem ønsker å oppgi at man er et ustrukturert menneske når det kommer til informasjonssikkerhet?

6.2.2. Normer

Analysen påviste en positiv sammenheng mellom normer og holdninger til bruk av sikkerhetstiltak. Normer er i denne studien uttrykt som hvilke forventninger en ansatt har til bruk av sikkerhetstiltak i virksomheten og fikk støtte med en signifikant ($p < 0.01$) stikoeffisient på 0.164 mot holdninger til bruk. For virksomheter er dette et fornuftig funn og illustrerer at ansatte mener det er viktig å følge etablerte sikkerhetsråd i virksomheten.

Sosial innflytelse har vært mye diskutert i IS-litteraturen. De fleste mennesker ønsker å oppføre seg i tråd med sosiale normer, enten det er i frykt om ikke å passe inn i den sosiale gruppen eller andre forhold. I undersøkelsen ble det spurt om viktigheten av å følge spesifikke sikkerhetsråd. At ansatte bestemmer seg for å følge sikkerhetsråd er tett knyttet til sikkerhetsretningslinjene og forventningene fra de rundt seg (Bulgurcu et al., 2010). Det å ikke følge etablerte sikkerhetsråd vil dermed tilsvare og bryte en norm i virksomheten. Dette er sjelden ønskelig.

Tidligere forskningslitteratur har studert sammenhengen mellom normer, intensjon og faktisk atferd. Sosial innflytelse har vist seg å påvirke sikkerhetsatferd i situasjoner der brukere ikke har tilgang til de formelle sikkerhetsmekanismene organisasjoner innfører (McGill & Thompson, 2017). McGill og Thompson (2017) foreslår at organisasjoner bør gi viktige nøkkelpersoner ansvaret for å fremme informasjonssikkerhet i virksomheten, fordi overordnede i større grad fremmer god sikkerhetsatferd hos en ansatt, enn kollegaer. Denne studien bekrefter at normer fra overordnede også påvirker holdninger til bruk.

Til tross for at relasjonen normer og holdninger til bruk ble støttet, var det kun normen «installere antivirusprogram» som fikk signifikant støtte i studien. Denne normen er dermed den som bidro mest til at relasjonen ble signifikant. Litteraturen skriver at skadevare og datalekkasjer ser ut til å være de mest fremtredende truslene mot brukere av mobile enheter. Skadelig programvare («*malware*») kommer i flere varianter og forsøker å skade eller gjøre enheten utilgjengelig. For eksempel kan skadelig programvare slette kritiske filer, tømme batteriet, forstyrre kommunikasjonen eller kryptere innholdet på enheten (Das & Khan, 2016)

En av mulig årsak for at antivirusprogramvare dominerer, er at tiltaket har fått mye oppmerksomhet i tidligere forskning, og at de andre sikkerhetstruslene ikke er like vanlig i utvalget. Tidligere ble skadelig programvare spredt gjennom e-post i nettleseren på en datamaskin, men i dag kan skadevare bli spredd gjennom mange flere kanaler enn tidligere og koster virksomheter mye penger (Shih et al., 2008). Antivirusprogrammer har lenge vært, og er, en løsning på mange personers og virksomheters bekymring mot skadevare (Thompson et al., 2017).

Mobile enheter tilbyr stadig større lagringskapasitet, og det har blitt vanlig å ta med privateide enheter på jobben. Bedre lagringskapasitet betyr også at det lagres flere personlige og forretningsmessige filer på enheten, noe som skaper et større skadeomfang for både brukeren og virksomheten (Mylonas et al., 2013). Man ser stadig flere vellykkede

phishingforsøk, og dette er svært gunstig for kriminelle som lever av datatyveri (Das & Khan, 2016).

Et godt og velment råd er å anbefale ansatte å styre unna e-poster og vedlegg fra ukjente avsendere. Dette rådet er dessverre ikke særlig realistisk i arbeidslivet. Mange mottar ofte henvendelser fra folk man ikke vet hvem er. I gode phishingforsøk vil en henvendelse kunne fremstå som å være fra en man kjenner, og innholdet i vedlegget kan også se helt legitimt ut. Dette er veldig vanskelig for brukeren.

6.2.3. Egenskaper med sikkerhetstiltak

For virksomheter er det svært viktig at deres ansatte bruker sikkerhetstiltak. I denne studien ble det brukt den velkjente «*Technology Acceptance Model*» (TAM) for å forklare sikkerhetstiltakenes påvirkningskraft mot holdninger til bruk. TAM er skreddersydd for å måle brukeraksept av IS og foreslår at personer med positive assosiasjoner til teknologi, også tar med seg disse assosiasjonene mot intensjonen om å bruke teknologien. I likhet med IS, kan oppfattelsen av suksess med et sikkerhetstiltak bli målt ved å studere nytteverdien og brukervennligheten av dem (Davis, 1989; Taylor & Todd, 1995). Mange tidligere studier har gitt støtte for TAM (se eksempler i Venkatesh et al. (2003)).

Oppfattet nytteverdi (PU) er definert som i hvilken grad brukeren føler at sikkerhetstiltaket vil øke sikkerheten på hans eller hennes enhet, og fikk støtte med en signifikant ($p < 0.001$) stikoeffisient på 0.378 mot holdninger til bruk, noe som er den sterkeste sammenhengen i studien.

Oppfattet brukervennlighet (EU) er definert som i hvilken grad en mobilbruker tror at å bruke sikkerhetstiltaket vil være enkelt eller uten problemer, og fikk også støtte med en signifikant ($p < 0.001$) stikoeffisient på 0.276 mot holdninger til bruk.

Dette forholdet illustrerer at det finnes en positiv sammenheng mellom sikkerhetstiltak som er godt formulert og er lett å bruke, og mot holdning til bruk. Virksomheter bør bruke denne kunnskapen til å utvikle sikkerhetsråd og -rutiner med gode egenskaper.

Dinev og Hu (2007) fikk ikke støtte for oppfattet nytteverdi mot holdninger i sin studie. Det kan argumenteres for at brukeren ønsket å bruke beskyttende teknologier (sikkerhetstiltak), ikke fordi han eller hun likte det, men fordi han eller hun mente det finnes en reell trussel. Hvis det var slik, er det klart at nytteverdi vil i mindre grad påvirke hans eller hennes holdninger til bruk.

Den originale TAM (Davis, 1989) hadde holdninger som en forklaringsfaktor for IT-bruk, men holdninger har i senere studier blitt eliminert (Venkatesh et al., 2003). Som et resultat av dette har de fleste TAM-studier hatt en direkte sti fra PU og EU til atferdsintensjoner (uten holdninger i mellom). Funnene fra denne studien illustrerer at TAM, slik som i «*Decomposed Theory of Planned Behavior*» (Taylor & Todd, 1995), kan bruke holdninger som en direkte påvirkning mot intensjon og faktisk atferd.

Noen respondenter kommenterte at det er vanskelig å vite om et sikkerhetsråd er ivaretatt godt nok. Det ble nevnt at man ofte måtte ta egne forholdsregler ute på farten fordi sikkerhetsrutinene enten var for dårlig kjent eller uklart formulert. Dette er et kjent dilemma i litteraturen. Renaud (2012) foreslår at virksomheten bør inkludere ansatte når regler og rutiner for informasjonssikkerhet blir laget. På denne måten kan ansatte føle at de blir verdsatt og bidrar selv til å øke virksomhetens informasjonssikkerhet. Dette vil også skape et mer forståelig regelverk for de ansatte, ettersom kompliserte ord og uttrykk blir formulert til noe alle kan forstå og sette seg inn i.

6.2.4. Holdninger

Ideen om at holdninger til bruk av sikkerhetstiltak påvirker faktisk bruk står sterkt i undersøkelsen. Generelt sett representerer holdninger et individ sin overordnede evaluering av en gitt atferd. I studiens kontekst gjenspeiler holdninger individets tro på at et sikkerhetstiltak er en fornuftig atferd som bidrar til å beskytte mot informasjonssikkerhetstrusler. Denne studien bekrefter at det finnes en positiv sammenheng mellom holdninger til bruk og faktisk bruk av sikkerhetstiltak med en signifikant ($p < 0.001$) stikoeffisient på 0.300.

Tidligere forskningslitteratur gjør et poeng av at holdninger må reflektere noe som har fått tid til å utvikle seg før man spør om dem. Informasjonssikkerhet er ofte påtvunget i form av sikkerhetsregler i virksomheten, utgjør ingen belønninger for den ansatte og er et tillegg i en allerede strevsom arbeidsdag. Det er dermed grunn til å tro at holdninger til informasjonssikkerhet er negativt.

Basert på svar og kommentarer, får studien en indikasjon på at de fleste har en god holdning til bruk av sikkerhetstiltak ute på farten. Tilbakemeldinger fra respondentene viser også at undersøkelsen bidro til at noen bestemte seg for å sette seg bedre inn i informasjonssikkerhetsretningslinjene i virksomheten. Dette er positivt. Resultatene viser at holdningene til bruk av sikkerhetstiltak blant ansatte i organisasjonen spiller en viktig rolle for faktisk bruk av tiltakene, noe som også er konsistent i tidligere studier (Dinev & Hu, 2007; Ifinedo, 2012; Ng & Rahim, 2005).

For virksomheter er dette et fornuftig funn og illustrerer at ansatte med gode holdninger til bruk av sikkerhetstiltak faktisk innfører dem i praksis. Virksomheter bør bruke denne kunnskapen til holdningsskapende arbeid, men det er viktig å merke seg at det kan finnes flere grupper i virksomheten med ulik oppfatning om informasjonssikkerhet (Da Veiga & Martins, 2017). Disse subkulturene kan ha ulik geografisk bakgrunn, etnisitet eller aldersgrupper, men deler det samme tankesett og normer. Hagen et al. (2011) foreslår å fremme den sikkerhetskulturen som viser størst interesse for informasjonssikkerhet. Dette kan skape en positiv effekt som fører til at andre subkulturer velger å følge etter og adoptere gode sikkerhetsholdninger i sine egne arbeidsoppgaver.

6.2.5. Kvalitet på support

IT-hjelp er en god støttespiller for ansatte i hverdagen. Det er viktig at ansatte får den hjelpen de trenger, enten det er i form av opplæring eller støtte underveis i arbeidsdagen. Denne studien fikk støtte for at det finnes en positiv sammenheng mellom kvaliteten på support i virksomheten og faktisk bruk av sikkerhetstiltak. Kvalitet på support er definert som hva virksomheten tilbyr av opplæring og tilrettelegging for sikkerhetstiltak, og analysen viste en signifikant ($p < 0.001$) stikoeffisient på 0.251 mot faktisk bruk.

Virksomheter bør bruke denne kunnskapen til å fokusere på å gjøre IT-hjelpen i virksomheten gode. Basert på tilbakemeldinger fra dette punktet er det to ting som er verdt å merke seg:

- Intern kontra ekstern IT-hjelp
- opplæringen av sikkerhetsrutiner

Det virker som ansatte har mindre til overs for ekstern IT-hjelp i virksomheten. Undersøkelsen tok ikke for seg forholdet mellom intern og ekstern IT-hjelp, men det kan tyde på at den eksterne IT-hjelpen hadde mindre kunnskap om virksomhetens sikkerhetsrutiner. Ekstern IT-hjelp kunne dermed ikke gi like gode tilbakemeldinger sammenliknet med intern IT-hjelp. Dette høres riktig og fornuftig ut, men studien har ikke tatt for seg litteratur som kan bekrefte eller avkrefte observasjonen.

Opplæring av ansatte ble også nevnt som et viktig poeng. Som en generell betraktning, ble det kommentert at det var uklart hva som måtte følges av sikkerhetsrutiner utenfor virksomheten. Innenfor virksomhetens rammer var det satt opp tekniske løsninger og diverse plakater med informasjonssikkerhetstips for å forhindre brukerfeil, men utenfor virksomheten er man helt for seg selv. Det ble også poengtert at nyansatte ikke fikk nok opplæring, og at det var nærmest umulig å huske noe som helst fra det ene sikkerhetskurset over lengre tid.

Litteraturen påpeker at organisasjoner bør passe på at ansatte får den tiden de trenger for å sette seg inn i og bli flinkere til sikkerhet. Det er ikke nok å utføre et opplæringskurs eller en sikkerhetskampanje. Det er viktig at det er en kontinuerlig prosess i virksomheten, slik at brukere kan vise sikker atferd og diskutere med hverandre (McGill & Thompson, 2017).

6.2.6. Oppfattet kontroll over sikkerhetsatferd

Variabelen «oppfattet kontroll over sikkerhetsatferd» mottok ikke empirisk støtte i denne studien, og det er et interessant funn i seg selv. Hypotesen ble tatt med fordi det ikke er sikkert at bruken av sikkerhetstiltak er frivillig for alle. Det kan hende at atferden er utenfor individets kontroll. For eksempel må man ofte registrere enheten i en «*Mobile Device Management*» (MDM) - løsning før man, i det hele tatt, får tilgang til å bruke enheten i en jobbsammenheng.

Flere respondenter i studien kommenterte at det var nærmest umulig å bryte eller suboptimere etterlevelsen av sikkerhetsrutiner grunnet strenge MDM-løsninger. Dersom man registrerer en mobil enhet i en MDM-løsning, gir man samtidig fra seg deler av kontrollen over enheten. MDM-løsninger installerer som oftest et sertifikat som gir virksomheten tilgang til blant annet posisjon og applikasjoner på enheten.

Basert på litteraturstudien, kom det frem flere argumenter som tyder på at ansatte ikke vil gi fra seg kontrollen over enheten (Bello et al., 2015; Hovav & Putri, 2016). Denne litteraturen samsvarer ikke med de resultatene som er gjort her. Tvert imot, basert på kommentarer og tilbakemeldinger, sitter studien igjen med inntrykket av at norske ansatte syntes det er helt greit å gi fra seg kontrollen over enheten. Om dette dreier seg om norsk feminin kultur eller andre forhold, har ikke studien noe grunnlag for å gå inn på.

6.3. Videre forskning

Studien har satt sammen forklaringer fra tidligere atferds- og personlighetsteorier for å deduktivt teste om de påvirker holdninger til bruk og faktisk bruk av sikkerhetstiltak utenfor virksomheten. Bruken av mobile enheter i ulike situasjoner og hvordan de håndterer sikkerhetstiltak er viktige faktorer med tanke på informasjonssikkerhet. Forskning på området har stort sett fokusert på tekniske og organisatoriske perspektiver, noe som øker aktualiteten for flere studier i retning den individuelle brukeren. Denne studien har bidratt til å belyse viktige faktorer knyttet til dette temaet.

Gjennom empirisk støtte, bekrefter studien at variabler fra kjente atferdsteorier (TPB, TAM, og D&M-ISSM) egner seg godt til å forklare atferd også innen informasjonssikkerhet når den ansatte befinner seg utenfor virksomheten. Funnene beskriver hvordan atferdsmessige kognitive faktorer kan påvirke brukerens holdninger til bruk, og faktisk bruk, av sikkerhetstiltak på mobile enheter ute på farten. Slike studier er fåtallige i tidligere IS-forskning, og denne studien bidrar med nyttig kunnskap til temaet.

En viktig implikasjon av funnene er at de reiser nye forskningsspørsmål utover det vi allerede vet. I en studie som analyserer holdninger til bruk og faktisk atferd er det umulig å dekke alle forklaringsfaktorer. Det kunne være nyttig å se etter andre faktorer som påvirker ansattes bruk av sikkerhetstiltak. En tilsvarende studie kan for eksempel legge til faktorer som ekspertise, motivasjon og tidligere erfaringer for å forklare holdninger til bruk og faktisk bruk av sikkerhetstiltak.

De ikke-signifikante variablene; kjennskap til sikkerhetstiltak (ISA), tro på egen mestringsevne (SE) og antatt kontroll over atferd (PBC) korrelerer ikke i henhold til tidligere studier. Studien har ikke grunnlag til å forklare hvorfor funnet er slik. En antakelse er at ulik bruk av MDM-løsninger blant respondentene har påvirket resultatene. Noen MDM-løsninger fjerner muligheten for ansatte å bryte eller suboptimere sikkerhetstiltak ute på farten. Dette kan føre til at ISA, SE og PBC får dårlig forklaringskraft. Videre forskning er nødvendig for å forstå hvorfor variablene i noen tilfeller øker sikkerhetsatferd og andre ganger ikke.

Vår studie bør følges opp av nye studier der det brukes andre fremgangsmåter. Et større utvalg av respondenter kunne inkludert et større spekter av brukere og flere forretningsområder. En annen vinkling kunne være å innføre tidsperspektivet i studien. Å utføre målinger over flere tidspunkt åpner for muligheten til å studere variansen i holdninger og faktisk atferd. For eksempel kunne man studert kontinuerlig bruk eller om atferden forandrer seg fra tidligere (og fremtidige) erfaringer.

Tidsperspektivet i en studie åpner også for nye studier mot personlighetstrekk. Selv om personligheten regnes som relativt stabil, vil den endre seg noe gjennom livet (Roberts & DelVecchio, 2000). Roberts og DelVecchio (2000) skriver at graden av åpenhet (kreativ og innovativ) minker ved økende alder. Dette er et interessant funn som kan ha implikasjoner for bruken av sikkerhetstiltak.

En interessant mulighet er å studere de enkelte sikkerhetstiltakene nærmere. I denne studien var det sikkerhetstiltaket «installere antivirus» som bidro mest til at relasjonen mellom normer og holdninger til bruk ble signifikant. Hvorfor er det slik? Hvordan bruker ansatte sikkerhetstiltak ute på farten? En ny fremgangsmåte kunne være å gjennomføre en eller flere casestudier. Da ville man fått en dypere forståelse for hvordan ansatte forholder seg til sikkerhetstiltak. En slik studie kunne for eksempel analysert utfordringer ved sikkerhetstiltak ute på farten.

Til slutt vil det være interessant å studere forskjeller mellom intern og ekstern IT-hjelp. Kommentarer fra studien informerer om flere interessante vinklinger. Bidrar intern kontra ekstern IT-hjelp til bedre faktisk bruk av sikkerhetstiltak ute på farten? Vil kontinuerlig opplæring av informasjonssikkerhet øke holdninger til bruk av sikkerhetstiltak ute på farten?

6.4. Praktiske implikasjoner

Studien belyser ulike faktorer som påvirker ansattes bruk av sikkerhetstiltak på mobile enheter når de er utenfor virksomheten (for eksempel ute på forretningsreise). Virksomheter som ønsker et høyere fokus på informasjonssikkerhet med mobile enheter bør være klar over følgende:

- Sikkerhetstiltaket *installere antivirusprogram* ga høyest prediksjonskraft i undersøkelsen. Studien viste at sikkerhetstiltakene utformet av virksomheten har en positiv sammenheng med holdninger til bruk. I praksis betyr dette at definerte sikkerhetsretningslinjer og -rutiner for informasjonssikkerhet ute på farten bidrar til å skape positive holdninger til bruk av sikkerhetstiltak.
  Studien viste at ansatte lytter til sine overordnede. Virksomheter kan bruke denne kunnskapen til å opplyse ansatte om at informasjonssikkerhet tas seriøst, og at de bør følge retningslinjene som finnes. Ansatte som mente det var viktig å følge retningslinjene for informasjonssikkerhet, viste også gode holdninger til bruk av sikkerhetstiltak ute på farten.

- Egenskaper ved sikkerhetstiltak påvirker holdninger til bruk positivt. Sikkerhetsretningslinjer og -rutiner som var tydelig definert og enkle å følge, bidro til at holdningene til bruk ble positive. Ansatte som forstod nytten av å følge sikkerhetsrutiner, viste også gode holdninger til bruk av sikkerhetstiltak. Det samme ble observert med ansatte som syntes det var enkelt å følge sikkerhetsrutinene. Virksomheter bør bruke denne kunnskapen til å lage tydelig definerte sikkerhetsrutiner som er enkelt for ansatte å følge ute på farten. Tiltakene bør være korte og konsise. Hvis mulig, involver ansatte dersom man utformer nye sikkerhetstiltak.

- Holdning til bruk av sikkerhetstiltak har en positiv sammenheng med faktisk sikkerhetsatferd. Undersøkelsen viste at ansatte med gode holdninger til å bruk av sikkerhetstiltak faktisk brukte sikkerhetstiltakene i praksis. Virksomheter bør fokusere på å skape en god sikkerhetskultur. Fokuser på en gruppe ansatte som viser gode sikkerhetsvaner. Denne oppmerksomheten kan være nok til å smitte over på andre grupper slik at de viser samme positive sikkerhetsoppførsel.

- Kvaliteten på IT-hjelp i virksomheten viste en positiv sammenheng til faktisk bruk av sikkerhetstiltak. Dette betyr at god IT-hjelp i virksomheten bidrar til at ansatte følger anbefalte retningslinjer når de er ute på farten. Virksomheter bør fokusere på god opplæring av brukerne og informere IT-hjelp om hvilke sikkerhetsrutiner som gjelder ute på farten. Opplæringen bør være atskilt fra hverdagslige oppgaver for å gi ansatte spillerom til å fullføre kurset i eget tempo. Ansatte glemmer fort, og kun et opplæringskurs eller en sikkerhetskampanje er ikke nok. Det er viktig at opplæring er en kontinuerlig prosess i virksomheten.

6.5. Begrensinger

Studien er underlagt noen begrensninger. Spesielt innen kvantitative studier er det vanskelig å vite om man har truffet målgruppen. Målgruppen for studien er personer som stadig jobber med mobil(e) enhet(er) utenfor virksomheten. Ettersom strategien for å rekruttere respondenter ble gjort med et toppen-og-ned perspektiv, er det spesielt vanskelig å vite hvem som faktisk har gjennomført undersøkelsen. En annen begrensning med en slik strategi er at respondentene har fått spørreskjemaet tilsendt fra sin overordnede. Det kan hende, selv om spørreundersøkelsen lover anonymitet, at respondenten har svart basert på hvordan han eller hun vil bli oppfattet i virksomheten, og ikke hvordan han eller hun faktisk oppfører seg.

Sikkerhetsatferden (faktisk bruk av sikkerhetstiltak) er selvrapportert. Dette er en generell begrensning i kvantitative studier, og det er derfor vanlig å rapportere intensjon om atferd. Denne studien argumenterer for at intensjon er såpass nærme faktisk atferd, og med hensyn til forenkling, ble bare faktisk atferd rapportert. Det er mulig å redusere denne begrensingen ved å ta i bruk scenarioteknikker (Bulgurcu et al., 2010). Scenarioteknikker gir respondentene omfattende informasjon om hypotetiske informasjonssikkerhetssituasjoner, og ved å spørre om disse situasjonene, kan forskere få dypere innsikt i respondentens sanne oppførsel.

Spørsmålene (indikatorene) anvendt i studien er oversatt fra engelsk til norsk. Selv om indikatorene viste god reliabilitet og validitet i tidligere forskning, kan det hende indikatorene tolkes annerledes på norsk.

Studien benyttet et kort instrument for å måle personlighetstrekk (BFI-10). Vanlige personlighetstester har ofte mange spørsmål som dekker forskjellige aspekter ved hvert personlighetstrekk. Denne studien brukte et instrument med kun to bipolare indikatorer per trekk. I forhold til kryssnasjonale forskjeller i personlighet, er det også sannsynlig at brukere av mobile enheter fra andre land har ulike holdninger til bruk og faktisk atferd. Resultatene fra personlighetstrekkene bør dermed leses med varsomhet.

De formative indikatorene ble ikke sjekket for konvergent validitet. Konvergent validitet for formative modeller krever at det gjennomføres en redundantanalyse. En slik analyse innebærer at variabelen har minst en generell refleksiv indikator, og det ble ikke tatt hensyn til dette i datainnsamlingen. Det gir ikke mening å ha et generelt spørsmål for de formative modellene i undersøkelsen. Eksempelvis er personlighetstrekk delt opp i fem unike dimensjoner (FFM), der hver dimensjon forteller noe viktig om deg som person. Å stille et generelt refleksivt spørsmål vil være nærmest umulig ettersom alle har personlighetstrekk, og det er det summen av dimensjonene som utgjør personlighetstrekket, ikke motsatt.

Utviklingen på forskningsfeltet går raskt. Litteraturstudien fokuserte på å identifisere de nyeste artiklene (flest artikler fra 2017). Etter litteratursøket var utvalget på 20 artikler. Dette var en håndterlig mengde artikler som var nok til å få en innsikt i problemområdet. Det ville vært interessant å se om resultatet hadde endret seg dersom utvalget var basert på en mer omfattende og gjennomgående litteraturstudie.

Sett tilbake på litteraturstudien, kan det virke som om studien fokuserte på smarttelefoner. Mobile enheter er en samlebetegnelse for alle typer håndholdte datamaskiner, noe som også betyr bærbare datamaskiner og nettbrett. Grunnen til at smarttelefoner ble overrepresentert, er nok fordi dette er blitt et populært forskningsemne den siste tiden. Ulike tiltak fra tiltakslisten ble revidert og fjernet for at det skulle passe med de fleste enheter. For eksempel er det ikke vanlig med organisatoriske regler og rutiner for USB-minnepinner eller skjermfilter på noe annet enn bærbare datamaskiner.

Rapporten har ikke tatt for seg bruken av smartklokker. Smartklokker er relativt nytt og ble ikke fanget opp i litteraturstudien. Det tar ofte en stund før artikler blir publisert. Ettersom artiklene i litteraturstudien var hentet fra fagfellevurderte journaler, der det kan ta opptil flere år å publisere, er det kanskje ikke så rart. Dersom litteraturstudien hadde brukt andre kilder, som for eksempel konferansebidrag, ville nok smartklokker vært representert. Smartklokker er på lik linje med andre mobile enheter potensielle sikkerhetstrusler for virksomheter.

En annen utfordring knyttet til en studie om informasjonssikkerhet var at utelukkende alle virksomheter måtte ta flere runder internt før de kunne svare hverken ja eller nei til deltakelse. I mange tilfeller måtte ledelsen i virksomheten studere og dele undersøkelsen internt før den kunne videresendes til ansatte. Noen virksomheter krevde også databehandleravtalen mellom Universitetet i Agder og Rambøll (SurveyXact), få forskerne bekreftet av en tredjepart på instituttet og/eller møte fysisk i virksomheten for å holde en presentasjon om studien eller signere taushetserklæring.

7. Konklusjon

Målet med denne studien har vært å forklare hvilke faktorer som påvirker holdninger til bruk og faktisk bruk av sikkerhetstiltak på mobile enheter utenfor organisatoriske rammer. Studien presenterer data fra en spørreundersøkelse med 210 respondenter som stadig jobber med mobil(e) enhet(er) ute på farten. Dataene ble analysert med Partial Least Squares Structural Equation Modelling (PLS-SEM).

Det er flere faktorer som påvirker holdninger til bruk. Ideen om at holdninger til bruk av sikkerhetstiltak påvirker faktisk bruk står sterkt i studien. Egenskaper med sikkerhetstiltak, delt opp i nytteverdi og brukervennlighet, viste begge positive sammenhenger mot holdninger til bruk. Dette funnet illustrerer at sikkerhetstiltak som er fornuftige og enkle å gjennomføre, bidrar til å skape gode holdninger til bruken av dem. Gode holdninger til bruk har også en signifikant positiv sammenheng med faktisk sikkerhetsatferd.

Studien fant også en signifikant positiv sammenheng mellom normer og holdninger til bruk. Det var sikkerhetstiltaket «installere antivirus» som bidro mest til at denne relasjonen ble signifikant. Funnet illustrerer at ansatte syntes det er viktig å følge anbefalte sikkerhetsråd, og at holdninger til bruk blir påvirket positivt av de normene (retningslinjene) ledelsen fremmer som viktige å innføre ute på farten.

Faktisk sikkerhetsatferd, uttrykt som selvrapportert bruk av sikkerhetstiltak, blir positivt påvirket av holdninger til bruk og kvaliteten på support i virksomheten. Dette funnet beskriver at gode holdninger til bruk av sikkerhetstiltak og god IT-hjelp i virksomheten bidrar til faktisk bruk av sikkerhetstiltak ute på farten.

Studien tok med personlighetstrekk for å se om «*Five-Factor Model*» (FFM) påvirket holdninger til bruk. Personlighetstrekk fikk ikke signifikant støtte i studien, men det var nært. Det var trekkene planmessighet og ekstroversjon som bidro mest til denne relasjonen.

Av praktiske implikasjoner fant man at ansatte lytter til sine overordnede. Ledelsen bør derfor informere sine ansatte om viktigheten av å bruke sikkerhetstiltak, også utenfor virksomheten. Det er viktig å utforme tydelig definerte sikkerhetsrutiner som er enkle for ansatte å følge når de er ute på farten. Tiltakene bør være enkle og konsise.

IT-hjelp er en god støttespiller for ansatte ute på farten og må ha nok kunnskap til å bistå ansatte med sikkerhetsrutiner i denne sammenhengen. Opplæring av ansatte bør være adskilt fra hverdagslige oppgaver og være en kontinuerlig prosess i virksomheten.

Referanser

Agudelo, C. A., Bosua, R., Ahmad, A. & Maynard, S. (2016). Understanding Knowledge Leakage & BYOD (Bring Your Own Device): A Mobile Worker Perspective. *arXiv preprint arXiv:1606.01450*.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211. doi: https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of applied social psychology, 32*(4), 665-683. doi: https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Ajzen, I. (2006). Constructing a Theory of Planned Behavior Questionnaire. Hentet 15.03.2018 fra https://www.researchgate.net/publication/235913732_Constructing_a_Theory_of_Planned_Behavior_Questionnaire

Ajzen, I. & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Englewood Cliffs, NJ: Prentice-Hall.

Al-Hadadi, M. & Al Shidhani, A. (2013). *Smartphone security awareness: Time to act.* Paper presentert på 2013 International Conference on Current Trends in Information Technology (CTIT).

Alsaleh, M., Alomar, N. & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *Plos One, 12*(3), e0173284. doi: https://doi.org/10.1371/journal.pone.0173284

Ashenden, D. & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security, 39*, 396-405. doi: https://doi.org/10.1016/j.cose.2013.09.004

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review, 84*(2), 191-215. doi: http://dx.doi.org/10.1037/0033-295X.84.2.191

Bandura, A. (1986). *Social foundations of thought and action: a social cognitive theory*. Englewood Cliffs, N.J: Prentice-Hall.

Bello, A. G., Armarego, J. & Murray, D. (2015). Bring your own device organizational information security and privacy. *ARPN Journal of Engineering and Applied Sciences, 10*(3), 1279-1287. doi: https://doi.org/10.1108/ICS-03-2016-0025

Bello, A. G., Murray, D. & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information and Computer Security, 25*(4), 475-492. doi: https://doi.org/10.1108/Ics-03-2016-0025

Block, J. (1995). A contrarian view of the five-factor approach to personality description. *Psychological bulletin, 117*(2), 187. doi: https://doi.org/10.1037/0033-2909.117.2.187

Bonne, B., Rovelo, G., Quax, P. & Lamotte, W. (2017). Insecure Network, Unknown Connection: Understanding Wi-Fi Privacy Assumptions of Mobile Device Users. *Information, 8*(3), 20. doi: https://doi.org/10.3390/info8030076

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *Mis Quarterly, 34*(3), 523-548. doi: http://www.jstor.org/stable/25750690

Burisch, M. (1984). Approaches to personality inventory construction: A comparison of merits. *American Psychologist, 39*(3), 214. doi: http://dx.doi.org/10.1037/0003-066X.39.3.214

Busch, P. A. & Moen, H. (2014). *Personlighetstrekk og ytelse i IT-supportteam* (Masteroppgave i Informasjonssystemer, Universitetet i Agder). Hentet fra http://hdl.handle.net/11250/224294

Cenfetelli, R. T. & Bassellier, G. (2009). Interpretation of Formative Measurement in Information Systems Research. *Mis Quarterly, 33*(4), 689-707. doi: https://doi.org/10.2307/20650323

Chin, E., Felt, A. P., Sekar, V. & Wagner, D. (2012). *Measuring user confidence in smartphone security and privacy.* Paper presentert på Proceedings of the Eighth Symposium on Usable Privacy and Security.

Coltman, T., Devinney, T. M., Midgley, D. F. & Venaik, S. (2008). Formative versus reflective measurement models: Two applications of formative measurement. *Journal of Business Research, 61*(12), 1250-1262. doi: https://doi.org/10.1016/j.jbusres.2008.01.013

Compeau, D. R. & Higgins, C. A. (1995). Application of social cognitive theory to training for computer skills. *Information systems research, 6*(2), 118-143. doi: https://doi.org/10.1287/isre.6.2.118

Costa Jr, P. T. & McCrae, R. R. (1992). Four ways five factors are basic. *Personality and individual differences, 13*(6), 653-665. doi: https://doi.org/10.1016/0191-8869(92)90236-I

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

Da Veiga, A. & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security, 70*, 72-94. doi: https://doi.org/10.1016/j.cose.2017.05.002

Das, A. & Khan, H. U. (2016). Security behaviors of smartphone users. *Information and Computer Security, 24*(1), 116-134. doi: https://doi.org/10.1108/Ics-04-2015-0018

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340. doi: https://doi.org/10.2307/249008

DeLone, W. H. & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research, 3*(1), 60-95. doi: https://doi.org/10.1287/isre.3.1.60

DeLone, W. H. & McLean, E. R. (2003). The DeLone and McLean model of information systems success: a ten-year update. *Journal of Management Information Systems, 19*(4), 9-30. doi: https://doi.org/10.1080/07421222.2003.11045748

Devaraj, S., Easley, R. F. & Crant, J. M. (2008). Research Note—How Does Personality Matter? Relating the Five-Factor Model to Technology Acceptance and Use. *Information Systems Research, 19*(1), 93-105. doi: https://doi.org/10.1287/isre.1070.0153

Dinev, T. & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 386. doi: https://doi.org/10.17705/1jais.00133

Eikebrokk, T. R., Iden, J., Olsen, D. H. & Opdahl, A. L. (2011). Understanding the determinants of business process modelling in organisations. *Business Process Management Journal, 17*(4), 639-662. doi: https://doi.org/10.1108/14637151111149465

Feldt, R., Torkar, R., Angelis, L. & Samuelsson, M. (2008). *Towards individualized software engineering: empirical studies should collect psychometrics.* Paper presentert på Proceedings of the 2008 international workshop on Cooperative and human aspects of software engineering.

Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention and behaviour: An introduction to theory and research* (Vol. 27). Reading, MA.: Addison-Wesley.

Freudenthaler, H. H., Spinath, B. & Neubauer, A. C. (2008). Predicting school achievement in boys and girls. *European journal of personality, 22*(3), 231-245. doi: https://doi.org/10.1002/per.678

Furnham, A. (1996). The big five versus the big four: the relationship between the Myers-Briggs Type Indicator (MBTI) and NEO-PI five factor model of personality. *Personality and Individual Differences, 21*(2), 303-307. doi: https://doi.org/10.1016/0191-8869(96)00033-5

Gkioulos, V., Wangen, G., Katsikas, S., Kavallieratos, G. & Kotzanikolaou, P. (2017). Security Awareness of the Digital Natives. *Information, 8*(2), 13. doi: https://doi.org/10.3390/info8020042

Goldberg, L. R. (1990). An alternative "description of personality": the big-five factor structure. *Journal of personality and social psychology, 59*(6), 1216. doi: https://doi.org/10.1037//0022-3514.59.6.1216

Goode, A. (2010). Managing mobile security: How are we doing? *Network Security, 2010*(2), 12-15. doi: https://doi.org/10.1016/S1353-4858(10)70025-8

Guido, G., Peluso, A. M., Capestro, M. & Miglietta, M. (2015). An Italian version of the 10-item Big Five Inventory: An application to hedonic and utilitarian shopping values. *Personality and Individual Differences, 76*, 135-140. doi: https://doi.org/10.1016/j.paid.2014.11.053

Hagen, J. M., Albrechtsen, E. & Johnsen, S. O. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security, 19*(3), 140-154. doi: https://doi.org/10.1108/09685221111153537

Hair, J., Hollingsworth, C. L., Randolph, A. B. & Chong, A. Y. L. (2017). An updated and expanded assessment of PLS-SEM in information systems research. *Industrial Management & Data Systems, 117*(3), 442-458. doi: https://doi.org/10.1108/IMDS-04-2016-0130

Hair Jr, J., Hult, G., Ringle, C. & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Los Angeles, California: Sage Publications Inc.

Hair Jr, J., Hult, G., Ringle, C. & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage Publications.

Hansen, M. K. (2018, 14.02.2018). Bevissthet. *I Store Norske Leksikon*. Hentet 01.03.2018 fra https://snl.no/bevissthet

Harris, J., Ives, B. & Junglas, I. (2012). IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. *Mis Quarterly Executive, 11*(3), 99-112. doi: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=79907364&site=ehost-live

Harris, M. A. & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97-114. doi: https://doi.org/10.1108/IMCS-03-2013-0019

Henseler, J., Ringle, C. M. & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135. doi: https://doi.org/10.1007/s11747-014-0403-8

Hogan, R., Hogan, J. & Roberts, B. W. (1996). Personality measurement and employment decisions: Questions and answers. *American psychologist, 51*(5), 469. doi: https://doi.org/10.1037/0003-066x.51.5.469

Hong, W., Thong, J. Y. L., Chasalow, L. C. & Dhillon, G. (2011). User Acceptance of Agile Information Systems: A Model and Empirical Test. *Journal of Management Information Systems, 28*(1), 235-272. doi: https://doi.org/10.2753/MIS0742-1222280108

Hovav, A. & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32*, 35-49. doi: https://doi.org/10.1016/j.pmcj.2016.06.007

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi: https://doi.org/10.1016/j.cose.2011.10.007

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode* (Vol. 3). Oslo: Cappelen Damm.

Jarvis, C. B., MacKenzie, S. B. & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of consumer research, 30*(2), 199-218. doi: https://doi.org/10.1086/376806

John, O. P., Donahue, E. M. & Kentle, R. L. (1991). The big five inventory—versions 4a and 54: Berkeley, CA: University of California, Berkeley, Institute of Personality and Social Research.

John, O. P. & Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement, and theoretical perspectives. *Handbook of personality: Theory and research, 2*(1999), 102-138.

Johnston, A. C. & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *Mis Quarterly, 34*(3), 549-566. doi: https://doi.org/10.2307/25750691

Judge, T. A. & Bono, J. E. (2000). Five-factor model of personality and transformational leadership. *Journal of applied psychology, 85*(5), 751. doi: https://doi.org/10.1037/0021-9010.85.5.751

Kakihara, M. & Sorensen, C. (2002, 7-10 Jan. 2002). *Mobility: an extended perspective.* Paper presentert på Proceedings of the 35th Annual Hawaii International Conference on System Sciences.

Karjalainen, M. & Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems, 12*(8), 518-555. doi: https://doi.org/10.17705/1jais.00274

Karwowski, M., Lebuda, I., Wisniewska, E. & Gralewski, J. (2013). Big Five Personality Traits as the Predictors of Creative Self-Efficacy and Creative Personal Identity: Does Gender Matter? *The Journal of Creative Behavior, 47*(3), 215-232. doi: https://doi.org/10.1002/jocb.32

Kildekompasset. (2016, 13.01.2016). Kildekritikk. *Kildekompasset*. Hentet 07.09.2017 fra http://kildekompasset.no/kildekritikk.aspx

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University, 33*(2004), 1-26. doi: https://doi.org/10.1.1.122.3308

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J. & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology, 51*(1), 7-15. doi: https://doi.org/10.1016/j.infsof.2008.09.009

Kitzrow, M. A. (2002). Applications of psychological type in clinical supervision. *The Clinical Supervisor, 20*(2), 133-146. doi: https://doi.org/10.1300/J001v20n02_11

Kristoffersen, L., Tufte, P. A. & Johannessen, A. (2011). *Forskningsmetode for økonomisk-administrative fag* (Vol. 3). Oslo: Abstrakt Forlag.

Küfner, A. C., Back, M. D., Nestler, S. & Egloff, B. (2010). Tell me a story and I will tell you who you are! Lens model analyses of personality and creative writing. *Journal of Research in Personality, 44*(4), 427-435. doi: https://doi.org/10.1016/j.jrp.2010.05.003

Lechner, C. M. & Rammstedt, B. (2015). Cognitive ability, acquiescence, and the structure of personality in a sample of older adults. *Psychological assessment, 27*(4), 1301. doi: http://dx.doi.org/10.1037/pas0000151

Loevinger, J. (1994). Has psychology lost its conscience? *Journal of Personality Assessment, 62*(1), 2-8. doi: https://doi.org/10.1207/s15327752jpa6201_1

Logan, P. Y. & Logan, S. W. (2003). Bitten by a bug: a case study in malware infection. *Journal of Information Systems Education, 14*(3), 301.

Maddux, J. E. & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479. doi: https://doi.org/10.1016/0022-1031(83)90023-9

Makimoto, T. (2013). The Age of the Digital Nomad: Impact of CMOS Innovation. *IEEE Solid-State Circuits Magazine, 5*(1), 40-47. doi: https://doi.org/10.1109/MSSC.2012.2231498

Makimoto, T. & Manners, D. (1997). *Digital Nomad*. Hoboken, NJ: Wiley.

Malmedal, B. & Røislien, H. E. (2016). *THE NORWEGIAN CYBER SECURITY CULTURE*. Hentet fra https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf.

Markelj, B. & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications, 20*, 84-89. doi: https://doi.org/10.1016/j.jisa.2014.11.001

McAdams, D. P. (1992). The five-factor model in personality: A critical appraisal. *Journal of personality, 60*(2), 329-361. doi: https://doi.org/10.1111/j.1467-6494.1992.tb00976.x

McCrae, R. R. & Costa, P. T. (1989). Reinterpreting the Myers-Briggs type indicator from the perspective of the five-factor model of personality. *Journal of personality, 57*(1), 17-40. doi: https://doi.org/10.1111/j.1467-6494.1989.tb00759.x

McCrae, R. R. & John, O. P. (1992). An introduction to the five-factor model and its applications. *Journal of personality, 60*(2), 175-215. doi: https://doi.org/10.1111/j.1467-6494.1992.tb00970.x

McDonald, S. & Edwards, H. M. (2007). Who should test whom? *Communications of the ACM, 50*(1), 66-71. doi: https://doi.org/10.1145/1188913.1188919

McGill, T. & Thompson, N. (2017). Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology, 36*(11), 1111-1124. doi: https://doi.org/10.1080/0144929X.2017.1352028

Myers, I. B., McCaulley, M. H., Quenk, N. L. & Hammer, A. L. (1998). *MBTI manual: A guide to the development and use of the Myers-Briggs Type Indicator* (Vol. 3): Consulting Psychologists Press Palo Alto, CA.

Mylonas, A., Kastania, A. & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security, 34*, 47-66. doi: https://doi.org/10.1016/j.cose.2012.11.004

Ng, B.-Y. & Rahim, M. (2005). A socio-behavioral study of home computer users' intention to practice security. *PACIS 2005 Proceedings*, 20. doi: http://aisel.aisnet.org/pacis2005/20

Ngoqo, B. & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security, 53*, 132-142. doi: https://doi.org/10.1016/j.cose.2015.05.011

NKOM. (2017). Nasjonal kommunikasjonsmyndighet. *Ekomstatistikken*. Hentet 15.02.18 fra https://ekomstatistikken.nkom.no/#/statistics/service?servicearea=Mobiltjenester

Nov, O. & Ye, C. (2008). *Personality and technology acceptance: Personal innovativeness in IT, openness and resistance to change.* Paper presentert på Hawaii International Conference on System Sciences, Proceedings of the 41st Annual.

Oates, B. J. (2006). *Researching Information Systems And Computing*. London: SAGE Publications Inc.

Orgeret, K. S. (2017, 21.03.2017). Kildekritikk. *I Store norske leksikon.* Hentet 07.09.2017 fra https://snl.no/kildekritikk

Pahnila, S., Siponen, M. & Mahmood, M. A. (2007). *Employees' behavior towards IS security policy compliance.* Paper presentert på 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 156b., Hawaii.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A. & Calic, D. (2015). *Factors that influence information security Behavior: An australian web-based study.* Paper presentert på International Conference on Human Aspects of Information Security, Privacy, and Trust.

Pavlou, P. A. & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS quarterly*, 115-143. doi: http://www.jstor.org/stable/25148720

Pett, M. A., Lackey, N. R. & Sullivan, J. J. (2003). *Making sense of factor analysis : the use of factor analysis for instrument development in health care research*. Thousand Oaks, Calif: Sage.

Pramod, D. & Raman, R. (2014). A study on the user perception and awareness of smartphone security. *International Journal of Applied Engineering Research, 9*(23), 19133-19144. doi: https://ssrn.com/abstract=2543737

Rammstedt, B. & John, O. P. (2007). Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German. *Journal of research in Personality, 41*(1), 203-212. doi: https://doi.org/10.1016/j.jrp.2006.02.001

Renaud, K. (2012). Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security and Privacy, 10*(3), 57-63. doi: https://doi.org/10.1109/MSP.2011.157

Ringle, C. M., Wende, S. & Becker, J. M. (2015). SmartPLS 3. Hentet fra www.smartpls.com
Roberts, B. W. & DelVecchio, W. F. (2000). The rank-order consistency of personality traits from childhood to old age: a quantitative review of longitudinal studies. *Psychol Bull, 126*(1), 3-25. doi: https://doi.org/10.1037/0033-2909.126.1.3
Robins, R. W., Trzesniewski, K. H., Tracy, J. L., Gosling, S. D. & Potter, J. (2002). Global self-esteem across the life span. *Psychology and aging, 17*(3), 423. doi: https://doi.org/10.1037//0882-7974.17.3.423
Rogers, E. M. (1983). *Diffusion of Innovations*. New York, NY: Free Press.
Rogers, R. W. (1975). A PROTECTION MOTIVATION THEORY OF FEAR APPEALS AND ATTITUDE CHANGE. *Journal of Psychology, 91*(1), 93. doi: https://doi.org/10.1080/00223980.1975.9915803
Rogers, R. W., Cacioppo, J. & Petty, R. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. New York: Guilford Press.
Rzadkowska, J. (2016). Carl Gustav Jung. *I Store Norske Leksikon*. Hentet 21.02.2018 fra https://snl.no/Carl_Gustav_Jung
Safa, N. S., Von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82. doi: https://doi.org/10.1016/j.cose.2015.10.006
Shih, D. H., Lin, B. S., Chiang, H. S. & Shih, M. H. (2008). Security aspects of mobile phone virus: a critical survey. *Industrial Management & Data Systems, 108*(3-4), 478-494. doi: https://doi.org/10.1108/02635570810868344
Shropshire, J., Warkentin, M. & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49*, 177-191. doi: https://doi.org/10.1016/j.cose.2015.01.002
Siponen, M., Mahmood, M. A. & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. doi: https://doi.org/10.1016/j.im.2013.08.006
Sommerfeldt, A. & Benjaminsen, T. A. (2017, 13.11.2017). Nomader. *I Store Norske Leksikon*. Hentet 17.01.2017 fra https://snl.no/nomader
Sommestad, T. & Hallberg, J. (2013). *A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance*, Berlin, Heidelberg.
Sommestad, T., Karlzén, H. & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy (IJISP), 9*(1), 26-46. doi: https://doi.org/10.4018/ijisp.2015010102
Språkrådet & Universitetet i Bergen. (2016). Mobilitet. I B. Kjelsvik & C. Ore (Red.), *Bokmålsordboka* (Revidert nettutgave 2016 utg.). Hentet fra http://ordbok.uib.no/perl/ordbok.cgi?OPP=mobilitet&ant_bokmaal=5&ant_nynorsk=5&bokmaal=+&ordbok=bokmaal
Store Norske Leksikon. (2017, 03.02.2017). Konformitet: psykologi. *I Store Norske Leksikon*. Hentet 13.03.2018 fra https://snl.no/konformitet_-_psykologi
Svendsen, G. B., Johnsen, J.-A. K., Almås-Sørensen, L. & Vittersø, J. (2013). Personality and technology acceptance: the influence of personality factors on the core constructs of the Technology Acceptance Model. *Behaviour & Information Technology, 32*(4), 323-334. doi: https://doi.org/10.1080/0144929x.2011.553740

Taylor, S. & Todd, P. A. (1995). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions. *International Journal of Research in Marketing, 12*(2), 137-155. doi: https://doi.org/10.1016/0167-8116(94)00019-k

Taylor, S. & Todd, P. A. (1995). Understanding Information Technology Usage - a Test of Competing Models. *Information Systems Research, 6*(2), 144-176. doi: https://doi.org/10.1287/isre.6.2.144

Teigen, K. H. (2016, 16.12.2016). Holdning. *I Store Norske Leksikon*. Hentet 27.02.2018 fra https://snl.no/holdning

Teigen, K. H. & Skre, I. B. (2016, 09.12.2016). Personlighetspsykologi. *I Store Norske Leksikon*. Hentet 13.03.2018 fra https://snl.no/personlighetspsykologi

Teigen, K. H. & Svartdal, F. (2016). Kognitiv Psykologi. *I Store Norske Leksikon*. Hentet 05.02.2018 fra https://snl.no/kognitiv_psykologi

Thompson, N., McGill, T. J. & Wang, X. Q. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security, 70*, 376-391. doi: https://doi.org/10.1016/j.cose.2017.07.003

Tu, Z. L., Turel, O., Yuan, Y. F. & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management, 52*(4), 506-517. doi: https://doi.org/10.1016/j.im.2015.03.002

Tupes, E. C. & Christal, R. E. (1992). Recurrent personality factors based on trait ratings. *Journal of personality, 60*(2), 225-251. doi: https://doi.org/10.1037/e531292008-001

Uffen, J., Kaemmerer, N. & Breitner, M. H. (2013). Personality Traits and Cognitive Determinants–An Empirical Investigation of the Use of Smartphone Security Measures. *Journal of Information Security 4 (2013), Nr. 4, 4*(4), 203-212. doi: http://dx.doi.org/10.4236/jis.2013.44023

Ulseth, T. (2012). Android. *I Store Norske Leksikon*. Hentet 19.02.2018 fra https://snl.no/Android

Ulseth, T., Abrahamsen, M. H. & Aleksandersen, D. (2017). iOS. *I Store Norske Leksikon*. Hentet 19.02.2018 fra https://snl.no/iOS

Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3-4), 190-198. doi: https://doi.org/10.1016/j.im.2012.04.002

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, 11*(4), 342-365. doi: https://doi.org/10.1287/isre.11.4.342.11872

Venkatesh, V. & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science, 46*(2), 186-204. doi: https://doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *Mis Quarterly, 27*(3), 425-478. doi: https://doi.org/10.2307/30036540

Warkentin, M., Johnston, A. C. & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267-284. doi: https://doi.org/10.1057/ejis.2010.72

Webster, J. & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii. doi: http://www.jstor.org/stable/4132319

Wong, K. K.-K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin, 24*(1), 1-32.

Zhang, X. J., Li, Z. & Deng, H. (2017). Information security behaviors of smartphone users in China: an empirical analysis. *The Electronic Library, 35*(6), 1177-1190. doi: https://doi.org/10.1108/EL-09-2016-0183

Zhao, H. & Seibert, S. E. (2006). The Big Five personality dimensions and entrepreneurial status: A meta-analytical review. *Journal of applied psychology, 91*(2), 259. doi: https://doi.org/10.1037/0021-9010.91.2.259

Vedlegg

Vedlegg A – Artiklene fra litteraturstudie

NR	Forfatter	Artikkel overskrift	Publisert	Journal
1	Alsaleh et al. (2017)	Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods	2017	PLOS One
2	Bello et al. (2015)	Bring your own device organizational information security and privacy	2015	ARPN Journal of Engineering and Applied Sciences
3	Bello et al. (2017)	A systematic approach to investigating how information security and privacy can be achieved in BYOD environments	2017	Information and Computer Security
4	Bonne et al. (2017)	Insecure Network, Unknown Connection: Understanding Wi-Fi Privacy Assumptions of Mobile Device Users	2017	Information
5	Das og Khan (2016)	Security behaviors of smartphone users	2016	Information and Computer Security
6	Gkioulos et al. (2017)	Security Awareness of the Digital Natives	2017	Information
7	Goode (2010)	Managing mobile security: How are we doing?	2010	Network Security
8	Harris og Patten (2014)	Mobile device security considerations for small- and medium-sized enterprise business mobility	2014	Information Management & Computer Security
9	Harris et al. (2012)	IT Consumerization: When Gadgets Turn Into Enterprise IT Tools	2012	Mis Quartley Executive
10	Hovav og Putri (2016)	This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy	2016	Pervasive and Mobile Computing
11	Markelj og Bernik (2015)	Safe use of mobile devices arises from knowing the threats.	2015	Journal of Information Security and Applications
12	McGill og Thompson (2017)	Old risks, new challenges: exploring differences in security between home computer and mobile device use	2017	Behaviour & Information Technology
13	Mylonas et al. (2013)	Delegate the smartphone user? Security awareness in smartphone platforms	2013	Computers & Security

14	Ngoqo og Flowerday (2015)	Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users	2015	Computers & Security
15	Pramod og Raman (2014)	A study on the user perception and awareness of smartphone security	2014	International Journal of Applied Engineering Research
16	Shih et al. (2008)	Security aspects of mobile phone virus: a critical survey	2008	Industrial Management & Data Systems
17	Thompson et al. (2017)	"Security begins at home": Determinants of home computer and mobile device security behavior	2017	Computers & Security
18	Tu et al. (2015)	Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination	2015	Information & Management
19	Uffen et al. (2013)	Personality Traits and Cognitive Determinants—An Empirical Investigation of the Use of Smartphone Security Measures	2013	Journal of Information Security
20	Zhang et al. (2017)	Information security behaviors of smartphone users in China: an empirical analysis	2017	The Electronic Library

Vedlegg B – Komplett konseptmatrise

Kategori		Alsaleh, Alomar & Alarifi (2017)	Bello, Armarego & Murray (2015)	Bello, Murray & Armarego (2017)	Bonne et al. (2017)	Das & Khan (2016)	Gkioulos et al. (2017)	Goode, A. (2010)	Harris Mark & Patten Karen (2014)	Harris, Ives & Junglas (2012)	Hovav & Putri (2016)	Markelj & Bernik(2015)	McGill & Thompson (2017)	Mylonas, Kastania & Gritzalis (2013)	Ngoqo & Flowerday (2015)	Pramod & Raman (2014)	Shih et al. (2008)	Thompson, McGill & Wang (2017)	Tu et al. (2015)	Uffen, Kaemmerer & Breitner (2013)	Zhang, Li & Deng (2017)
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Type studie	Kvantitativ				x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Kvalitativ	x	x	x	x					x											
Land	Skandinavia						x	x													
	Øvrige Europa				x		x	x		x		x		x						x	
	Afrika					x									x						
	Asia					x				x	x	x				x					x
	Australia		x	x														x			
	Nord-Amerika	x						x		x			x						x		
Ståsted	Leder / management		x					x	x	x											
	Ansatt	x	x	x					x	x	x	x						x	x		x
	Ekspert / Forsker							x											x		
	Hjemmebruker	x			x	x							x	x						x	
	Student	x					x				x				x	x					x
Kontekst	Privat	x	x	x	x	x	x	x	x	x	x	x	x	x	x			x			x
	Organisatorisk		x	x				x	x	x	x	x						x	x	x	x
Søketype	Databasesøk	x		x	x	x	x	x	x	x		x	x		x	x	x	x	x		
	Foroversøk		x																	x	x
	Bakoversøk										x			x							
Sikkerhetsrisikoer knyttet til	Bruker	x	x	x	x	x	x	x	x			x	x	x	x	x		x	x	x	x
	Enhet	x		x			x		x		x			x		x	x				x
	Organisasjon		x	x						x	x		x				x		x	x	
Tiltak for å minske risikoen	Opplæring og sikkerhetskampanjer		x	x		x					x	x	x		x					x	x
	Tekniske sikkerhetskontroller og -applikasjoner	x	x	x	x		x		x	x	x	x	x	x		x	x	x	x		x
	Organisatoriske regler og standarder		x	x	x	x		x	x	x	x						x				
	Kunnskapsdeling og samarbeid	x		x									x					x	x		
	Toppledelsens engasjement			x				x	x								x		x		

Vedlegg C – Spørreskjema

Undersøkelse av informasjonssikkerhet med mobile enheter

Hei og takk for at du deltar på denne undersøkelsen!

Undersøkelsen dreier seg om sikkerhet ved mobile enheter. Mobile enheter (smarttelefoner, nettbrett og laptoper) er en stor del av hverdagen til de fleste, og det er nå vanskelig å tenke seg en hverdag uten.

Du blir kontaktet fordi du forholder deg til en eller flere mobile enheter i forbindelse med jobben. Alle data i undersøkelsen blir behandlet anonymt, og ingen av dine svar kan spores tilbake til deg. Undersøkelsen er en del av en masterutredning ved Universitetet i Agder. Prosjektet avsluttes 4. juni 2018.

Dersom det er noe du lurer på, kan du kontakte oss på følgende måter:

Ole Reidar Holm
Tel: +47 975 643 85
E-post: olerh16@uia.no

Frode Mathias Bekkevik
Tel: +47 415 89 544
E-post: frodeb13@uia.no

Bakgrunnsinformasjon

Alder (Rund av til nærmeste heltall)

Ca. år _____

Kjønn

(1) ❑ Kvinne

(2) ❑ Mann

Anslå antall år utdanning etter grunnskole
Grunnskole er den 10-årige (tidl. 9 år) obligatoriske skolen for barn og ungdom i alderen 6-16 år.

Ca. år _____

Hvor lenge har du vært ansatt i virksomheten? (Rund av til nærmeste heltall)

Ca. år _____

Hvilke(n) mobil(e) enhet(er) bruker du i jobbsammenheng? (Velg en eller flere)

(1) ❑ Smarttelefon (iPhone, Samsung, Nexus, Huawei, med flere)

(2) ❑ Nettbrett (iPad, med flere)

(3) ❑ Bærbar datamaskin / laptop

(4) ❑ Annet _____

Bakgrunnsinformasjon

Hvor passende er disse påstandene som en beskrivelse av deg?

Jeg ser meg selv som ...

	Helt uenig	2	3	4	Helt enig
⋯ reservert	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
⋯ generelt tillitsfull	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
⋯ tendens til å være lat	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
⋯ avslappet og håndterer stress bra	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
⋯ lite kunstnerisk interesse	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
⋯ utadvendt og sosial	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
⋯ finner lett feil ved andre	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
⋯ gjør en godt gjennomført jobb	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
⋯ lett nervøs	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
⋯ har en livlig fantasi	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

Har din(e) mobil(e) enhet(er) blitt konfigurert for å fungere i virksomheten?

(1) ❑ Ja

(2) ❑ Nei

(3) ❑ Vet ikke

Har du tidligere blitt utsatt for en sikkerhetshendelse (privat eller på jobb)?

Eksempel på sikkerhetshendelser:
- mistet enheten
- blitt hacket
- identitetstyveri
- frastjålet informasjon
- kredittkortsvindel

(1) ❑ Ja

(2) ❑ Nei

(3) ❑ Vet ikke

Å følge sikkerhetsråd "ute på farten"

De neste spørsmålene dreier seg om å følge sikkerhetsrutiner når du er ute på farten. «På farten» handler om de gangene du bruker mobilen, nettbrettet eller laptopen utenfor virksomheten. Ta stilling til hva du selv gjør for å etterkomme behovene for IT-sikkerhet på mobile enheter i virksomheten.

Eksempler på situasjoner hvor du er på farten:
- Jobbe på kafé eller andre offentlige steder
- Ute på forretningsreise
- Sjekke e-post eller kalender på vei til jobb

Hvor viktig er det at du følger disse sikkerhetsrutinene ute på farten?

	Ikke viktig	**2**	**3**	**4**	**Svært viktig**	**Vet ikke / ikke relevant**
Ikke klikk på filer fra ukjente avsendere	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Ikke etterlat enheten uovervåket	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Ikke lån bort enheten til fremmede	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Ikke bruk samme passord flere steder	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Ikke koble til usikrede trådløse nettverk	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Ikke bruk ukjent eller uklarert utstyr (f.eks minnepenn)	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Ikke skriv ned eller lagre passord (f.eks på gule lapper)	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑

	Ikke viktig	2	3	4	Svært viktig	Vet ikke / ikke relevant
Ikke modifiser (endre) operativsystemet (Jailbreak / Rooting)	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Meld fra om sikkerhetshendelser eller mistanke om avvik	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Aktivere automatisk lås	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Installere antivirusprogram	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Aktivere fjernsletting & fjernsporing	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Ta jevnlig sikkerhetskopi	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Bruk VPN (Virtuelt Privat Nettverk)	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Pass på at internettrafikken er kryptert (HTTPS)	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Krypter informasjon på enheten	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Legg enheten i låsbart skap når den ikke brukes	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑
Skru av Bluetooth & WiFi når det ikke brukes	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑	(6) ❑

Ta stilling til følgende påstander om sikkerhetsrutiner i din virksomhet

	Helt uenig	2	3	4	Helt enig
Generelt sett er jeg godt kjent med virksomhetens sikkerhetsrutiner når jeg er ute på farten	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Jeg har satt meg godt inn i hvilke sikkerhetsrutiner som skal følges ute på farten	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Totalt sett, følger jeg anbefalte sikkerhetsrutiner ute på farten	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Jeg tenker mye på å holde den mobile enheten trygg ute på farten	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

Når det kommer til å følge sikkerhetsråd ute på farten ...

	Helt uenig	2	3	4	Helt enig
... er det opp til meg selv å bestemme om jeg skal følge anbefalte sikkerhetsrutiner	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

Ta stilling til følgende påstander om sikkerhetstiltak på farten:

	Helt uenig	2	3	4	Helt enig
Å følge anbefalte sikkerhetsråd når jeg er ute på farten bidrar til å holde virksomheten trygg	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Å følge anbefalte sikkerhetsråd når jeg er ute	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

	Helt uenig	2	3	4	Helt enig
på farten bidrar til å holde informasjon på enheten trygg					
Å følge anbefalte sikkerhetsråd når jeg er ute på farten har flere fordeler enn ulemper	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Jeg tror de fleste klarer å følge anbefalte sikkerhetsråd når de er ute på farten	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Det er enkelt å følge anbefalte sikkerhetsråd når man er ute på farten	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Sikkerhetsråd ute på farten er enkle å forstå	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

Når jeg er ute på farten ...

	Helt uenig	2	3	4	Helt enig
... har jeg de ferdighetene og kunnskapen som trengs for å følge anbefalte sikkerhetsråd	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... klarer jeg å følge anbefalte sikkerhetsrutiner uten hjelp fra andre	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... hjelper jeg andre med anbefalte sikkerhetsrutiner	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

Generelt sett, mener jeg sikkerhet på mobile enheter ute på farten er ...

	Helt uenig	2	3	4	Helt enig
... negativt	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... fornuftig	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... nyttig	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... tidskrevende	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

For meg, er det å følge virksomhetens retningslinjer for sikkerhet ute på farten ...

	Helt uenig	2	3	4	Helt enig
... negativt	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... fornuftig	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... nyttig	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... tidskrevende	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

For meg, vil det å koble seg til et åpent trådløst nettverk på café være ...

	Helt uenig	2	3	4	Helt enig
... negativt	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... fornuftig	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... nyttig	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... tidsbesparende	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

For meg, vil det å gå fra enheten ubevoktet være ...

	Helt uenig	2	3	4	Helt enig
... negativt	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... fornuftig	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... nyttig	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
... tidsbesparende	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

IT-hjelp i virksomheten

IT-hjelp er de personene i virksomheten man går til dersom man har behov for assistanse og hjelp med IKT-verktøy. Vennligst ta stilling til spørsmålene under.

Ta for deg følgende påstander om IT-hjelp i virksomheten

	Helt uenig	**2**	**3**	**4**	**Helt enig**
IT-hjelp har gitt meg god opplæring og trening i bruk av sikkerhetsrutiner	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
IT-hjelp gir rask bistand på sikkerhetsrutiner når jeg trenger det	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
IT-hjelp er lett tilgjengelige når jeg trenger assistanse med sikkerhetsrutiner	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Når jeg har et problem med en sikkerhetsrutine, viser IT-hjelp stor interesse for å løse problemet mitt	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

Har du noen kommentarer eller tilleggsopplysninger vedrørende undersøkelsen?

_____

_____

_____

_____

_____

Takk for innsatsen!
Dine svar er nå registrert. Du kan nå lukke dette vinduet ved å trykke avslutt nede i hjørnet.

Vennlig hilsen

Ole Reidar Holm
Tel: +47 975 643 85
E-post: olerh16@uia.no

Frode Mathias Bekkevik
Tel: +47 415 89 544
E-post: frodeb13@uia.no

Institutt for informasjonssystemer
Universitetet i Agder

Vedlegg D – Resultater fra PLS-analyse

Path Coefficients

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
ATT -> AB	0,300	0,302	0,075	4,000	0,000
EU -> ATT	0,276	0,243	0,066	4,215	0,000
ISA -> ATT	0,057	0,050	0,065	0,865	0,194
N -> ATT	0,164	0,255	0,069	2,389	0,008
P -> ATT	0,107	0,129	0,078	1,364	0,086
PBC -> AB	0,064	0,064	0,060	1,061	0,144
PU -> ATT	0,378	0,345	0,072	5,264	0,000
SE -> ATT	-0,050	-0,033	0,071	0,705	0,240
SQ -> AB	0,251	0,254	0,082	3,044	0,001

R Square

	R Square	R Square Adjusted
AB	0,197	0,185
ATT	0,478	0,463

f Square

	AB	ATT
AB		
ATT	0,092	
EU		0,099
ISA		**0,003**
N		0,030
P		**0,020**
PBC	**0,005**	
PU		**0,181**
SE		**0,003**
SQ	0,068	

Construct Reliability and Validity

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
AB	0,708	0,715	0,872	0,773
ATT	0,844	0,849	0,889	0,617
EU	0,816	0,816	0,891	0,732
ISA	0,890	0,893	0,948	0,901
N		1,000		
P		1,000		
PBC	1,000	1,000	1,000	1,000
PU	0,843	0,845	0,905	0,761
SE	0,791	0,832	0,879	0,711
SQ	0,914	0,919	0,940	0,796

Outer Loadings

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
ab_1 <- AB	0,895	0,893	0,025	35,221	0,000
ab_2 <- AB	0,864	0,862	0,033	26,085	0,000
att_fornuftig_1 <- ATT	0,750	0,751	0,046	16,187	0,000
att_fornuftig_2 <- ATT	0,830	0,832	0,037	22,242	0,000
att_nyttig_1 <- ATT	0,761	0,760	0,047	16,283	0,000
att_nyttig_2 <- ATT	0,858	0,856	0,031	27,496	0,000
att_positivt_r2 <- ATT	0,721	0,723	0,055	13,124	0,000
eu_1 <- EU	0,823	0,823	0,031	26,162	0,000
eu_2 <- EU	0,900	0,899	0,020	45,489	0,000
eu_3 <- EU	0,842	0,841	0,036	23,544	0,000
isa_1 <- ISA	0,946	0,945	0,015	64,596	0,000
isa_2 <- ISA	0,952	0,952	0,013	74,002	0,000
n_situasjon_1 -> N	0,237	0,210	0,119	1,990	0,023
n_situasjon_2 -> N	0,297	0,259	0,121	2,461	0,007
n_situasjon_3 -> N	0,384	0,330	0,129	2,984	0,001
n_situasjon_4 -> N	0,396	0,332	0,144	2,752	0,003
n_situasjon_5 -> N	0,334	0,281	0,141	2,366	0,009
n_situasjon_6 -> N	0,254	0,214	0,133	1,914	0,028
n_situasjon_7 -> N	0,306	0,266	0,116	2,634	0,004
n_situasjon_8 -> N	0,648	0,553	0,126	5,126	0,000
n_situasjon_9 -> N	0,522	0,443	0,137	3,797	0,000
n_teknisk_1 -> N	0,460	0,394	0,143	3,214	0,001
n_teknisk_2 -> N	0,761	0,657	0,100	7,579	0,000
n_teknisk_3 -> N	0,513	0,439	0,137	3,733	0,000
n_teknisk_4 -> N	0,462	0,396	0,132	3,504	0,000
n_teknisk_5 -> N	0,383	0,320	0,139	2,760	0,003

n_teknisk_6 -> N	0,460	0,386	0,133	3,450	0,000
n_teknisk_7 -> N	0,282	0,240	0,150	1,880	0,030
n_teknisk_8 -> N	0,434	0,371	0,118	3,664	0,000
n_teknisk_9 -> N	0,487	0,419	0,126	3,876	0,000
p_apenhet -> P	0,105	0,094	0,177	0,593	0,277
p_apenhet_r -> P	-0,130	-0,084	0,192	0,678	0,249
p_ekstroversjon -> P	0,445	0,363	0,198	2,253	0,012
p_ekstroversjon_r -> P	0,037	0,051	0,198	0,185	0,427
p_medgjorlig -> P	0,169	0,158	0,181	0,933	0,175
p_medgjorlig_r -> P	0,249	0,211	0,187	1,330	0,092
p_nevrotisme -> P	-0,117	-0,087	0,219	0,533	0,297
p_nevrotisme_r -> P	-0,396	-0,276	0,244	1,621	0,053
p_planmessighet -> P	0,210	0,178	0,185	1,137	0,128
p_planmessighet_r -> P	0,777	0,600	0,284	2,739	0,003
pbc_1 <- PBC	1,000	1,000	0,000		
pu_1 <- PU	0,902	0,900	0,024	37,309	0,000
pu_2 <- PU	0,908	0,906	0,023	40,297	0,000
pu_3 <- PU	0,803	0,804	0,038	21,329	0,000
se_1 <- SE	0,930	0,918	0,063	14,747	0,000
se_2 <- SE	0,871	0,855	0,090	9,698	0,000
se_3 <- SE	0,712	0,702	0,119	6,006	0,000
sq_1 <- SQ	0,837	0,837	0,028	29,804	0,000
sq_2 <- SQ	0,908	0,907	0,017	54,735	0,000
sq_3 <- SQ	0,923	0,920	0,019	49,859	0,000
sq_4 <- SQ	0,900	0,898	0,022	41,576	0,000

Outer Weights

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
ab_1 <- AB	0,602	0,601	0,051	11,730	0,000
ab_2 <- AB	0,534	0,535	0,051	10,411	0,000
att_fornuftig_1 <- ATT	0,236	0,236	0,021	11,032	0,000
att_fornuftig_2 <- ATT	0,260	0,261	0,022	11,720	0,000
att_nyttig_1 <- ATT	0,250	0,248	0,027	9,235	0,000
att_nyttig_2 <- ATT	0,285	0,283	0,024	11,665	0,000
att_positivt_r2 <- ATT	0,240	0,237	0,023	10,518	0,000
eu_1 <- EU	0,403	0,402	0,036	11,136	0,000
eu_2 <- EU	0,392	0,391	0,026	14,903	0,000
eu_3 <- EU	0,375	0,376	0,034	11,085	0,000
isa_1 <- ISA	0,510	0,509	0,045	11,297	0,000
isa2_2 <- ISA	0,543	0,544	0,045	12,097	0,000
n_situasjon_1 -> N	0,094	0,103	0,148	0,637	0,262
n_situasjon_2 -> N	-0,124	-0,086	0,202	0,613	0,270
n_situasjon_3 -> N	0,010	0,003	0,182	0,053	0,479

n_situasjon_4 -> N	0,150	0,115	0,188	0,799	0,212
n_situasjon_5 -> N	-0,053	-0,060	0,247	0,216	0,414
n_situasjon_6 -> N	-0,041	-0,055	0,184	0,223	0,412
n_situasjon_7 -> N	0,145	0,130	0,133	1,093	0,137
n_situasjon_8 -> N	0,297	0,265	0,334	0,889	0,187
n_situasjon_9 -> N	0,105	0,097	0,181	0,579	0,281
n_teknisk_1 -> N	0,185	0,161	0,225	0,821	0,206
n_teknisk_2 -> N	0,475	0,415	0,188	2,530	0,006
n_teknisk_3 -> N	0,107	0,097	0,247	0,434	0,332
n_teknisk_4 -> N	0,003	-0,001	0,241	0,014	0,494
n_teknisk_5 -> N	0,020	-0,017	0,247	0,080	0,468
n_teknisk_6 -> N	0,261	0,217	0,222	1,172	0,121
n_teknisk_7 -> N	-0,192	-0,136	0,538	0,357	0,360
n_teknisk_8 -> N	-0,096	-0,097	0,188	0,512	0,304
n_teknisk_9 -> N	0,243	0,221	0,178	1,369	0,086
p_apenhet -> P	0,198	0,155	0,181	1,096	0,137
p_apenhet_r -> P	-0,307	-0,229	0,222	1,380	0,084
p_ekstroversjon -> P	0,460	0,359	0,251	1,834	0,033
p_ekstroversjon_r -> P	-0,271	-0,198	0,260	1,044	0,148
p_medgjorlig -> P	0,107	0,105	0,189	0,564	0,286
p_medgjorlig_r -> P	0,059	0,063	0,198	0,297	0,383
p_nevrotisme -> P	0,289	0,221	0,262	1,105	0,135
p_nevrotisme_r -> P	-0,384	-0,251	0,274	1,403	0,080
p_planmessighet -> P	-0,087	-0,044	0,215	0,405	0,343
p_planmessighet_r -> P	0,787	0,601	0,312	2,521	0,006
pbc_1 <- PBC	1,000	1,000	0,000		
pu_1 <- PU	0,352	0,352	0,022	15,992	0,000
pu_2 <- PU	0,362	0,361	0,024	15,154	0,000
pu_3 <- PU	0,440	0,442	0,048	9,241	0,000
se_1 <- SE	0,473	0,474	0,111	4,262	0,000
se_2 <- SE	0,373	0,358	0,139	2,685	0,004
se_3 <- SE	0,330	0,325	0,154	2,142	0,016
sq_1 <- SQ	0,309	0,312	0,041	7,489	0,000
sq_2 <- SQ	0,277	0,277	0,029	9,421	0,000
sq_3 <- SQ	0,237	0,233	0,031	7,717	0,000
sq_4 <- SQ	0,301	0,303	0,033	9,174	0,000