Rapport

Kunnskapsgrunnlag om bevisstgjøringsstrategier som skal motvirke rekruttering av ubevisste innsidere i norske virksomheter

Forfattere:
Marte Høiby, Dorthea M. K. Vatn, Jannicke Fiskvik og Kristin Thaulow

Oppdragsgiver:
Sivil klareringsmyndighet

Rapport

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim
Sentralbord: 40005100
info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Kunnskapsgrunnlag om bevisstgjørings-strategier som skal motvirke rekruttering av ubevisste innsidere i norske virksomheter

VERSJON
0.1

DATO
2022-12-14

FORFATTER(E)
Marte Høiby
Dorthea Mathilde Kristin Vatn
Jannicke Fiskvik
Kristin Thaulow

OPPDRAGSGIVER(E)
Sivil klareringsmyndighet (SKM)

OPPDRAGSGIVERS REFERANSE
Kathinka Skott Hansen

PROSJEKTNUMMER
102028481

ANTALL SIDER OG VEDLEGG:
28+ Bilag/vedlegg

Overskrift sammendrag

Formålet med dette kunnskapsgrunnlaget er å belyse temaet bevisstgjøringsstrategier knyttet til informasjonssikkerhet og innsiderrisiko. På bakgrunn av en gjennomgang av eksisterende relevant forskningslitteratur innen sosialpsykologi, sikkerhetskultur og informasjonssikkerhet, fremstiller kunnskapsgrunnlaget noen modeller, konsepter og teorier knyttet til utfordringene med informasjonssikkerhet og innsiderrisiko. Videre fremlegges en diskusjon av ulike strategier og elementer i disse, samt anbefalinger for hva som kan være viktig å hensynta i arbeid med bevisstgjøring for den aktuelle problemstillingen.

UTARBEIDET AV
Marte Høiby

SIGNATUR
Marte H. Høiby
Marte H. Høiby (Dec 22, 2022 10:38 GMT+1)

GODKJENT AV
Anita Øren

SIGNATUR
Anita Øren
Anita Øren (Dec 22, 2022 10:39 GMT+1)

RAPPORT NR
2022:01518

GRADERING
Åpen

ISBN:
978-82-14-07977-7

Historikk

VERSJON	DATO	Versjonsbeskrivelse
0.1	2022-12-14	Første utkast
1.0	2022-12-21	Ferdig utkast

Innholdsfortegnelse

Forsidefoto: Shutterstock

1 Introduksjon

I stortingsmeldingen *Samfunnssikkerhet i en usikker verden* (Meld. St. 5 (2020-2021), 2020) trekker regjeringen frem et behov for å øke den forskningsbaserte kunnskapen om motvirkning av innsiderisiko. Alle årsrapportene til nasjonale sikkerhetsmyndigheter fra 2022 understreker innsiderrisiko som en økende bekymring, og et behov for å motvirke rekruttering av ubevisste innsidere (E-tjenesten, 2022; NSM, 2022; PST, 2022). Begrepet viser til at personer ikke er klar over sin egen sårbarhet, og at mennesker spiller en viktig rolle i en organisasjons informasjonssikkerhet (Glaspie & Karwowski, 2018).

Formålet med dette kunnskapsgrunnlaget er å belyse teamet bevisstgjøringsstrategier knyttet til informasjonssikkerhet og innsiderisiko. Dette gjøres gjennom en redegjørelse av teoretiske tilnærminger til bevisstgjøring og atferdspåvirkning i sosialpsykologien, litteratur på sikkerhetskultur og på informasjonssikkerhet, samt noen studier som har undersøkt metoder og effekter av holdnings- og bevisstgjøringskampanjer. Kunnskapsgrunnlaget bygger på to hoveddeler. Første del fremstiller eksisterende forskning om tilnærming og praksis for bevisstgjøringsstrategier knyttet til sikkerhet og informasjon. Mens del to, på bakgrunn av eksisterende litteratur, diskuterer vitenskapelige erfaringer fra ulike metoder som fremkommer i den utvalgte litteraturen, og oppsummerer noen anbefalinger for hva som kan være viktig å hensynta i utformingen av en bevisstgjøringsstrategi for ønsket resultat.

Med utgangspunkt i behov for et kunnskapsgrunnlag om ulike bevisstgjøringskampanjer med fokus på innsiderrisiko vil dette kunnskapsnotatet forsøke å besvare følgende forskningsspørsmål:

1) Hva sier litteraturen om bevisstgjøringsstrategier og effekt av disse?
2) Hvordan kan eksisterende kunnskap relateres til problemstillingen, og hva kan evt. overføres?
3) Hva mangler det kunnskap om, og hva bør undersøkes videre?

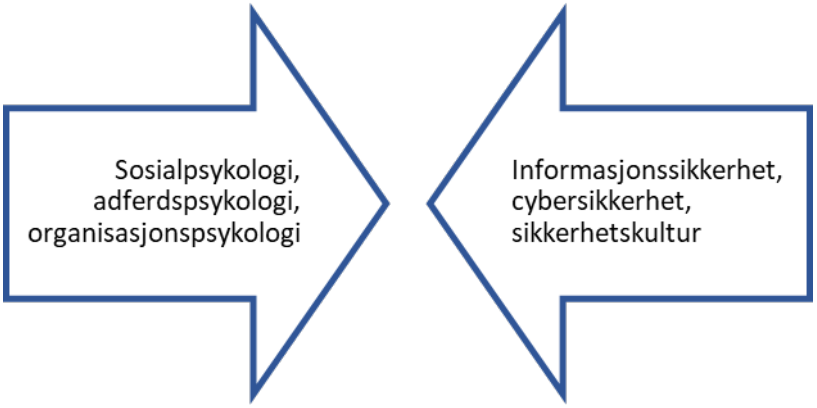
Selv om bevisstgjøringskampanjer kan anses som et eget forskningsfelt, er det i natur tverrfaglig og trekker på flere fagområder og teoretiske tradisjoner. Det er derfor hensiktsmessig å avgrense fokuset, og dette kunnskapsgrunnlaget ser på strategier for bevisstgjøring samt hvordan bevisstgjøring kan føre til handling.

1.1 Fra bevisstgjøring til atferdsendring: Fagområder og avgrensning

Forskningslitteraturen er opptatt av å skille mellom kunnskap, trening og utdanning (Tsohou et al., 2008). Det er en vei å gå fra bevisstgjøring til atferdsendring – så det er viktig å konkretisere hva som er ønsket å oppnå i praksis når en ser til litteraturen.

I dette kunnskapsgrunnlaget er vi interessert i å se på hvordan bevisstgjøring skal føre til handling, og hvordan både bevissthet og adferd kan vedvare over tid. Fordi utfordringen i dette tilfellet er knyttet til rekruttering av ubevisste innsidere, tar vi utgangspunkt både i sosialpsykologi og forskning på sikkerhetskultur og informasjonssikkerhet der de knytter seg til sosialpsykologien, og da spesielt bevisstgjøringsstrategier og atferdspåvirkning. Atferdspåvirkning brukes gjerne også for blant annet å løse politiske utfordringer innen helse, finans, miljø og klima, så her finnes flere relevante eksempler som ikke hovedsakelig handler om å beskytte informasjon, men i stedet hvordan informasjon kan påvirke menneskets forståelse og motivere til ønsket handling (som for eksempel å beskytte gradert informasjon).

Bevisstgjøringskampanjer med fokus på rekruttering av ubevisste innsidere trekker derfor på flere fagområder, og befinner seg i et krysningsfelt mellom psykologi på den ene siden, og sikkerhetskultur og informasjonssikkerhet på den andre, som vist i Figur 1.



Figur 1 Tverrfaglig krysningsfelt for bevisstgjøringskampanjer

1.2 Tilnærming og metode

Fordi vi her adresserer et tverrfaglig område tar tilnærmingen utgangspunkt i andre studier som har hatt som formål å samle og sammenstille kunnskap på feltet (Tsohou et al., 2008). Metoden benyttet er en litteraturstudie med bruk av to søkestrategier: databasesøk og snøballmetoden. I førstnevnte brukers sentrale nøkkelord og søkestrenger i databaser som har indeksert litteratur. Snøballmetoden baserer seg på å stadig identifisere nye relevante referanser underveis i litteraturgjennomgangen, inkludere disse og gjenta prosessen.

Samlet sett omfatter utvalget fagfellevurderte publikasjoner i internasjonale tidsskrift, konferanseartikler og akademiske bøker.

1.3 Oppbygning av rapporten

Kunnskapsgrunnlaget går systematisk gjennom bevisstgjøring og atferdsendring som resultat av påvirkning, og ser først på personlige faktorer, til kulturelle og deretter kontekstuelle faktorer. Kapittel 2 innleder med å redegjøre for sosialpsykologisk teori, sammenfatter sentral forskning og trekker frem relevante poenger for hvordan man kan utforme en bevisstgjøringskampanje slik at den blir mest mulig treffsikker. Med fokus på organisasjon, tar kapittel 3 for seg for litteratur på sikkerhetskultur, før kapittel 4 gir et overblikk over forskning på informasjonssikkerhet i organisasjoner og virksomheter. Kapittel 5 ser på kontekstuelle faktorer, altså hva som kan gjøres i miljøet rundt mennesker og kultur, for å påvirke måten en person eller en gruppe tenker, velger og handler. Kapittel 6 tar for seg empiriske studier som undersøker metoder og effekt av bevisstgjøringskampanjer, og presenterer funn fra noen utvalgte case-studier. Kapittel 7 konkluderer rapporten gjennom en diskusjon av hovedpunkter fra de øvrige kapitlene, samt en presentasjon av anbefalinger for videre arbeid med bevisstgjøringskampanjer med fokus på informasjonssikkerhet og innsiderisiko.

2 Et sosialpsykologisk perspektiv på bevisstgjøringsstrategier: fra holdning til handling

Sosialpsykologi er et bredt fagfelt som tar for seg studier av hvordan måten folks tanker, følelser og atferd er påvirket av det virkelige eller forestilte nærværet til andre mennesker (Aronson et al., 2014). I et sosialpsykologisk perspektiv er hele den sosiale situasjonen interessant, og et felt som får betydelig akademisk oppmerksomhet er sosial innflytelse. Sosialpsykologi har grensesnitt mot flere andre fagområder som sosiologi, økonomi og statsvitenskap. Det som likevel gjør sosialpsykologi til et unikt fagfelt er at analysenivået hovedsakelig er på *individet i konteksten av den sosiale situasjonen*, og ikke grupper eller institusjoner. Målet innenfor sosialpsykologien er å identifisere universelle egenskaper ved menneskelig natur som gjør oss mottakelig for sosial innflytelse (Aronson et al., 2014). Sosialpsykologi er et nyttig fagfelt å hente kunnskap fra i arbeidet med bevisstgjøringskampanjer fordi dette feltet har både teori og empiri som forteller noe om hvordan kunnskap, holdninger og atferd er forbundet. Ved å ta utgangspunkt i dette vil man kunne si noe *hvordan* man kan utforme en bevisstgjøringskampanje for at den skal være mest mulig treffsikker.

I et sosialpsykologisk perspektiv vil det være sentralt å ta utgangspunkt i menneskers holdninger for å vurdere nytten til ulike bevisstgjøringsstrategier. Dette fordi det ofte er ens holdninger som bestemmer hva vi gjør i ulike situasjoner. Holdninger blir i litteraturen enkelt definert som evalueringer av folk, objekter eller ideer (Ajzen & Fishbein, 2005), og skal en bevisstgjøringsstrategi ha nytte må den i et sosialpsykologisk perspektiv rette seg inn mot holdningene til enkeltindivider.

Det finnes ulike måter å kategorisere holdninger på. Aronson et al. (2014) skiller mellom holdninger som er kognitivt baserte, affektivt baserte eller atferdsbaserte. *Kognitivt* baserte holdninger er holdninger som er basert på konkrete og relevante fakta, for eksempel om et holdningsobjekt oppfyller sitt mål. Et eksempel kan være at man liker en viss type telefon fordi den har visse funksjonaliteter som andre telefoner ikke har. *Affektivt* baserte holdninger er de holdningene som er grunnlagt mer i følelser enn i en objektiv vurdering av hvorvidt et holdningsobjekt holder mål. En affektivt basert holdning kan komme fra mange ulike opphav, men til felles har disse holdningene at de ikke kommer av en rasjonell vurdering og dermed ikke er basert på logikk. Et eksempel på en affektivt basert holdning kan være at man ikke spiser kjøtt fordi det strider mot ens religiøse overbevisning. Det å skulle endre en affektivt basert holdning kan være utfordrende for den enkelte, fordi en holdningsendring ofte vil kreve at en også gjør verdiendringer. *Atferdsbaserte* holdninger stammer fra folks observasjoner av hvordan de oppfører seg mot et objekt. Et eksempel kan være at man trekker slutningen at man liker å trene fordi man gjør dette ofte. I tillegg til å skille mellom kognitivt baserte, affektivt baserte og atferdsbaserte holdninger er det vanlig å skille mellom implisitte og eksplisitte holdninger. De eksplisitte holdningene er de holdningene vi bevisst vedkjenner oss og lett kan fortelle om. De implisitte holdningene er de som er ufrivillige og ukontrollerbare, og som også ofte er ubevisste (Gawronski & Bodenhausen, 2007).

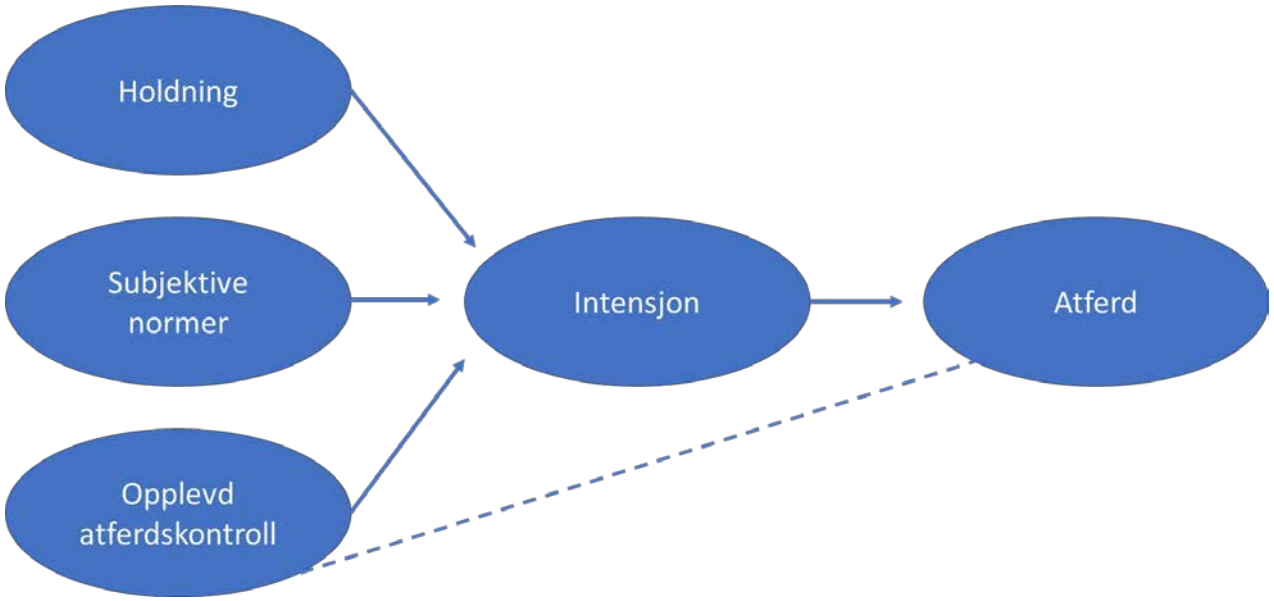
Interessen for holdninger innen sosialpsykologien stammer fra det at holdninger ofte rettleder hvilke handlinger en gjør. Holdninger endres ofte i møte med sosial innflytelse, og i forbindelse med bevisstgjøringsstrategier som skal motvirke rekruttering av ubevisste innsidere i norske virksomheter vil det være individers holdninger til sikkerhet som er de interessante å ta for seg. Skal man endre ansattes holdninger til sikkerhet, vil det være viktig å forstå det teoretiske grunnlaget bak holdninger og hvordan dette kan brukes inn i en bevisstgjøringskampanje. Det finnes en rekke teoretiske tilnærminger til holdninger innenfor sosialpsykologien, men det er likevel en sentral teoretisk tilnærming som skiller seg ut når det

kommer til å ta for seg den spesifikke sammenhengen mellom holdninger og atferd, nemlig Theory of Planned Behavior (TPB) (Ajzen, 2011).

2.1 Theory of Reasoned Action (TRA) og Theory of Planned Behavior (TPB)

Theory of Planned Behavior (TPB), på norsk oversatt til Teorien om planlagt atferd, er et teoretisk rammeverk utviklet av Ajzen og Fishbein på 1960-tallet (Ajzen, 2011). Bakgrunnen for utviklingen var at de ønsket å undersøke hvorfor forskningen på den tiden så ut til å indikere at verbale holdninger, altså holdninger som er uttalte, sjelden predikerer faktisk atferd. Løsningen ble å skille på *generelle holdninger* mot noe, og *spesifikke holdninger* mot å gjøre en bestemt atferd. Denne forskjellen ble oppsummert i den teoretiske tilnærmingen "Theory of Reasoned Action" (TRA), oversatt til Teorien om overveid handling, som regnes som forløperen til TPB. I følge TRA vil holdninger kun forutsi atferd når holdningen er knyttet til en spesifikk handling (f.eks. bli venn) og en bestemt målperson (f.eks. kollega i annen avdeling) innen en viss tidsramme (før jul). Til forskjell fra spesifikke holdninger, vil ikke en generell holdning på samme måte spesifisere bestemte handlinger, målpersoner eller tidsramme. Innen TRA knyttes spesifikke holdninger til atferd via intensjoner som er formet av en persons holdninger og subjektive normer. Subjektive normer vil vise til hvorvidt en atferd er sosialt akseptert.

Utgangspunktet til TRA var den atferden folk hadde frivillig kontroll over, men dette bidro til å begrense hvilken atferd man kunne ta for seg (Ajzen, 2011). Modellen ble derfor utviklet til å også ta for seg *grad av kontroll* et individ har over atferden. Ved å ta for seg dette ble modellen omdøpt til "Theory of Planned Behavior" (TPB), og i Figur 2 fremkommer TPB-modellen i sin helhet. I henhold til TPB vil graden av kontroll et individ har over atferden påvirke effekten intensjoner har på atferd. Folk vil bare handle på sine intensjoner i den grad de har informasjonen, intelligensen og evnene til å gjøre handlingen, samtidig som de kan komme forbi eventuelle ytre hindringer som kan stå i veien for handlingen. Holdninger, subjektive normer og opplevd atferdskontroll vil alle ha en sammenheng med hvilke atferdsintensjoner et individ har. Intensjonene vil videre ha en sammenheng med hvilken atferd et individ utviser, gitt at den opplevde atferdskontrollen er til stede.



Figur 2 De ulike elementene som inngår i TPB og hvordan de er forbundet

Det er gjort mange studier på TPB og det har blitt publisert metaanalyser som bidrar til å aggregere funnene fra mange enkeltstudier, og man finner da korrelasjoner på 0.59 til 0.66 mellom holdninger, subjektive normer og opplevd atferdskontroll på en side og intensjoner på den andre siden (Ajzen, 2011). Hvorvidt det er empirisk støtte for den teoretiske antakelsen om at individers opplevde atferdskontroll påvirker hvorvidt en intensjon blir til faktisk atferd er mer usikkert (Armitage & Conner, 2001).

Oppsummert gir TPB et teoretisk rammeverk for hvordan holdninger, intensjoner og atferd henger sammen, og i seksjon 2.3 vil det diskuteres hvordan man kan bruke dette teoretiske utgangspunktet inn i arbeidet med en bevisstgjøringskampanje.

2.2 The Protection Motivation Theory

Selv om det er noe usikkert hvorvidt en intensjon blir til faktisk atferd, så er forskningen likevel klar på at det er viktig for en bevisstgjøringskampanje at målgruppen forstår hva som står på spill, for at ønsket atferd skal være oppnåelig. Protection Motivation Theory (PMT) ble utviklet av Rogers i 1975 med mål om å bidra til oppklaring rundt hvordan mennesker reagerer på indusert frykt og tydelighet på et fagfelt som omfattet mange og sprikende teorier knyttet til bruk av frykt som appell i bevisstgjøring (Rogers, 1975). Beskyttelsesmotivasjonsteorien, som den kan oversettes til norsk, er ofte omtalt som teorien som best kan bidra til å forutse individers intensjon for trygg atferd. Den tar utgangspunkt i at mennesker responderer på frykt basert på en vurdering av trusselen (sannsynlighet for at den inntreffer og alvorlighetsgrad dersom den gjør det) og evne til å håndtere den. Dette vil bli adressert i følgende diskusjon om utforming av en bevisstgjøringskampanje.

2.3 Hvordan utforme en bevisstgjøringskampanje fra et sosialpsykologisk perspektiv

Fra sosialpsykologisk litteratur kan vi hente ut elementer som kan brukes i utformingen av en bevisstgjøringskampanje for å bidra til at den skal gi størst mulig effekt. Det er også et poeng å nevne at en slik kampanje kan følges opp med en mer langsiktig strategi for å styre bevissthet og atferd i ønsket retning.

Som skissert over, antyder litteraturen at bevisstgjøringskampanjer kan ha begrenset effekt alene, men at de er svært nyttige som element i en mer langsiktig strategi.

Målet med en bevisstgjøringskampanje vil være at ansatte får holdninger til sikkerhet som gjør at risikoen for innsiderekruttering blir minimal og at ansattes handlinger bidrar til at informasjonssikkerheten øker. I et sosialpsykologisk perspektiv vil det være viktig å fokusere på hvordan man kan påvirke holdningene til god sikkerhetsatferd, da dette sammen med den opplevde kontrollen ansatte har over sin atferd påvirker hvorvidt de vil danne atferdsintensjoner om å opptre på måter som ansees som gode i et sikkerhetsperspektiv. I følge Aronson et al. (2014) bør man i ethvert holdningsendringsprogram først avklare hvilken type holdning man ønsker å endre. I det at man ønsker å bruke bevisstgjøringsstrategier til å øke informasjonssikkerhet og minimere innsiderisiko ligger det at det er kognitivt baserte holdninger man ønsker å endre/videreutvikle. Gjennom bevisstgjøring er det da en tanke om at mer kunnskap vil gjøre at ansatte får holdninger som vil lede til atferd som er i tråd med opprettholdelsen av god informasjonssikkerhet. Videre vil derfor ulike strategier man kan bruke for å understøtte at bevisstgjøring vil bidra til den holdningsendringen man ønsker å oppnå presenteres.

Det er altså veien fra holdninger til atferd litteraturen innenfor sosialpsykologi i stor grad fokuserer på. En bevisstgjøringskampanje vil rette seg mot menneskers holdninger, og målet med en bevisstgjøringsstrategi vil være at individene former atferdsintensjoner som er i tråd med den ønskede atferden. Av TPB vil dette kunne skje dersom de riktige forutsetningene er til stede (sosiale normer og opplevd atferdskontroll).

2.3.1 Holdningsendring gjennom overbevisende kommunikasjon

Det er gjort mange studier som ser på hva som skal til for å overbevise mennesker til holdningsendring. Petty og Cacioppo (1986) har utviklet en modell kalt "Elaboration Likelihood Model of Persuasion" som sier noe om under hvilke betingelser mennesker påvirkes av det faktiske innholdet i kommunikasjonen de blir utsatt for, og under hvilke omstendigheter mer overfladiske aspekter spiller inn. Er temaet i den informasjonen folk blir utsatt for veldig personlig relevant for individet, vil argumentene som føres være viktig. Jo bedre argumenter, jo større sannsynlighet for at holdninger endres som følge av informasjonen menneskene får. Er det derimot slik at informasjonen folk blir utsatt for ikke oppleves som så veldig relevant personlig, vil overfladiske aspekter ved kommunikasjonen spille mer inn på hvorvidt folk endrer holdning (Petty et al., 1981). Overfladiske aspekter som har noe å si i en slik sammenheng kan for eksempel være *hvem* som formidler informasjonen (rolle, utseende) og *måten* det formidles på (lengden på en tale/notat etc.). Ettersom bevisstgjøringskampanjen retter seg mot ansatte med sikkerhetsklarering på tvers av sentrale virksomheter og organisasjoner er det grunn til å tenke at en bevisstgjøringskampanje som skal bidra til informasjonssikkerhet og redusert innsiderisiko oppleves som høyst personlig relevant. Det gjør at det *faglige innholdet* i bevisstgjøringskampanjen er viktig, og argumentene som fremmes må være logiske og gode. Det er også et viktig poeng at holdninger basert på en vurdering av innhold og argumentasjon, med større sannsynlighet beholdes over tid.

Selv om man kan anta at temaene informasjonssikkerhet og reduksjon av innsiderrisiko oppleves som personlige relevant for de fleste som er målgruppen for bevisstgjøringskampanjen, kan man anta at det alltid vil være noen som opplever innholdet som mindre personlig relevant. Derfor bør man ikke undervurdere mer trivielle aspekter for å øke treffsikkerheten til bevisstgjøringskampanjen. Dette vil handle om at man spiller på aspekter som at informasjonen er enkelt formidlet, at eventuelt materiell som utformes er estetisk pent og at de som eventuelt formidler informasjonen fremstår som troverdige. Utover hvorvidt

informasjonen i en bevisstgjøringskampanje oppleves som personlig relevant eller ikke, peker også forskning på at det personlighet kan spille inn på hvor motivert man er til å ta for seg argumentene i kommunikasjonen man blir utsatt for. I følge Petty et al. (2009) vil enkelte mennesker finne mer glede ved det å tenke nøye gjennom innholdet i argumentasjonsrekker de blir utsatt for fordi de skårer høyt på "need for cognition". De som skårer høyt liker å bruke tid på krevende kognitive aktiviteter (Aronson et al., 2014).

2.3.2 Holdningsendring gjennom å indusere frykt

Fear arousal er en strategi som spiller på bruk av frykt for ønsket effektoppnåelse (se f.eks. Rogers & Thistlethwaite, 1970). Det finnes en del ulike fryktmodeller, og Rogers (1983) utviklet Protection Motivation Theory (PMT) med mål om å bidra til oppklaring og tydelighet på dette feltet, som var preget av mange ulike teorier. Det finnes flere studier som har sett på betydningen av å spille på frykt i kampanjer, og et eksempel er den klassiske studien til Leventhal, Watts og Pegano (1967). Deltakerne i studien ble blant annet delt i tre grupper, der én gruppe skulle se en fryktinduserende film om konsekvensene av røyking, én gruppe skulle få en informasjonsbrosjyre om hvordan man kunne slutte å røyke, og én gruppe fikk både se den fryktinduserende filmen og informasjonsbrosjyren. Det de fant var at det var de som både fikk se filmen og fikk informasjonsbrosjyren som hadde den største nedgangen i antall sigaretter tre måneder etter eksperimentet.

Å spille på frykt kan virke enten veldig overtalende, eller kontraproduktivt (Ahluwalia, 2000). I følge Aronson et al. (2014) vil ikke ekstremt fryktinduserende kommunikasjon nødvendigvis bidra til at folks holdninger endres fordi folk overveldes og dermed ikke ønsker å forholde seg til det som kommuniseres. Ønsker man likevel å spille på frykten for visse konsekvenser i en bevisstgjøringskampanje er det viktig at det samtidig tilbys løsninger på hva som kan gjøres for å unngå de skremmende konsekvensene. I studien til Leventhal et al. (1967) så man at det var de som både ble utsatt for fryktinduserende informasjon og samtidig ble gitt verktøy for å gjøre noe var de som hadde sterkest effekt av den fryktinduserende informasjonen. Oversatt til en bevisstgjøringskampanje for å øke informasjonssikkerhet og redusere risikoen for innsiderrisiko er det viktig at individene får konkrete verktøy de kan bruke og råd de kan følge dersom man vektlegger alvorlige konsekvenser i det man kommuniserer. For eksempel kan dette være å gi konkrete råd som understreker viktigheten av å ikke innta mye alkohol som gjør at man kan havne i sårbare situasjoner i settinger der det man vet at det økt risiko for at infiltratører er til stede (f.eks. konferanser, reiser). Dette for å unngå at en infiltratør med dårlige hensikter kan få noe på en og bruke det til å presse en for informasjon.

Som en motpol til å bruke en bevisstgjøringskampanje til å indusere frykt, kan man også tenke at det å spille på positive følelser kan være en nyttig strategi i utformingen av en slik kampanje. Dersom vi er usikre på hva vår holdning rundt noe er, vil vi ofte bruke våre umiddelbare følelser som en mental snarvei (Clore & Huntsinger, 2007). I reklame for nye produkter vi ikke har et forhold til vil det være sentralt å få en til å føle seg vel, for da vil man kunne overføre disse positive følelsene til en positiv holdning til det nye produktet og slik øke sjansen for at vi kjøper det. Reklame som man utsettes for i settinger der man slapper av og hygger seg, er også forbundet med god effekt fordi man i en slik setting ikke mobiliserer "selvkontrollressursene" sine (Aronson et al., 2014). Hvordan dette konkret skal la seg oversette til en bevisstgjøringskampanje er ikke nødvendigvis helt rett fram, men det å bygge kampanjen inn i hyggelige sosiale sfærer på jobben kan være en mulig strategi.

2.3.3 Betydningen av å spille på sosiale normer

Det å minne folk på adekvate sosiale normer kan i mange tilfeller være en effektiv måte å oppnå atferdsendring på. Dette lar seg knytte til konstruktet "subjektive normer" i Theory of Planned Behavior (TPB) som er med å avgjøre hvorvidt en atferdsintensjon dannes (Ajzen, 2011). Normer kan inndeles i injunktive normer og deskriptive normer (Jacobson et al., 2011). Mens de injunktive normene sier noe om hvilken oppfattelse man har om hvorvidt en atferd er akseptert eller ikke av andre, vil de deskriptive normene handle om en oppfattelse av hvordan atferden faktisk er i virkeligheten. Et eksempel er at man vet at det ikke er greit å slippe inn andre gjennom inngangsdøren på jobb med sitt personlige nøkkelkort (injunktiv norm), men likevel er det en norm som gjør at dette er noe alle likevel gjør (deskriptiv norm). Forskning viser at det å minne folk på de gode injunktive normene er viktig for at den ønskede atferden skal utvises, og her vil trolig rollemodeller kunne spille en viktig rolle.

Som en del av bevisstgjøringsstrategien kan man knytte til seg enkeltpersoner på de ulike arbeidsplassene som kan få ansvar for å modellere de viktige injunktive normene som må følges, og slik sikre at de deskriptive normene ikke avviker fra disse. Drar man paralleller til forskning på forsøpling gjort av Reno et al. (1993) vil for eksempel det å se at en kollega nekter noen å bli med inn inngangsdør på sitt nøkkelkort, gjøre det lettere for andre å gjøre det samme selv. Det å spille på hva de fleste andre gjør er også en effektfull måte å påvirke atferden til mennesker. Goldstein et al. (2008) gjorde en studie der de undersøkte hvordan ulike formuleringer på hotellbad bidro til hvorvidt gjester valgte å gjenbruke håndkleet eller ikke. De så at det å understreke at 75% av gjestene valgte å gjenbruke håndklær på grunn av miljøet var mye mer effektfullt enn kun å understreke at gjenbruk av håndklær er et viktig miljøbidrag. Oversatt til en bevisstgjøringskampanje som skal bidra til informasjonssikkerhet kan man sørge for å innhente tall for andelen av ansatte som gjør en viktig positiv handling (f.eks. aldri slipper inn noen på sitt nøkkelkort), og formidle dette som en del av kampanjen.

2.3.4 Betydningen av å spille på kognitiv dissonans og konkurranse

En sentral drivkraft i ethvert menneske er behovet vi har for å opprettholde et positivt selvbilde, og dette er kjernen i Festingers (1957) konsept "kognitiv dissonans". Dette konseptet viser til den drivkraften vi har til alltid å opprettholde et godt og stabilt selvbilde, og kognitiv dissonans viser til ubehaget en kjenner på når man handler eller opptrer på måter som strider mot idealer vi egentlig har satt oss (Aronson et al., 2014). Som en del av en bevisstgjøringskampanje kan man for eksempel legge til rette for at de ansatte som er hovedmålet for kampanjen må formidle innholdet i kampanjen til andre i organisasjonene de er i, for slik skape en opplevelse av kognitiv dissonans dersom de selv begynner å avvike fra de retningslinjene de selv formidler.

Det å introdusere positive elementer av konkurranse kan også være et element i en bevisstgjøringsstrategi. For eksempel er det studier som har sett på hvordan man kan tilrettelegge for energieffektiv atferd på arbeidsplasser, og da har man funnet at det å få ulike avdelinger til å konkurrere om å ha lavest energibruk er mer effektivt enn å bare måle og formidle energibruken til den enkelte avdeling (Siero et al., 1996). I en bevisstgjøringsstrategi for å øke informasjonssikkerhet og redusere innsiderrisikoen kan man for eksempel identifisere konkret atferd eller konkrete rutiner som bør følges, finne måter å måle dette på, og formidle dette til alle. Skulle man ikke ønske å formidle åpent ulike avdelingers etterfølgelse av rutiner, er det også en viss effekt av at man på individnivå også legger til rette for en viss loggføring på hvor ofte man utfører en viktig atferd (Aronson et al., 2014).

2.3.5 Når leder bevisstgjøringsstrategier til *faktisk* ønsket atferd?

I henhold til Theory of Planned Behavior (TPB) vil en holdning bli til atferd under visse betingelser. For det første må det være sosiale normer som understøtter at holdningen blir til atferdsintensjon. Det betyr at det må være sosialt akseptert å utvise den ønskede atferden på arbeidsplassen og andre relevante arenaer. For det andre sier TPB at individer må ha informasjon, intelligens og evner til å utvise atferden. Målet med en bevisstgjøringsstrategi er at enkeltindivider utvikler holdninger som gjør at de opptrer på måter som bidrar til informasjonssikkerhet og unngår innsiderrekruttering. Skal en holdning bli til spontan atferd må holdningen være tilgjengelig for folk, og tilgjengelighet er noe som etableres med erfaring (Aronson et al., 2014). I dette perspektivet vil det være lurt å sikre at bevisstgjøringsstrategier for informasjonssikkerhet er noe ansatte jevnlig utsettes for. Dette peker mot at en enkeltstående kampanje ikke nødvendigvis er det man skal gå for, men heller mer en bevisstgjøringskampanje som pågår over tid.

Dersom en bevisstgjøringskampanje skal gå over tid, er det viktig ikke å bli for formanende i kommunikasjonen. Ifølge reaktansteorien til Jack Brehm utviklet på 1960-tallet vil forsøk på overtalelse kunne slå motsatt ut dersom folk opplever at sin frihet blir innskrenket (Rosenberg & Siegel, 2018). Kjernen i reaktansteorien handler om at når individer opplever at egen fri atferd trues, vil de gjøre det de kan for å beholde den. Teorien sier ikke at det er målet om mer frihet generelt som er motivasjonen, men heller frykten for å tape frihet man allerede har. I arbeidet med å øke informasjonssikkerhet og redusere innsiderrisiko er det derfor klokt å ha et bevisst forhold til hvorvidt ens tiltak endrer folks opplevelse av frihet. Dersom man blir veldig formanende i kommunikasjonen og setter i verk tiltak som gir en opplevelse av mindre frihet kan det ha motsatt effekt.

Ved å gå fra tanken om enkeltstående bevisstgjøringskampanjer til mer overordnede strategier som pågår over tid, peker man mot betydningen av sikkerhetskultur som blir presentert i det følgende.

3 Sikkerhetskultur

Mens sosialpsykologi i hovedsak fokuserer på enkeltindividet i den sosiale konteksten, vil sikkerhetskultur omfavne dynamikken i en organisasjon og hvordan individer fungere sammen i et kollektiv. Sikkerhetskultur anses vanligvis som en del av organisasjonskultur, også med tanke på at informasjonssikkerhet har blitt en viktig funksjon i organisasjoner (AlHogail & Mirza, 2014). Ofte knyttes forskning på organisasjonskultur til sosiologi, men det er et felt som trekker på mange fagområder og tradisjoner, med eksempelvis flytende overganger til psykologi. En formell og ofte gjengitt definisjon på organisasjonskultur kommer fra sosialpsykologen Edgar H. Schein som beskriver organisasjonskultur som

> a pattern of shared basic assumptions learned by a group as it solved its problems of external adaptation and internal integration, which has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems (Schein, 2010, p. 18).

Organisasjonskultur har i sentrale studier blitt brukt som en fortolkningsramme for å forstå en organisasjon (Bolman & Deal, 2017; Morgan, 1998), men disse har hatt mindre fokus på hvordan slik kultur oppstår og formes. Nyere studier legger vekt på at alt i en organisasjon, inkludert kultur, oppstår nedenfra-opp gjennom relasjoner og praksiser (Johannessen, 2022).

Som en del av en organisasjonskultur, retter sikkerhetskultur seg inn mot å øke bevisstheten om sikkerhet og hvordan sikkerhetssystemer i en organisasjon blir påvirket av holdninger og oppførsel til ansatte og eksisterende sikkerhetsretningslinjer (Malcolmson, 2009).[1] Som følge av en økende digitalisering av samfunnet hvor informasjon blir stadig viktigere, har forskningsfeltet videre fått et søkelys på informasjonssikkerhetskultur. Det finnes ingen omforent definisjon av informasjonssikkerhetskultur, men kan forstås som oppfatninger, holdninger, verdier og kunnskap om hvordan ting gjøres i en organisasjon for å følge opp nødvendige informasjonssikkerhetskrav med mål om å beskytte informasjonsverdier (AlHogail & Mirza, 2014).

En systematisk litteraturgjennomgang av forskning på informasjonssikkerhetskultur viser at mange studier og rammeverk bygger på Scheins modell for organisatorisk kultur (AlHogail & Mirza, 2014; Mahfuth et al., 2017). I sin teori om organisasjonskultur, opererer Schein med tre lag, (a) observerbare artefakter (f.eks. kleskode, fysiske omgivelser, talemåter) (b) verdier (f.eks. uskrevne regler og sentrale prinsipper), og (c) underliggende grunnleggende antakelser (f.eks. hvordan man definerer hva som er sant og virkelig) (Schein, 2010). Med utgangspunkt i Schein, har Van Niekerk og Von Solms (2010) i sitt rammeverk for informasjonssikkerhetskultur lagt til et fjerde lag til modellen, nemlig kunnskap. Her inngår nødvendig underliggende kunnskap relatert til informasjonssikkerhet. Et sentralt argument er at kunnskap er en viktig faktor i håndteringen av holdninger og oppfatninger blant ansatte når det gjelder samvirke med organisasjonsverdier, og dermed sentral i oppbygningen av en informasjonssikkerhetskultur.

Viktigheten av kunnskap underbygges også i studien til Gundu og Flowerday (2013). Deres modell illustrerer hvordan bevisstgjøringskampanjer om informasjonssikkerhet kan bygge kunnskap om informasjonssikkerhet og dermed påvirke atferd knyttet til informasjonssikkerhet, og skape sikkerhetskultur (Gundu & Flowerday, 2013, p. 77). Studien er gjort på ansatte i små og mellomstore bedrifter, og tar utgangspunkt i utilsiktet uønsket atferd fra såkalt uvitende ansatte.[2]

Et annet utgangspunkt i litteraturen er at den menneskelige faktoren ofte vurderes som det svakeste punktet i sikkerhetskjeden, hvor utfordringen med bevisste og ubevisste innsidere trekkes frem (Da Veiga & Eloff, 2010; Gundu & Flowerday, 2013). Dette igjen underbygger behovet for en god sikkerhetskultur i organisasjoner for å være beskyttet fra innsiden og påvirke ansattes oppførsel. På samme tid, fra et i utgangspunktet negativt fokus på mennesker i en organisasjon, understrekes den menneskelige faktor som noe positivt og en ressurs som kan forebygge og håndtere eventuelle sikkerhetsbrudd. I sum vil man med en god sikkerhetskultur kunne utgjøre en "menneskelig brannmur" (AlHogail & Mirza, 2014; Mahfuth et al., 2017).

Oppsummert kan det å bygge og vedlikeholde en sikkerhetskultur i en virksomhet være en mer langsiktig metode å beskytte virksomheten på enn mer avgrensede bevisstgjøringskampanjer. Kunnskap, trening, måling og tilpasning kan også fungere som elementer i å bygge en sikkerhetskultur. En sikkerhetskultur må

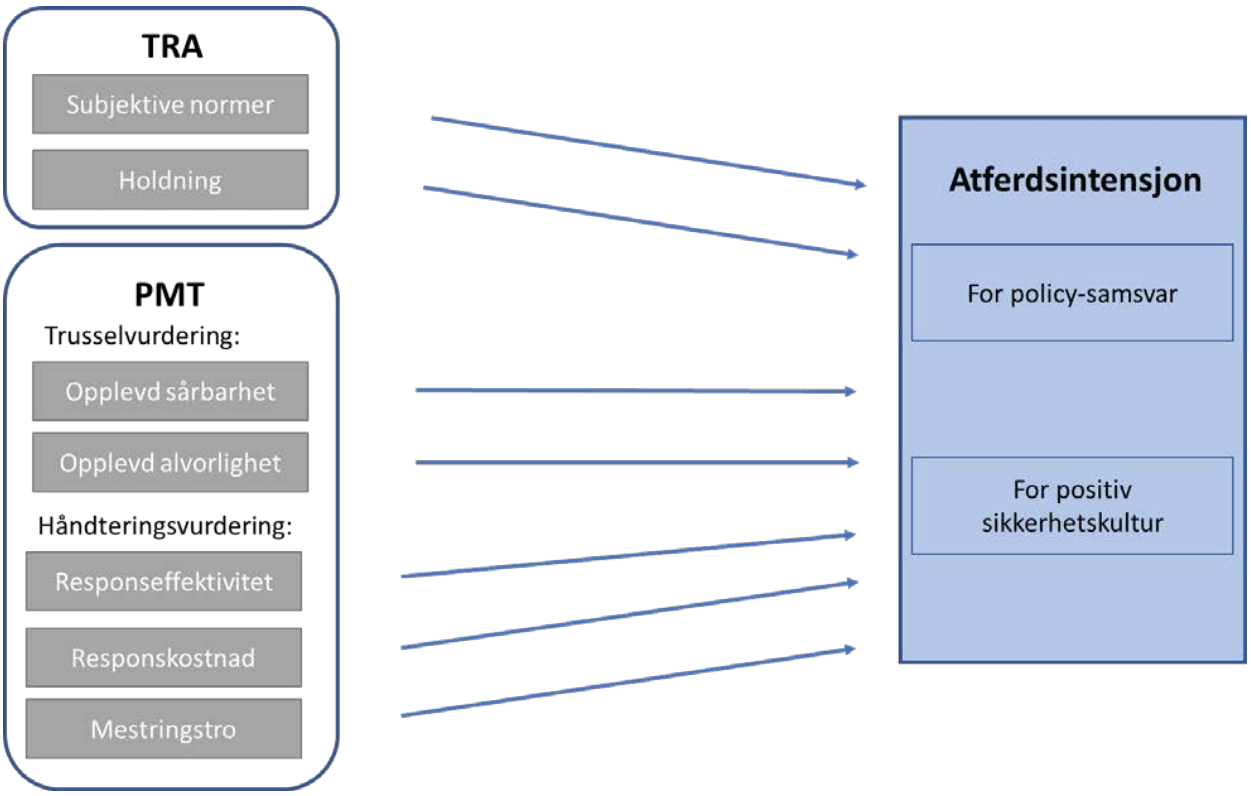
[1] Merk at det på engelsk skilles mellom *security* culture og *safety* culture, hvor sistnevnte ofte har et fokus på en harmonimodell for organisasjonslivet (se f.eks, Antonsen, 2017). Med sikkerhetskultur referer vi i denne rapporten til 'security culture'.

[2] Det bør tas høyde for at de ansatte i virksomhetene omfattet av studien på det tidspunktet den ble gjennomført generelt hadde mindre fokus på informasjonssikkerhet enn de ville hatt dersom studien ble gjennomført i dag med tanke på økende grad av digitalisering og fokus på temaet generelt i samfunnet siden 2013.

bygges og vedlikeholdes over tid, og bør gjerne aktualiseres gjennom konkrete hendelser hvor man vurderer hendelsen fra et sikkerhetskulturperspektiv. I et slikt perspektiv er det fokus på den menneskelige faktoren som en ressurs og dermed et positivt grunnlag for sikkerhetskulturbygging.

En kombinasjon av TRA (teorien om overveid handling) og PMT (beskyttelsesmotivasjonsteorien) som sikter mot sikkerhetssamsvar både på individnivå og kulturelt i virksomheten, kan være en god løsning. Gundu og Flowerday (2012) benytter en slik teoretisk tilnærming i sin studie, der de trekker på subjektive normer og holdninger fra TRA-teori, og trusselvurdering (threat appraisal) og vurdering av håndteringsevne (coping appraisal) fra PMT.

Modellen nedenfor illustrerer hvordan subjektive normer og holdninger hos ansatte i virksomheter kan påvirke motivasjon til å overholde virksomhetens sikkerhetspolicy, og at dette i kombinasjon med de ansattes egne oppfatninger (tro og kunnskap) om sårbarhets- og alvorlighetsgrad av trusler, samt vurderinger av egen evne og mulighet til å håndtere trusler, kan fungere i samspill for en sterkere intensjon for sikker atferd totalt. Vurderinger av evne til å håndtere trusler baserer seg på oppfatninger om effektivitet av respons, oppfatninger om kostnad av respons (i form av penger, tid og innsats) og oppfatninger om evne til å mestre. På denne måten foreslår Gundu og Flowerday at både samsvar med virksomheters sikkerhetspolicy og en sikkerhetskultur kan utvikles i samspill.



Figur 3 Modell gjenskapt fra Gundu og Flowerday (2012)

4 Informasjonssikkerhet

Informasjonssikkerhet er ofte vurdert som evnen til å håndtere risiko relatert til virksomheters informasjonsverdier og behandling av personopplysninger. I dette kunnskapsgrunnlaget er hensikten primært å belyse sikring av informasjonsverdier. Men det betyr ikke at det ikke finnes relevante metoder å se til der målet har vært å sikre personopplysninger, og litteratur som adresserer begge dilemmaer er derfor relevante å studere.

Med internettets utbredelse har både privat og offentlig sektor sett et raskt voksende behov for tilpasning med hensyn til informasjonssikkerhet (Regjeringen, 2019). Fremmedstatlig etterretningsaktivitet mot offentlig og privat virksomhet, inkludert data- og IKT-relatert kriminalitet, utgjør de fremste digitale truslene mot det norske samfunnet. Cybersikkerhet omfatter ikke bare informasjonssikkerhet, men også funksjonelle (f.eks. effektiviserende) teknologiske og ofte automatiserte systemer. Tingenes internett (på engelsk, Internet of Things/IoT) er et begrep som brukes for å omtale gjenstander utstyrt med elektronikk, programvare, sensorer og annet som gjør dem identifiserbare. Internett er i dag i alt fra leker til kjøkkenapparater og inngangsdører, og denne nye integrerte virkeligheten setter menneskene i en situasjon der informasjon blir mer tilgjengelig både for dem selv og for andre. Cybersikkerhet er et fagfelt som styrkes kraftig i både statlig og privat virksomhet, og det er en stadig etterspørsel etter ny kunnskap. Som følge av høy prioritet i anvendt forskning, har også studier innen cybersikkerhet økt i omfang og utgjør nå et empirisk grunnlag som kan være verdifullt å se til for kunnskap om informasjonssikkerhet. Dette empiriske grunnlaget kan fortelle noe om hvordan menneskelige faktorer agerer i samspill med teknologi – men også noe om hvilke vurderinger som ligger til grunn for menneskelig atferd relatert til informasjonssikkerhet og hvordan man kan innvirke på denne gjennom kontekstuelle og psykologiske virkemidler. Dette kunnskapsgrunnlaget har valgt å fremheve noe av litteraturen på dette feltet, samt å vurdere om det i noen grad kan være overførbart til informasjonssikkerhet også utenfor cyberdomenet – eller om disse virkelighetene i teknologisk avanserte samfunn er så integrert at det har mindre verdi å skille dem enn å behandle dem under ett.

Flere forskningsartikler har et overlappende fokus på informasjonssikkerhet i og utenfor cyberdomenet. I de mest digitaliserte samfunnene, som Norge er et eksempel på, blir gapet mellom det virtuelle liv og det virkelige liv stadig mindre. Dette kan føre til at forskningen på og i slike samfunn i mindre grad er opptatt av å skille mellom digitale og ikke-digitale kontekstuelle faktorer og årsaker innen samfunnsvitenskapen. Befolkningen lever i og med den digitale teknologien og kan helt enkelt ikke skilles fra den eller situasjonene den brukes i.

I litteraturen om informasjonssikkerhet og bevisstgjøringsstrategier brukes begreper som bevissthet, kunnskap og trening (awareness, education/learning, training) om hverandre. Noen omtaler disse som separate elementer i bevisstgjøringsstrategier, mens andre benytter dem mer integrert eller mindre bevisst (Tsohou et al., 2008). Den inkonsistente begrepsbruken er ifølge Tsohou et al.((2008) problematisk først og fremst fordi det forstyrrer bevissthet og dermed hindrer planmessighet rundt mål og effekt. Det er i litteraturen generelt uklart i hvilken grad bevissthet om informasjonssikkerhet er en prosess eller et produkt, og om det bør tilnærmes annerledes enn sikkerhetstrening og -utdanning (Tsohou et al., 2008, p. 223). En god prosess er ifølge forskerne uansett en som innlemmer utvikling, implementering og evaluering gjennomgående, og som vurderer utviklingen i henhold til mål.

Mennesket er altså sentralt i informasjonssikkerhet både i og utenfor cyberdomenet, og dette peker samtidig på sannsynligheten for at innsiderisiko også er forbundet med angrep i og utenfor cyberrommet. Innsiderisiko kan også ses på i et næringslivsperspektiv (Gundu & Flowerday, 2013); altså årsaker til at ansatte i en virksomhet kan lekke kritisk informasjon med eller uten intensjon om å gjøre det. Gundu og Flowerday (2013) påpeker at trusselen ved ikke-intensjonelle handlinger, altså feilgrep, blant ansatte ikke bør undervurderes i et helhetlig sikkerhetsperspektiv. Slike handlinger, som verken er forsøk på å diskreditere selskapet eller skaffe fortjeneste ved å selge konfidensiell data, er ofte resultat av utilfredsstillende opplæring og trening i informasjonssikkerhet, samt manglende sikkerhetsbevissthet og forståelse av konsekvenser av handlinger (Gundu & Flowerday, 2013, p. 69). Deres studie konkluderer med at omfanget av risiko knyttet til ubevisste handlinger kan reduseres betydelig ved hjelp av godt konstruerte bevisstgjøringskampanjer om informasjonssikkerhet.

5 Kognitiv vs. kontekstuell tilnærming

Når vi vurderer ulike strategier for hvordan å påvirke andres bevissthet og/eller atferd, har vi til nå sett på muligheter innen det kognitive – altså psykologiske tilnærminger som skal gjøre det lettere å påvirke menneskers motivasjon, holdning, valg og vaner – både på individ-nivå og gjennom kultur. I fagfeltet økonomisk psykologi omtales dette som den kognitive modellen (se f.eks. Dolan et al., 2012).

Men det er også mulig å påvirke for ønsket atferd gjennom tilrettelegging for respons på faktorer i omgivelsene (Dolan et al., 2012). Det er dette som omtales som kontekstuell tilnærming til atferdspåvirkning. Den kontekstuelle modellen, i motsetning til den kognitive, benytter seg av de ofte automatiserte prosessene som skjer ved vurdering og innflytelse, og måten mennesker responderer på omgivelsene. Denne modellen antar at mennesker ofte foretar irrasjonelle og inkonsistente valg og at disse kan påvirkes av kontekstuelle faktorer.

Gode rammebetingelser kan redusere forekomst av menneskelig svikt og kan konstrueres i teknologi, sikkerhetsmekanismer, rutiner og mer. Smart teknologi for automatiserte sikkerhetssystemer blir stadig mer utbredt og tilgjengelig for å sikre systemer, spesielt i urbane digitaliserte områder og såkalte smarte byer.

5.1 Atferdsøkonomisk perspektiv

Atferdsøkonomi er et krysningsfelt mellom psykologi og mikroøkonomi og tar utgangspunkt i at individet ikke alltid er rasjonelt, men motivert av egeninteresser og lønnsomhet i forhold til disse. I et atferdsøkonomisk perspektiv, flyttes altså fokuset fra menneskets indre motivasjon til dets muligheter av valg, valgenes tilgjengelighet og lønnsomhet. Og det er en økende enighet i atferdsvitenskapen at menneskers atferd er signifikant influert av faktorer knyttet til kontekst og situasjon (Dolan et al., 2012).

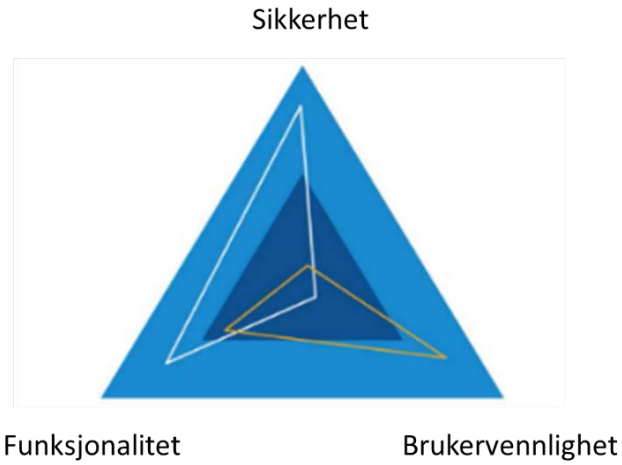
Som del av denne forskningen, har Dolan et al. (2012) utviklet MINDSPACE-modellen. MINDSPACE er et mnemisk akronym for ulike elementer som spiller inn på menneskers atferd som resultat av kontekstuell heller enn kognitiv innflytelse. Akronymet står for Messenger, Incentives, Norms, Defaults, Salience, Priming, Affect, Commitments og Ego. *Messenger* peker på at det betyr noe hvem som kommuniserer; *Insentiver* på at vi kan vurdere respons opp mot belønning; *Normer*, på at vi bryr oss om hva andre gjør og mener; *Defaults* på at vi er tilbøyelige for forhåndsinnstilte (ofte enkle eller tidsbesparende) alternativer; *Salience* på at budskapet må oppleves relevant for oss, *Priming* på fenomenet der små drypp av påvirkende informasjon til sammen kan ha en større innflytelse; *Affect* på at vi kan foreta valg basert på emosjoner; *Commitments* på at vi lett forplikter oss til det vi kjenner og har prøvd, og *Ego* på at vi gjerne foretar valg som får oss til å føle

oss bedre. Alle disse elementene av kontekstuelle faktorer der tilnærminger kan benyttes som verktøy for å styre menneskelig atferd. MINDSPACE ble i utgangspunktet utviklet for å bistå britiske myndigheter med et rammeverk som tilrettelegger for bruk av atferdsteori i utforming av offentlig politikk. Siden, har det vært benyttet i flere land og i både privat og offentlig sektor. Det kan være nyttig å se til som en kolleksjon av elementer som kan benyttes til å konstruere det kontekstuelle rommet og miljøet.

Utenfor cyberrommet, er utenforstående som vil skaffe seg ulovlig adgang eller tilgang til informasjon en særlig risiko for virksomheter som utvikler, oppbevarer eller har tilgang til gradert informasjon. Men det er ikke like lett å konstruere omgivelsene til ansatte når de ikke er på jobb eller på arbeidsgivers domene, digitalt eller fysisk. Å påvirke ansattes atferd utenfor det profesjonelle tid og rom vil derfor være en særskilt del av problemstillingen knyttet til innsiderisiko, og som andre arbeidsplasser ikke nødvendigvis har tilsvarende behov for å sette søkelys på. Det er likevel mulig å konstruere omgivelsene slik at de ansatte blir påminnet om viktigheten av å være varsom og til tider årvåken. Priming, som nevnt i MINDSPACE, eller forhåndspåvirkning, som det oversettes til norsk, kan for eksempel benyttes ved å trykke korte beskjeder eller bilder på kaffekopper på kontoret der de ansatte blir påminnet om at de også har et ansvar når de går hjem fra jobb eller befinner seg på fotball-cup med barna i helgen.

5.2 Sikkerhet og funksjonalitet

For å oppnå sikrere atferd, må det lønne seg å foreta valg som fører til økt sikkerhet. Men når man vil øke sikkerheten i virksomheter, har dette ofte vist seg å gå på bekostning av brukervennlighet og funksjonalitet. Triangelet for sikkerhet, funksjonalitet og brukervennlighet (Figur 4 under) viser hvordan forstyrrelser i forholdet mellom disse tre elementene kan føre til 'security fatigue'. Negative opplevelser knyttet til sikkerhet gjør at brukere vil sette spørsmålstegn ved om sikkerheten er så viktig likevel, og kan føre til at brukeren vil foreta valg som innebærer økt risiko. Tidsbesparelse, enklere gjennomføring eller kostnadsbesparelse kan være prioriteringer som kan gå på bekostning av sikkerhet. God balanse i forholdet mellom sikkerhet, funksjonalitet og brukervennlighet er derfor viktig, og enhver organisasjon bør balansere mellom disse tre egenskapene for å komme frem til et balansert informasjonssikkerhetssystem.



Figur 4 Triangelet for sikkerhet, funksjonalitet og brukervennlighet

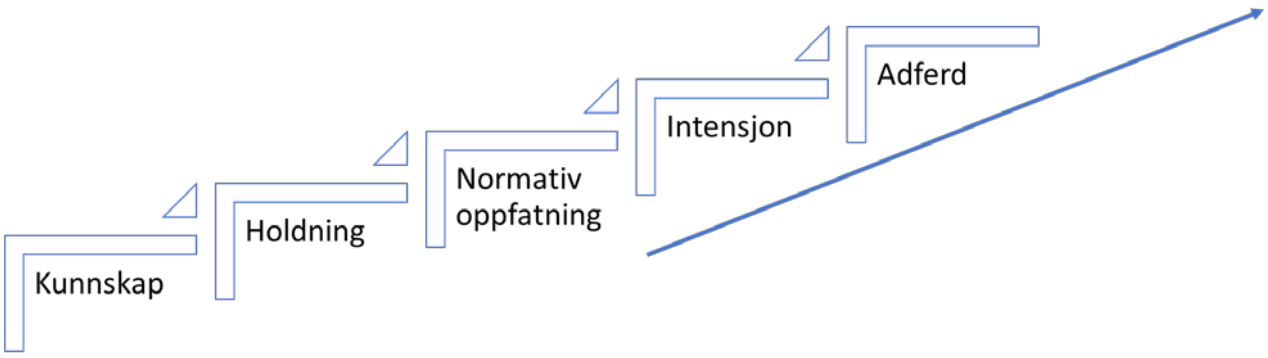
6 Empirisk grunnlag fra andre studier: Noen metoder og effekten av disse

Det finnes et økende antall studier som undersøker metoder og effekt av bevisstgjøringskampanjer. I dette kapittelet tar vi for oss slike case-studier fra litteraturen i utvalget, og oppsummerer noen av tilnærmingene og funnene som er gjort i nyere forskning. I dette kapittelet presenteres først noen erfaringer fra studier som retter seg mot informasjonssikkerhet generelt inkludert beskyttelse av kritisk informasjon i virksomheter, etterfulgt av funn fra case-studier innen cybersikkerhet.

6.1 Bevisstgjøring og informasjonssikkerhet

Metoder brukt i bevisstgjøringsarbeid er mange, og i løpet av det siste tiåret har flere digitale løsninger, som e-læring, gaming og e-kommunikasjon erstattet tradisjonelle klasseromsundervisningsvarianter og fysiske foredrag. Virtuelle teknologier, som XR (eXtended Reality – utvidet virkelighet med plattformer som VR og AR), er blitt mer avanserte og mer utbredt.

Men fremdeles benytter mange virksomheter tradisjonelle varianter. En studie måler effektiviteten av syv ulike metoder for bevisstgjøring om informasjonssikkerhet som er mye brukt i bevisstgjøringskampanjer (Khan et al., 2011). Metodene er presentasjoner, eposter, gruppediskusjoner, nyhetsbrev, videospill, databasert trening (Computer-based training, CBT) og posters. Forskerne kategoriserer effekt inn i fem ulike komponenter, og redegjør for hvilke effekter de ulike metodene eller verktøyene treffer. De fem effekt-komponentene strekker seg over en fem stegs stige som tegner prosessen fra kunnskap til atferd. Som vist i Figur 5 under, går de fem stegene fra kunnskap om informasjonssikkerhet på første trinn, til holdning til informasjonssikkerhet på andre, normative oppfatninger på tredje, intensjon på fjerde, og atferd knyttet til informasjonssikkerhet på femte og øverste trinn.



Figur 5 Femstegsmodell for måling av sikkerhetsbevissthet (Khan et al., 2011)

Metodene ble altså vurdert etter hvorvidt de tilfredsstiller de fem komponentene i prosessen fra kunnskap til endret atferd (se Tabell 1). Mest effektivt var gruppediskusjon, som tilfredsstiller alle fem komponenter i stigen. Presentasjon/foredrag tilfredsstiller fire av fem, og alle utenom komponenten om å innvirke på subjektive normer. E-post-meldinger tilfredsstiller tre av de fem, og alle utenom påvirkning på subjektive normer og atferd. Resten tilfredsstiller kun to av fem komponenter, og blant disse treffer både nyhetsbrev og posters i å påvirke kunnskap og holdninger, mens videospill påvirker holdninger og intensjoner, og CBT påvirker subjektive normer og atferd.

Tabell 1 Effekt av ulike metoder for økt bevissthet om informasjonssikkerhet (Khan et al., 2011)

1	Metode	Kunnskap	Holdnings-endring	Subjektive normer	Intensjon	Atferds-endring	Effekt-oppnåelse
2	Presentasjoner	v	v	x	v	v	4
3	Epost-meldinger	v	v	x	v	x	3
4	Gruppediskusjon	v	v	v	v	v	5
5	Nyhetsbrev	v	v	x	x	x	2
6	Videospill	x	v	x	v	x	2
7	Databasert trening	v	v	x	x	x	2
8	Posters	v	v	x	x	x	2

En case-studie av informasjonssikkerhetstrening i bedrifter ser på effekten av kombinerte tilnærminger ved informasjonssikkerhetslæring (Eminağaoğlu et al., 2009). I studien gis 2900 ansatte i et selskap opplæring i informasjonssikkerhet, blant annet i bruk av passord, i tillegg til at de eksponeres for komplementært bevisstgjøringsmateriell som pedagogiske plakater, animasjoner og innlegg på selskapets intranett, spørreundersøkelser og enkle nettquizer. Dette ble gjennomført i en 12-måneders periode, og de ansatte måtte endre passord tre ganger i løpet av perioden. Målinger av sikkerhetsbevissthet ble foretatt ved hvert intervall, samt gjennomgående i perioden. Resultatene ble sammenlignet og statistisk analysert, og viser at bevisstgjøringskampanjen hadde en ønsket virkning på de ansatte. Blant annet oppnådde de betydelig reduksjon i bruk av svake passord blant de ansatte og økt bevissthet både ved valg og bruk av disse. I tillegg begynte ansatte å delta mer aktivt i sikkerhetskontroller og -mekanismer de ble eksponert for i kampanjen, og forholde seg generelt sterkere til selskapets sikkerhetspolicy. Studiens konklusjon understreker betydningen av å kontrollere, måle, vurdere og justere tiltak underveis, og peker på dette som avgjørende for en vellykket kampanje. Konklusjonen legger samtidig vekt på at materiell kan være effektivt støtteverktøy i en kampanje dersom det er enkelt, raskt og kortfattet (Eminağaoğlu et al., 2009, p. 229), og at dette bør komme i tillegg til læring og trening. Mange glemmer det de eksponeres for gjennom trening, og slikt materiell kan friske opp bevissthet rundt konsepter fra trening som har funnet sted tidligere.

6.2 Erfaringer fra bevisstgjøringskampanjer for cybersikkerhet

En betydelig andel case-studier fra sikkerhetskampanjer finner vi innen feltet cybersikkerhet. Dette gir godt empirisk grunnlag for å kunne vurdere slike erfaringer opp mot det man ønsker å oppnå med en kampanje. Økningen i antall cyber-hendelser de senere år er betydelig, og mange av dem retter seg mot sårbarheter forårsaket av menneskelige faktorer (NSM, 2019).

En betydelig andel av litteraturen innen informasjonssikkerhet og cybersikkerhet ser på hvordan ansatte i bedrifter kan trenes eller utdannes til å bedre beskytte informasjon og tilgang til IKT-systemer gjennom fokus på for eksempel passord-beskyttelse og verifisering, samt bevissthet rundt digitale angrep. De har også til felles at de vurderer menneskene i organisasjonen som den fremste og mest kritiske forsvarslinjen (Tipton & Krause, 2007). Dette underbygger forståelsen om at mennesket og teknologien fungerer sammen i integrerte systemer og prosesser og må behandles under ett. Information Security Awareness (ISA) er et større fagfelt med tiltagende fremvekst fra millenniumskiftet, og det er også et konsept etablert i mange virksomheter.

Innen cyber, har design og valgarkitektur fått større fokus etter at det ble tydelig at svikt også i digital adgangsbeskyttelse i stor grad skyldtes menneskelige faktorer (Yeoh et al., 2022). Sosial manipulering (*social engineering* på engelsk) er et konsept innen informasjonssikkerhet som omfatter metoder for å tilegne seg tilgang ved å utnytte menneskelige faktorer. I sosial manipulering benytter ondsinnede aktører avanserte psykologiske metoder for å manipulere mennesker til å gi fra seg beskyttet informasjon og tilgang til beskyttede systemer. Sosial manipulering er utbredt i cyberdomenet, og phishing-angrep er et kjent eksempel på metode. Et phishing-angrep kan for eksempel opptre i form av en falsk programvareoppdatering, virus-trussel eller lignende, som skal lokke brukeren til å foreta valg som fører til at inntrengeren får tilgang. En nyere case-studie av en omfattende sikkerhetsbevissthetskampanje om phishing, viser at kombinasjonen av simuleringskampanjer og trening har vist seg spesielt nyttig. Forskerne hevder at sikkerhet relatert til phishing er en lengre læringsprosess, og at menneskers atferd kan styrkes gjennom forsterkning (forsterkning er et faguttrykk i psykologien som betyr styrking av en respons ved hjelp av operant eller instrumentell betinging) eller modereres gjennom straff. Kampanjen hadde mål om å redusere antall personer som responderer på phishing-epost, øke antall innrapporteringer av suspekte e-post, og identifisere mulige grupper i organisasjonen som er spesielt sårbare for phishing-angrep. Til sammen 10,000 ansatte deltok i studien. I dag har flere tilgang til mer avansert teknologi som kan beskytte tilgang mot menneskelig svikt ved å begrense valgalternativer i tekniske systemer.

En studie av van Steen et al. (2020) er en av de nyere og ser på sikkerhetskampanjer for cybersikkerhet, utviklet av myndighetene. Forskerne inkluderte 17 slike kampanjer fra hele verden i studien. De viser til at bevisstgjøringskampanjer ofte fokuserer på læring og bevissthet, men feiler i sin forutinntatthet om endret atferd som følge av kunnskap om risikofaktorer og forståelse av hvordan sikkerhet kan bedres. Ingen av de 17 kampanjene prøvde å få folk til å bli mer cybersikre, utover utdanning eller trening. De fleste av kampanjene inneholdt ulike former for "instruksjoner" om hvordan man utfører atferden, for eksempel sjekklister for hvordan man kan holde seg trygg på nettet. Det var også kampanjer som inneholdt videoer med "imaginær straff" – som et scenario der man ser fiktive individer bli hacket fordi de brukte et usikret trådløst nettverk (fra kampanjen StopThinkConnect). Steen og kollegene (2020) har flere forslag til hvordan slike kampanjer kan forbedres, og ett av forslagene er å ha en *strukturert* tilnærming der man har med hvert aspekt av beslutningsprosessen i forhold til det å utvise en trygg oppførsel i cybersfæren. Det vil si å bruke mange ulike metoder for å ha innvirkning på beslutningsprosessen, og også fokusere mer spesifikt på enkelte målgrupper og hvilke plattformer som er best egnet. I tillegg mener forskerne det er viktig å inkorporere eksisterende kunnskap om endring av sikkerhetsatferd i kampanjene, og at det vil variere fra case til case hvilke atferdsendrings-teknikker som vil egne seg. Det blir imidlertid understreket i studien at det ikke er tilstrekkelig kun med økt bevissthet, da det ikke trenger å lede til en endring i atferd. I anbefalingene sine skriver de derfor at det kun er ved direkte atferdsmålinger man kan vurdere effektiviteten til en sikkerhetskampanje. En annen studie av van Steen (2022) foreslår at cybersikker atferd kan styres gjennom sluttbruker-interaksjon og teknisk design. Ved å begrense brukerens alternativer og dermed lede i retning av tryggere valg (såkalt *nudging*) eller å begrense risiko ved å fjerne risikable valgmuligheter i teknologien (såkalt *techno regulation*). Dette er eksempler på hvordan valg-arkitektur benyttes i praksis i cyberrommet.

En annen studie, har tatt for seg et antall cybersikkerhetskampanjer og vurdert suksessen av disse i forhold til hvorvidt de lykkes i å endre atferd (Bada et al., 2019). Studien har sett på to britiske kampanjer og to kampanjer rettet mot det afrikanske kontinentet i helhet. Kampanjene som studien har sett på er The GetSafeOnline Campaign, The Cyber Streetwise Campaign, The ISC Africa og Parents' Corner Campaign – altså alle myntet på sikker atferd på internett. Spesielt for utvalget er den ulike geografiske dimensjonen, og det viste seg at kampanjene spilte på ulike kulturelle og sosiale tilnærmimnger. Blant annet hadde

kampanjene rettet mot de afrikanske målgruppene et mer kollektivt fokus i forhold til de britiske som var mer individualistisk innrettet. Studien viser først til den samlede litteraturen innen sosialpsykologi og peker spesielt på at risikopersepsjon er sentralt, at forståelse kan lede til motivasjon som kan lede til handling, at mulighet til å utføre ønsket atferd må være lønnsom og at hindringer har stor betydning. Videre, understreker den at bevisstgjøringskampanjer feiler når løsninger ikke er i tråd med risiko, når progresjon og verdi ikke blir vurdert underveis, når ukorrekte antagelser om mennesker og motivasjon styrer og urealistiske mål settes (Information Security Forum referert i Bada et al., 2019). Å lykkes med en bevisstgjøringskampanje derimot, mener studien at fordrer bevisst forhold til strategi og valg (ryddighet i begrepsbruk om bevissthet vs. forståelse, kunnskap eller handling), realistiske forventninger, engasjement, engasjerende og treffende materiell, intervaller med måling og tilpasning og evaluering underveis og i etterkant. Dette reflekterer i stor grad det som også er skissert i teoridelen av dette kunnskapsgrunnlaget.

6.3 Teknologiske virkemidler for trening og læring

En del av teknologiene som muliggjør erfaringsbaserte konsepter, som for eksempel VR og gaming, kan bringe inn potensielt nye metoder til bruk innen bevissthet om cybersikkerhet. En studie av trening med gaming fra utvalget (Oroszi, 2019) viser at deltakerne som testet et escape room for å bli mer oppmerksomme på sikkerhetsrisiko, oppga at de likte bedre å lære ved å selv erfare situasjoner enn å være i en klasseromsetting. Årsaken var at man likte at man kunne kjenne egne svakheter, og dermed selv gjøre endringer i atferden. Ifølge artikkelforfatteren, som har flere års erfaring med å gjennomføre "security escape room games" i ulike organisasjoner og konferanser, kan dette være en godt egnet og effektiv metode for å øke ansattes bevissthet og kunnskap om informasjonssikkerhet. Oroszi (2019) fant også ut at man kunne bruke straff som virkemiddel om en deltaker for eksempel åpnet et simulert epost-vedlegg med skadelig innhold underveis i spillet. Straffen kunne være at teamet fikk tilleggstid som kunne påvirke vinnermulighetene.

Det finnes generelt mye forskning på læring og trening ved bruk av gaming og i virtuelle miljøer. Veneruso og kolleger (2020) har utviklet et videospill i VR, CyberVR, som har som målsetting å øke brukerens bevissthet om cybersikkerhet. I konseptet kan brukerne både se og ha interaksjon med omgivelsene rundt seg mens de har på seg et VR-headset. I spillet er du-personen en IT-tekniker som skal løse ulike oppgaver, og gjennom seks forskjellige mini-spill blir man introdusert til relevante tema innen cybersikkerhet, og hvordan man kan løse eller forstå utfordringene. Forskerne utførte en brukerstudie med 40 deltakere der de fant ut at CyberVR var mer engasjerende enn tradisjonell tekstbok-læring, men at de to ulike tilnærmingene ellers er like effektive. De mener også at VR-konseptet kan ha en langtidseffekt inn mot læring, for eksempel ved forbedringer som et resultat av læringserfaringen. Dette vet man imidlertid ikke nok om ennå, og det påpekes også av forfatterne at faktorer som VR-utstyr kan ha innvirket på resultatet. Det finnes ellers mange VR-applikasjoner innen trening og læring, og det er både utfordringer og mange muligheter når det gjelder bruken av denne teknologien inn mot bevisstgjøring og ferdighetstrening. Xie et al. (2021) studerte ulike VR-apper for trening og læring og fant blant annet ut at *kvalitativ forskning* er viktig for å forstå hvordan en person har erfart situasjonen i VR-scenarioet. Dette er vesentlig for å få til en overføringsverdi av treningen – noe som er viktig for at organisasjoner skal kunne ruste ansatte på best mulig måte i forhold til kunnskap og ferdigheter.

Når det gjelder e-læring demonstrerte Gundu og Flowerday (2013), at denne formen for læring kan være mer effektivt enn tradisjonell klasseromsundervisning når det gjelder læring om informasjonssikkerhet. Ansatte i et ingeniørfirma i Sør-Afrika gjennomgikk via e-læring en form for bevisstgjøringsprosess for

informasjonssikkerhet. Det aktuelle e-læringsprogrammet de ansatte fullførte var blitt utviklet i et aksjonsforskningsprosjekt, og bestod av en nettside med relevant tematikk innen informasjonssikkerhet. Ifølge forfatterne er det ulikt fra firma til firma hvilke temaer som får mest plass, ut fra hvilken situasjon den enkelte virksomheten befinner seg i (Gundu & Flowerday, 2013). Ved måling av e-læringen hadde forskerne fokus på å avdekke effektivitet av både budskap, metodikk og atferdsendring. De understreker også betydningen av ansattes holdninger i forhold til informasjonssikkerhet, som sammen med kunnskap og atferd kan bidra til økt sikkerhet. Studien deres viste at økt kunnskap ga positive endringer i både holdninger og atferd. De mener også at bruken av e-læring var mer økonomisk gunstig, ettersom de direkte kostnadene kun gikk til å designe websiden og til firmaets egen IT-tekniker som vedlikeholdt og oppdaterte nettsiden. De indirekte kostnadene gikk ned, ettersom ansatte kunne ta e-læringen når det passet dem, slik at minst mulig produktiv arbeidstid gikk til spille. Alt i alt konkluderes det med at gode informasjonssikkerhets-kampanjer resulterer i en positiv kultur for informasjonssikkerhet.

7 Diskusjon og anbefalinger

Dette kunnskapsgrunnlaget tar for seg litteratur innen fagfeltene sosialpsykologi, sikkerhetskultur og informasjonssikkerhet, og fremstiller noen hovedtrekk innen forskningslitteratur om bevisstgjøringsstrategier og effekt av disse. Formålet er å fremlegge eksisterende kunnskap på feltet, som kan danne et faglig grunnlag for bevisstgjøring relatert til innsiderisiko i norske virksomheter som behandler gradert informasjon. Videre diskuteres hva som kan overføres til en bevisstgjøringsstrategi som skal motvirke rekruttering av ubevisste innsidere, og hva som kan være interessant å undersøke med tanke på utfordringene forbundet med informasjonssikkerhet og innsiderisiko. Det understrekes at innsiderisiko forbundet med rekruttering av *bevisste* innsidere – altså de som selv er klar over at de fungerer som innsidere – ikke er hensyntatt i dette kunnskapsgrunnlaget, og at en litteraturundersøkelse som tar for seg den problemstillingen trolig ville kreve en noe annen innretning.

Fra et sosialpsykologisk perspektiv vil det være viktig at en bevisstgjøringskampanje formidler gode argumenter for *hvorfor* temaet er viktig. Dette fordi kampanjen retter seg mot sikkerhetsklarerte mennesker som det er naturlig å anta opplever at temaet har en personlig relevans, og at det dermed er de kognitivt baserte holdningene man jobber med. Det å kommunisere tydelig hvorfor temaet er viktig og hvordan den enkelte kan bidra for å øke informasjonssikkerhet og redusere innsiderrisiko blir i et slikt perspektiv sentralt. Fra et sosialpsykologisk perspektiv er det også grunn til å tenke at det kan være fruktbart å spille på en moderat mengde frykt for mulige konsekvenser av informasjon på avveie og hva det kan føre til for den som rekrutteres ubevisst. Det kan være nyttig for disse å vite hvordan en slik rekruttering kan foregå, hvilken prosess de kan havne i og hva det kan utvikle seg til, dersom de ikke utviser forsiktighet. Dersom man velger å spille på frykt, legger forskningen vekt på at bevisstgjøringskampanjen må formidle hva den enkelte konkret kan gjøre for å unngå de negative konsekvensene.

Å spille på sosiale normer og enkeltmenneskers behov for å opprettholde et positivt selvbilde er også nyttige faktorer inn i en kampanje. Dette er noe man kan gjøre ved å sikre at "god" atferd modelleres i det daglige slik at folk blir minnet på hva de deskriptive normene er. Ved å gjøre de ansatte til en del av bevisstgjøringskampanjen slik at de må være med på å formidle hva god atferd er, kan man skape en opplevelse av kognitiv dissonans dersom de selv begynner å fravike den atferden de selv lærer bort til andre. Gruppediskusjoner kan være en god metode for både å sette normer på agendaen og for å modellere atferd (Khan et al., 2011). Denne metoden er anbefalt fordi den i tillegg til å bygge kultur gjør det på en måte som gir de deltagende anledning til å utvikle holdninger på egne og hverandres premisser.

Selv om sosialpsykologien kan vise til en lang forskningstradisjon som har sett på sammenhengen mellom bevisstgjøringskampanjer og endret atferd hos enkeltindivider, er det nyttig å se til andre fagområder som i større grad setter informasjonssikkerhet i en større kontekst. Ved å ta utgangspunkt i konseptet *sikkerhetskultur* kan man se på bevisstgjøringskampanjer som del av den større organisasjonen også. For å lykkes med bevisstgjøringskampanjer som skal bidra til økt informasjonssikkerhet er det viktig å forstå hvordan for eksempel ledelse kan være sentralt for å sette temaet på agendaen. Videre vil ledere på ulike nivå være viktige rollemodeller, og vil kunne både bevisst og ubevisst være med å signalisere viktigheten av innholdet i en bevisstgjøringskampanje. Samtidig vil det også være viktig å fokusere på de relasjoner og praksiser som oppstår nedenfra-opp (Johannessen, 2022). Selv om utgangspunktet kan være at den menneskelige faktoren utgjør et svakt ledd i virksomhetens sikkerhet, bør det i stedet vurderes som en ressurs.

Ved å i tillegg se på muligheter innen kontekstuell tilnærming til atferdspåvirkning kan det i arbeid med informasjonssikkerhet trolig være av betydning å vurdere rammebetingelsene sikkerhetsklarerte ansatte jobber under. En kontekstuell tilnærming forutsetter at mennesker foretar irrasjonelle og inkonsistente valg, og det å lage systemer som reduserer både sannsynligheten og konsekvensene av menneskelig svikt blir dermed viktig. Dette berører også et organisatorisk aspekt, da det er ledelse og beslutningstakere som vil ha ansvaret for rammebetingelsene ansatte jobber under.

Oppsummert er det flere fagfelt og ulik litteratur å trekke på i utarbeidelse av bevisstgjøringsstrategier, og det er trolig fruktbart å trekke linjer mellom flere fagfelt for å bidra til at en bevisstgjøringskampanje sammen med utvikling av både god sikkerhetskultur og gode rammebetingelser bidrar til informasjonssikkerhet og redusert innsiderrisiko også på lang sikt. Skal det gjennomføres en bevisstgjøringskampanje bør det vurderes om denne skal ledsages av parallelle tiltak som påminnelser, kontekstuelle endringer, trening og læring. Sikkerhet bør utformes som en langsiktig strategi, og noen ganger, som i tilfellet med kampanjen mot phishing-angrep (se 6.2), så krever det ikke bare kunnskap, men også stadig og utviklende læring. Her kan trening i VR og andre teknologiske metoder bidra til å gjøre læringen både mer virkelighetsnær (relevant) og tilgjengelig ute på de ulike arbeidsstedene. I tillegg bør kampanjen designes i intervaller der det kontrolleres og måles underveis, slik at justeringer kan foretas og vurderinger og tiltak måles igjen. Kampanjer fungerer ofte best som påminnelser om eksisterende kunnskap eller for de som har gjennomgått trening.

Framtidig forskning bør på systematisk vis ta for seg effekten av en bevisstgjøringskampanje knyttet til den konkrete problemstillingen om rekruttering av ubevisste innsidere for å kunne si noe om hvilke virkemidler som er effektive. Fra de empiriske case-studiene som dette kunnskapsgrunnlaget har sett på, kommer det tydelig frem at forskjellige målsetninger og problemstillinger krever hver sine tilnærminger. Forskning som ser på hvordan organisasjoner kan jobbe med utviklingen av god sikkerhetskultur og som setter informasjonssikkerhet og innsiderrisiko på agendaen vil også være nyttig, og spesielt om dette settes i sammenheng med utviklingen av gode rammebetingelser og design. Erfaringsbaserte virtuelle trenings-apper i VR er eksempler på nyere metoder og kan utforskes videre i aktuelle miljøer; både utvikling av scenarioer og forskning på opplevelsen av disse. Et av de kanskje mest presserende bidrag fra forskningen på den aktuelle problemstillingen bevisstgjøring om innsiderisiko, vil likevel være å følge opp tiltak ved å måle effekt og foreslå justeringer videre i en lengre og mer helhetlig prosess.

Referanser

Ahluwalia, R. (2000). Examination of Psychological Processes Underlying Resistance to Persuasion. *Journal of Consumer Research*, *27*(2), 217–232. https://doi.org/10.1086/314321

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, *26*(9), 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Ajzen, I., & Fishbein, M. (2005). The influence of attitudes on behavior. In D. Alarracín, B. T. Johnson, & M. P. Zanna (Eds.), *The handbook of attitudes* (pp. 173–221). Springer-Verlag.

AlHogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 1–7. https://doi.org/10.1109/WCCAIS.2014.6916579

Antonsen, S. (2017). *Safety Culture: Theory, Method and Improvement*. CRC Press. https://doi.org/10.1201/9781315607498

Armitage, C. J., & Conner, M. (2001). Efficacy of the Theory of Planned Behaviour: A meta-analytic review. *British Journal of Social Psychology*, *40*(4), 471–499. https://doi.org/10.1348/014466601164939

Aronson, E., Wilson, T. D., & Akert, R. M. (2014). *Social Psychology* (8th ed.). Pearson Education Limited.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* (arXiv:1901.02672). arXiv. https://doi.org/10.48550/arXiv.1901.02672

Bolman, L. G., & Deal, T. E. (2017). *Artistry, Choice and Leadership: Reframing Organizations* (6th ed.). Jossey-Bass/Wiley.

Clore, G. L., & Huntsinger, J. R. (2007). How emotions inform judgment and regulate thought. *Trends in Cognitive Sciences*, *11*(9), 393–399. https://doi.org/10.1016/j.tics.2007.08.005

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

Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. (2012). Influencing behaviour: The mindspace way. *Journal of Economic Psychology*, *33*(1), 264–277. https://doi.org/10.1016/j.joep.2011.10.009

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report*, *14*(4), 223–229. https://doi.org/10.1016/j.istr.2010.05.002

E-tjenesten. (2022). *Fokus 2022*. Forsvaret. https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus

Festinger, L. (1957). *A Theory of Cognitive Dissonance*. Stanford University Press.

Gawronski, B., & Bodenhausen, G. V. (2007). Unraveling the processes underlying evaluation: Attitudes from the perspective of the APE model. *Social Cognition*, *25*(5), 687–717.

Goldstein, N. J., Cialdini, R. B., & Griskevicius, V. (2008). A Room with a Viewpoint: Using Social Norms to Motivate Environmental Conservation in Hotels. *Journal of Consumer Research*, *35*(3), 472–482. https://doi.org/10.1086/586910

Gundu, T., & Flowerday, S. V. (2012). The enemy within: A behavioural intention model and an information security awareness process. *2012 Information Security for South Africa*, 1–8. https://doi.org/10.1109/ISSA.2012.6320437

Gundu, T., & Flowerday, S. V. (2013). Ignorance to Awareness: Towards an Information Security Awareness Process. *SAIEE Africa Research Journal*, *104*(2), 69–79. https://doi.org/10.23919/SAIEE.2013.8531867

Jacobson, R. P., Mortensen, C. R., & Cialdini, R. B. (2011). Bodies obliged and unbound: Differentiated response tendencies for injunctive and descriptive social norms. *Journal of Personality and Social Psychology*, *100*, 433–448. https://doi.org/10.1037/a0021470

Johannessen, S. O. (2022). *Complexity in Organizations: A Research Overview* (1st ed.). Routledge. https://www.routledge.com/Complexity-in-Organizations-A-Research-Overview/Johannessen/p/book/9780367860189

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862–10868. https://doi.org/10.5897/AJBM11.067

Leventhal, H., Watts, J. C., & Pagano, F. (1967). Effects of fear and instructions on how to cope with danger. *Journal of Personality and Social Psychology*, *6*, 313–321. https://doi.org/10.1037/h0021222

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1–6. https://doi.org/10.1109/ICRIIS.2017.8002442

Malcolmson, J. (2009). What is security culture? Does it differ in content from general organisational culture? *43rd Annual 2009 International Carnahan Conference on Security Technology*, 361–366. https://doi.org/10.1109/CCST.2009.5335511

Meld. St. 5 (2020-2021). (2020). *Samfunnssikkerhet i en usikker verden*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm20202021000500dddpdfs.pdf

Morgan, G. (1998). *Images of Organization: Executive Edition*. SAGE Publications.

NSM. (2022). *Risiko 2022*. https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

Oroszi, E. D. (2019). Security awareness escape room—A possible new method in improving security awareness of users. *2019 International Conference on Cyber Situational Awareness, Data Analytics*

And Assessment (Cyber SA), 1–4. https://doi.org/10.1109/CyberSA.2019.8899715

Petty, R. E., Barden, J., & Wheeler, S. C. (2009). The Elaboration Likelihood Model of persuasion: Developing health promotions for sustained behavioral change. In R. J. DiClemente, R. A. Crosby, & M. C. Kegler (Eds.), *Emerging theories in health promotion practice and research* (2nd ed., pp. 185–214). Jossey-Bass/Wiley.

Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of Persuasion. In R. E. Petty & J. T. Cacioppo (Eds.), *Communication and Persuasion: Central and Peripheral Routes to Attitude Change* (pp. 1–24). Springer. https://doi.org/10.1007/978-1-4612-4964-1_1

Petty, R. E., Cacioppo, J. T., & Goldman, R. (1981). Personal involvement as a determinant of argument-based persuasion. *Journal of Personality and Social Psychology*, *41*, 847–855. https://doi.org/10.1037/0022-3514.41.5.847

PST. (2022). *Nasjonal trusselvurdering 2022*. https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2022/

Regjeringen. (2019). *Nasjonal strategi for digital sikkerhet* (Strategi Departementenes sikkerhets-og serviceorganisasjon 05/2019). https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Reno, R. R., Cialdini, R. B., & Kallgren, C. A. (1993). The transsituational influence of social norms. *Journal of Personality and Social Psychology*, *64*, 104–112. https://doi.org/10.1037/0022-3514.64.1.104

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W., & Thistlethwaite, D. L. (1970). Effects of fear arousal and reassurance on attitude change. *Journal of Personality and Social Psychology*, *15*, 227–233. https://doi.org/10.1037/h0029437

Rønnestad, I., Søfteland, A., & Drabløs, C. (2010). *Fryktbaserte røykesluttkampanjer - motiverende eller distanserende? : En kvalitativ undersøkelse av røykesluttkampanjen 'Røyken tar pusten fra deg'* [Bachelor thesis]. https://biopen.bi.no/bi-xmlui/handle/11250/94420

Rosenberg, B. D., & Siegel, J. T. (2018). A 50-year review of psychological reactance theory: Do not read this article. *Motivation Science*, *4*(4), 281–300. https://doi.org/10.1037/mot0000091

Schein, E. H. (2010). *Organizational Culture and Leadership* (4th ed.). Jossey-Bass, A Wiley Imprint.

Siero, F. W., Bakker, A. B., Dekker, G. B., & Van den burg, M. T. C. (1996). Changing organizational energy consumption behavior trhough comparative feedback. *Journal of Environmental Psychology*, *16*(3), 235–246. https://doi.org/10.1006/jevp.1996.0019

Tipton, H. F., & Krause, M. (2007). *Information Security Management Handbook* (6th ed.). CRC Press. https://doi.org/10.1201/9781439833032

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Information Security Journal: A Global Perspective*, *17*(5–6), 207–227. https://doi.org/10.1080/19393550802492487

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

van Steen, T. (2022). When Choice is (not) an Option: Nudging and Techno-Regulation Approaches to Behavioural Cybersecurity. In D. D. Schmorrow & C. M. Fidopiastis (Eds.), *Augmented Cognition* (pp. 120–130). Springer International Publishing. https://doi.org/10.1007/978-3-031-05457-0_10

van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity*, *6*(1), tyaa019. https://doi.org/10.1093/cybsec/tyaa019