"*Spørgsmålet er ikke om I bliver hacket, men hvornår*"

- Tre niveauer til opbygning af en IT-sikkerhedskultur i danske SMV'er

IT-Ledelse, 10. Semester – Specialeafhandling

31-05-2022

Vejleder: Kasper Trolle Elmholdt

Gruppemedlemmer:

Daniel Lund Kjær - 20174003

Line Lund Jørgensen - 20172990

Pernille Jensen - 20176334

Rune Kristensen - 20202161

Sofie Werner Henriksen – 20172954

Anslag: 169875

Abstract

Due to recent years' digital evolution and an increasing amount of cyberattacks, cybersecurity is a rapidly emerging phenomenon that organizations must incorporate into their daily work practice. Within the field of cybersecurity, two different aspects are challenging organizations; the technical aspect of cybersecurity, which consists of software, hardware, data, etc., and the non-technical aspect of cybersecurity which involves human behavior and awareness in relation to cybersecurity. The technical aspect of cybersecurity is thoroughly studied within the academic field of cybersecurity. Consequently, the authors of this master's thesis conducted a literature review of cybersecurity from a non-technical perspective prior to this master thesis, which became the foundation of this study. As such, the literature suggested numerous theories and exciting views on the subject; however, it was often in the context of larger enterprises. Thus, due to the shortage of academic work within the field, this study investigates how the management in small- and medium-sized enterprises (SMEs) can deal with cybersecurity challenges. Through analysis of empirical data based on four experts on the subject and three different theoretical perspectives combined with the prior acquired knowledge from the literature review, this master's thesis has established a framework, which serves as a strategic contribution for management in SMEs in strengthening cybersecurity. The framework consists of three different levels: a technological level, a psychological level, and a cultural level. The framework is intended to be generic, making it valuable for many different types of SMEs. In addition, the framework is meant to be established in an SME by the management, who will determine how they will operate within the specific business. This master's thesis contributes an SME perspective on the challenges that exist within the subject of cybersecurity

Forord

Dette speciale er udformet i perioden februar til 31 maj 2022 på IT-ledelse 10. Semester på Institut for digitalisering på Aalborg Universitet.

Specialet er et bidrag til forskningsfeltet om IT-sikkerhed, som beskæftiger sig med hvordan ledelsen kan være med til at højne IT-sikkerheden i SMV'erne. Dette er undersøgt grundet et stigende fokus på IT-sikkerhed generelt, men med et manglende fokus på konkrete tiltag ledelsen kan anvende til dette formål i SMV'erne.

I forbindelse med udformningen af specialet skal der lyde en stor tak til eksperterne som bidrog med deres tid og viden indenfor feltet, for at gøre udarbejdelsen af dette speciale og tilhørende resultater mulige.

Til slut skal der lyde en tak til vejleder, Kasper Trolle Elmholdt, for opbakning, vejledning og positivt humør.

Indhold

1. Introduktion

I takt med digitaliseringens frembrud har virksomheder generelt skiftet kurs til i dag at være mere teknologidrevne. Dette har medført en ændring i arbejdstilgang som giver både nye muligheder og forudsætninger for virksomheder, men åbner samtidig også op for en række nye fokuspunkter, heriblandt IT-sikkerhed, som er blevet et kritisk opmærksomhedspunkt for de fleste typer og størrelser af virksomheder. IT-sikkerhed er derudover også kommet i fokus, på grund af en stigning af hackingangreb på virksomheder, hvorfor det nu er blevet en realitet, at alle virksomheder må investere både tid og ressourcer i forebyggelse og respons mod disse nye trusler (Dansk Erhverv, u.å). Dette kan dog være en vanskelig opgave, da det er op til virksomhederne selv at vurdere, hvor meget der skal investeres i IT-sikkerhed samt hvordan det skal takles både eksternt, men også internt. Det er dog ikke kun virksomhederne og Dansk Erhverv, der er opmærksomme på IT-sikkerhed. Regeringen fremlagde i december 2021 en ny 2-årig cyber- og informationsstrategi, som blandt andet indebærer fordeling af midler til danske virksomheder samt politiets efterforskning af angreb på virksomheders IT-sikkerhed (Digitaliseringsstyrelsen, 2021).

Særligt de små- og mellemstore virksomheder (SMV'er) er udsatte når det kommer til IT-sikkerhed, fordi deres størrelse gør dem langt mere sårbare og til et lettere mål. Det skyldes ikke et manglende fokus på IT-sikkerhed i SMV'erne, men manglende handling bag dette fokus (Lloyd, 2020). SMVdanmark ønsker også at sætte øget fokus på problemet, og påpeger i den forbindelse, at der er behov for øget viden og ikke mindst rådgivning til SMV'erne, hvis ikke udviklingen med et stigende antal hackerangreb skal få store konsekvenser, ikke kun for SMV'erne selv, men også for deres samarbejdspartnere. Derudover påpeger SMVdanmark, at SMV'erne allerede har nok at se til i deres kerneforretning og i at varetage dagligdagsopgaver, hvilket gør IT-sikkerhed svært at prioritere (SMVdanmark, 2019). SMV'erne oplever således en større ressourcemæssig begrænsning, når det kommer til IT-sikkerhed. Erhvervsstyrelsen har foretaget en analyse af digital sikkerhed i danske SMV'er i forhold til deres risikoniveau som virksomhed, der viser, at "*40 pct. af danske SMV'er har et utilstrækkeligt IT-sikkerhedsniveau*" (Erhvervsstyrelsen, 2021). Denne analyse fra Erhvervsstyrelsen kan sættes i relation til et litteraturstudie lavet af specialegruppen på 9. semester, der kan beskrives som et forarbejde til dette speciale. Litteraturstudiet danner et grundlag, for det fokus det vil blive lagt jævnfør afsnit *1.3 Problemfelt*. De 40 procent understøtter resultaterne fra litteraturstudiet

om et behov for ændringer eller tiltag fra SMV'ernes ledelse, der kan få virksomhederne og dens medarbejdere til at have fokus på IT-sikkerhed og opnå et højere niveau heraf (Bilag B). SMV'erne møder dog fortsat en række udfordringer, når de vælger at bruge ressourcer på IT-sikkerhed og skal finde frem til den rigtige information om hvad der for dem er det rette at gøre for at afhjælpe og imødekomme problemerne med IT-sikkerhed. Dette fremgår ligeledes i den førnævnte analyse fra Erhvervsstyrelsen, hvor "*79 pct. af SMV'erne er enige i at enkle og konkrete råd om IT-sikkerhed kan øge deres fokus på digital sikkerhed*" (Erhvervsstyrelsen, 2021). Dette er også derfor at flere SMV'er er begyndt at rekruttere IT-specialister, men også her møder SMV'erne udfordringer, da "*57 pct. af virksomhederne oplever det som vanskeligt at finde frem til folk med den rigtige viden*" (Erhvervsstyrelsen, 2021). Rekrutteringen bliver derfor ofte en blindgyde for mange SMV'er, som selv må varetage opgaven om at styrke IT-sikkerheden. Ovenstående understreger yderligere behovet for fokus på IT-sikkerhed i danske SMV'er. Erhvervsministeriet, Dansk Erhverv, Dansk Industri, Finans Danmark, Forsikring & Pension, HK, IDA, Industriens Fond, IT-Branchen og SMVdanmark er gået sammen om en såkaldt *Cybersikkerhedspagt*, hvor målsætningen er, at Danmark skal have Europas mest digitale sikre SMV'er. Inddragelsen af alle disse parter skal ifølge dem selv sikre en koordineret og forpligtende indsats, som skal styrke IT-sikkerheden i SMV'er ved blandt andet at udveksle data og viden om digitale trusler, samarbejde på tværs og udvikle indsatser til at styrke ovenstående (Erhvervsministeriet, 2022).
Dette påpeger vigtigheden af at skabe øget opmærksomhed på SMV'er og deres sårbarhed i relation til IT-sikkerhed, samt hvordan det er muligt for dem at imødekomme denne sårbarhed og handle aktivt herpå.

1.2 Begrebsafklaring

Følgende afsnit har til formål at afdække centrale og relevante begreber for dette speciale. Disse begreber er udvalgt, da de er centrale for specialet, men kan opfattes på forskellige måder hvorpå en klar forståelse for deres anvendelse er påkrævet for at skabe gennemsigtighed i specialet.

1.2.1 Små og mellemstore virksomheder

Perspektivet for dette speciale er centreret omkring SMV'er, hvoraf der er behov for en klar afgrænsning af disse. SMV'er står for 99.8% af de eksisterende virksomheder i EU, men feltet

omhandlende en klar definition har ikke været belyst i samme grad som større virksomheder. Ulrich Loecher sætter fokus på dette ved at lave et klart skel mellem SMV'er og større virksomheder, der både trækker på kvantitative og kvalitative kriterier (Loecher, 2000). Først og fremmest omfavner SMV'er alle brancher. Der er således i højere grad tale om en definition i forhold til virksomhedens størrelse. I EU's kvantitative definition af SMV'er indgår antal medarbejdere, omsætning og årlig balance som bærende kriterier. Loecher argumenterer for, at dette er grundet kriteriernes simplicitet såvel som, at de er sammenlignelige og praktisk anvendelige. EU's kriterier er rammesættende for hvordan SMV'er anskues i dette speciale, og defineres således:

- SMV'er har et maksimal antal medarbejdere på 250.
- SMV'er har en maksimal årlig omsætning på 50 millioner Euro.
- SMV'er har en maksimal årlig balance på 43 millioner Euro.

Denne definition er valgt, da det udover EU-standard også er den definition som Danske SMV'er selv anvender og betragter sig ud fra (Jensen, Moltrup-Nielsen & Nielsen, 2016).

1.2.2 IT-sikkerhed

Der findes flere forskellige definitioner for begrebet IT-sikkerhed inden for feltet, som afdækker fænomenet, hvorfor der kan findes overlap og ligheder mellem dem. Disse begreber er blandt andet *Information and communication technology* (*ICT*), *Information security* og *Cybersecurity*. Grundlæggende har *ICT* til formål at beskytte den underliggende informationsteknologis struktur, hvor *Information security* udover *ICT* har fokus på alt den omkringliggende information (Von Solms & Van Niekerk, 2013). *Cybersecurity* bliver gennem ISO-standarden ISO/IEC 27032:2012 (2012) defineret som "*The preservation of the confidentiality, integrity and availability of information in Cyberspace*", hvilket gør *Cybersecurity* til et bredere og mere omfattende begreb end de andre to. Oversat til en dansk betegnelse for dette vil *IT-sikkerhed* være dækkende. IT-sikkerhed defineres som:

"It-sikkerhed handler om at beskytte noget – først og fremmest digitale devices, software og online profiler imod virus, hacking og andet misbrug. (...). Spørgsmål om it-sikkerhed angår således også kommunikationskompetencer, som viden om hvilke medier der bruges til hvad og med hvilke normer (...). Til sidst kan it-sikkerhed også handle om at beskytte sine data fra udbytning." (Undervisningsministeriet, 2018).

Cybersecurity og IT-sikkerhed handler dermed begge om beskyttelse af digital information igennem de tekniske og fysiske rammer samt en forståelse for virksomheden og dens medarbejdere, der også er en del af sikkerheden som helhed, hvorfor der er truffet et valg om at anvende begrebet IT-sikkerhed i dette speciale. Derudover anses IT-sikkerhed også som den danske oversættelse af Cybersecurity, hvorfor det giver mening at benytte den danske betegnelse, idet afgrænsningen for dette speciale er et fokus på SMV'er i Danmark. Dette giver med andre ord også belæg for, selv om Cybersecurity som begreb blev anvendt gennem litteraturstudiet, så vil det i dette speciale blive omtalt som IT-sikkerhed, og fortsat dække og de samme elementer.

1.3 Problemfelt

IT-sikkerhed er ud fra ovenstående et område, hvor der ofte famles i blinde, særligt for SMV'er. Der findes endnu ikke en best practice, hvortil en af grundene kan være, at virksomhederne holder kortene tætte, når de er blevet udsat for et IT-angreb, og fordi IT-sikkerhed er så stor og omfangsrig en størrelse, som få virksomheder endnu har grebet om (Melnyk, Schoenherr, Speier-Pero, Peters, Chang & Friday, 2021). Det emergerende fokus på IT-sikkerhed og disse tilhørende udfordringer førte til at specialegruppen som nævnt ovenfor på 9. semester udarbejdede et litteraturstudie på baggrund af en systematisk tilgang gennem opsatte kriterier, omhandlende IT-sikkerhed i et ikke-teknisk perspektiv. Formålet med den systematiske metode bag litteraturstudiet var således objektivt at indsamle en mængde af artikler, der relaterede sig til hinanden ud fra de prædefinerede udvælgelseskriterier. Det mest centrale kriterium for litteraturstudiet var fravælgelsen af tekniske elementer og perspektiver, hvilket skyldes en ønsket afgrænsning til adfærds- og vidensaspektet af IT-sikkerhed. I litteraturstudiets analyse blev der fundet tre overordnede tendenser indenfor IT-sikkerhed i et ikke-teknisk perspektiv: *Adfærd, Cybersecurity træning* og *Ledelse*. Litteraturstudiet vil i dette speciale være fundamentet for den forforståelse, som anvendes i udformningen af specialets problemformulering og en opsummering af de vigtigste pointer vil blive fremlagt i efterfølgende jævnfør afsnit *1.3.1 Adfærd*, *1.3.2 Ledelse* og *1.3.3 Træning*. Det samlede litteraturstudie kan findes i bilag B.

1.3.1 Adfærd

Det menneskelige aspekt eller hvordan medarbejderne agerer i virksomheden, blandt de største årsager til hackingangreb. Denne adfærd skyldes i høj grad manglende viden blandt medarbejderne, manglende engagement fra ledelsen (Reeves et al., 2021b) og et manglende fokus på IT-sikkerhed som gennemsyrer hele virksomheden (Bada & Nurse, 2019). Derudover er fokus skiftet fra hacking af selve virksomheden til at gå efter medarbejderne og deres adfærd i forhold til IT-sikkerhed (Greitzer, Moore, Cappelli, Andrews, Carroll & Hull, 2008). Ergen, Ünal & Saygili (2021) fremlægger en liste over anbefalet adfærd i relation til IT-sikkerhed. Her fandt de frem til en forskel mellem attitude og adfærd, som kom til udtryk gennem holdninger som "Det sker ikke for mig" i relation til hacking og yderligere at medarbejderne betragtede deres enheder som værende sikre. Dette skyldes, at medarbejderne føler sig overbeviste om, at de besidder den rette viden omkring IT-sikkerhed, men sandheden er ofte, at de har den forkerte viden og derfor mangler træning i IT-sikkerhed (Ergen et al. 2021). For at medarbejderne får den rigtige viden om IT-sikkerhed er det vigtigt, at en virksomhed forsøger at skabe awareness om problemet (Alshaikh, Maynard & Ahmad, 2021). Denne awareness kan blandt andet skabes gennem awareness-programmer, som kan bidrage til at ændre adfærden hos medarbejderne (Alshaikh & Adamson, 2021). Ergen et al. (2021) påpeger dog, at awareness er et vigtigt element i at skabe en adfærdsændring, men at det ikke er tilstrækkeligt til at skabe en adfærdsændring alene.

Ydermere fremlægges det i litteraturen, hvilken adfærd en medarbejder kan udvise, hvis de udsættes for en overvældende mængde af tiltag om IT-sikkerhed, også kaldet *Cyber fatigue* (Reeves et al., 2021b). *Cyber fatigue* er overeksponering af IT-sikkerhedsrelaterede tiltag, som ofte leder til, at medarbejderen får et negativt syn på alt hvad der indebærer IT-sikkerhed, og i nogle tilfælde vil medarbejderen modarbejde de tiltag, som virksomheden forsøger at etablere (Reeves et al., 2021a).

1.3.2 Ledelse

Der findes en stor udfordring hos ledelsen i forhold til at granske IT-sikkerhed. Ledelsen skal indsætte initiativer både med et økonomisk og menneskeligt aspekt for øje – For hvor meget skal der investeres i IT-sikkerhed, når man ikke kender det fulde omfang heraf? Og er det virkelig nødvendigt, at alle medarbejdere får træning i IT-sikkerhed? Yderligere ligger der også en opgave i at tilpasse IT-sikkerhedstræningen til medarbejdernes behov og jobfunktion

(Reeves, Calic & Delfabbro, 2021b). For store mængder af IT-sikkerhedstræning kan dog også resultere i en række konsekvenser som cyber fatigue, modstand mod IT-sikkerhedstiltag og spild af økonomiske ressourcer. En ledelsesmæssig opgave bliver derfor at balancere mellem at klæde medarbejderne på, så de udviser passende adfærd i forhold til IT-sikkerhed samtidig med, at de ikke bliver overvældet med information (Reeves, Delfabbro & Calic, 2021a; Korpela, 2015). Derudover er det nødvendigt at IT-sikkerhedstiltag betragtes på et strategisk plan af ledelsen, hvor det ikke kun tager udgangspunkt i implementering af træning og systemer, men ligeledes processerne efter angreb (Ahmad, Desouza, Maynard, Naseer & Baskerville, 2020). Ifølge Ahmad et al., (2020) kan der etableres ledelsesteams, som er ansvarlig for fem områder, der danner grundlag for strategier, som har til formål at beskytte virksomheden og reducere chancen for trusler. En anden central tilgang i litteraturen er, at der skal være fokus på at skabe vidensdeling i virksomheden. Ahmad et al. (2020) fremskriver et holistisk billede af en virksomhed, hvor der i høj grad er fokus på vidensdeling på tværs af alle niveauer både horisontalt og vertikalt. For mange virksomheder og deres ledelse er det en udfordring at vurdere, hvorvidt det er en økonomisk fordel at investere i IT-sikkerhed fordi IT-sikkerhed kræver løbende finansiel forpligtelse, som kan være udfordrende for en virksomheds budgetter (Zhang et al., 2021).

1.3.3 Træning

Gennem litteraturstudiet blev problematikken om adfærd anset for at kunne ændres gennem tiltag som træning af medarbejdere i IT-sikkerhed. Dette undersøgte Reeves et al., (2021b) gennem træningsprogrammet *Security Education, Traning,* og *Awarenss* (SETA). I den forbindelse blev nogle af de fremskrevne problematikker ved SETA fremhævet som kedeligt indhold, manglende kontekst og for meget information, hvilket kunne resultere i det omtalte cyber fatigue og manglende effekt af træningen. Ydermere blev det i samme undersøgelse fremhævet, at et element for at opnå en mere succesfuld træning var, at den skulle være mere interaktiv (Reeves et al., 2021b). He & Zhang (2019) fremskriver, at IT-sikkerhedstræning kan være mange ting, og kan gøres gennem fysisk undervisning eller gennem et online træningsformat, og derigennem kan man inspirere og kommunikere best practices for at ændre adfærden hos medarbejderen. Træning skal være beskrevet klart og tydeligt gennem virksomhedens procedure eller retningslinjer, frem for blot at fortælle medarbejderne, hvad de skal gøre (He & Zhang 2019). Foruden de ovenstående problematikker er en central tendens i forhold til træning, at disse skal tilpasses virksomhedens kontekst samt den enkelte

medarbejder (Korpela, 2015; Furnell & Vasileiou, 2017), da IT-sikkerhed ikke udelukkende er en teknisk udfordring for virksomheder, men også vedrører de mere bløde menneskelige aspekter, hvorfor det er nødvendigt at medarbejderne besidder færdigheder, der understøtter virksomhedens sikkerhed (Furnell & Vasileiou, 2017). Ifølge Sussmann (2021) kaldes disse færdigheder *Non-technical knowledge, Skills* og *Abilities* og dette indebærer blandt andet problemløsning, kommunikation og samarbejde. Litteraturen foreslår at fremtidige IT-sikkerhedseksperter både besidder de tekniske og ikke-tekniske færdigheder (Haney & Lutters, 2021; Sussmann, 2021).

1.3.4 Afgrænsning

Denne specialeafhandling vil, med afsæt i at løse nogle af de problemstillinger, som er beskrevet ovenfor, have fokus på, hvordan der kan udformes et rammeværk, som kan benyttes af ledelsen i SMV'erne til at skabe et større fokus på IT-sikkerhed samt en forbedring heraf gennem træning af medarbejdere og et fokus på deres adfærd. Dette fordi det er gennem medarbejderne, at retningslinjer fra ledelsen om IT-sikkerhed skal efterleves. Det valgte fokus på ledelsen skyldes litteraturens opmærksomhed på, at det er hos ledelsen at IT-sikkerhed starter, hvis det skal på dagsordenen ude i virksomhederne. Derudover undersøgte og henvendte mange af artiklerne i litteraturstudiet sig til større virksomheder, der ofte allerede har en IT-afdeling etableret, hvilket i en dansk kontekst med fokus på SMV'er ikke altid er muligt at imødekomme. Et fokus på SMV'er og deres manglende ressourcer til IT-sikkerhed er derfor særligt interessant og ikke mindst relevant. Kombinationen af litteraturens fokus på de tre overordnede tendenser *adfærd, ledelse og træning*, et manglende fokus på SMV'er samt en identificering af deres store behov for noget mere konkret og håndgribeligt til at håndtere udfordringerne med IT-sikkerhed udgør afgrænsningen for dette speciale. De omtalte udfordringer vil blive adresseret og bearbejdet gennem viden fra litteraturstudiet i samspil med empiri indsamlet gennem ekspertinterviews jævnfør afsnit *2.4 Interview*.

1.4 Problemformulering

Ovenstående introduktion og problematisering af identificerede fænomener inden for IT-sikkerheds domænet har udmundet i følgende problemformulering:

Hvilken betydning har ledelsen i forhold til IT-sikkerhed, og hvordan kan et rammeværk med fokus på medarbejderadfærd understøtte ledelsen i formålet om at styrke IT-sikkerhed i små- og mellemstore virksomheder?

Formålet med dette speciale samt besvarelsen af problemformuleringen vil være at undersøge medarbejderadfærd i forhold til IT-sikkerhed, hvortil denne forståelse bidrager til at udvikle et rammeværk, der kan understøtte ledelsen i SMV'erne i deres initiativ om at skabe bedre forudsætninger for IT-sikkerhed. Målet med rammeværket bliver ydermere at forholde det så overordnet som muligt, idet rammeværket tiltænkes alle SMV'er på trods af størrelse og branche. Yderligere er en målsætning for værktøjet, at det kan anvendes sammen med ledelsens øvrige tiltag, hvor det udviklede rammeværk skal bidrage til at påvirke medarbejdernes adfærd inden for IT-sikkerhed og på den måde fungere som en forsikring for virksomhederne. Specialet er skrevet med henblik på at kunne bidrage til både et akademisk og praktisk formål i forbindelse med IT-sikkerhed. Specialets akademisk formål er at bidrage med et SMV-perspektiv på IT-sikkerhed til den eksisterende forskningslitteratur, der er begrænset på området. Specialets praktiske formål vil derfor være at skabe et rammeværk, der kan bidrage til SMV'ernes ledelses strategiske tiltag og retningslinjer i forbindelse med IT-sikkerhed.

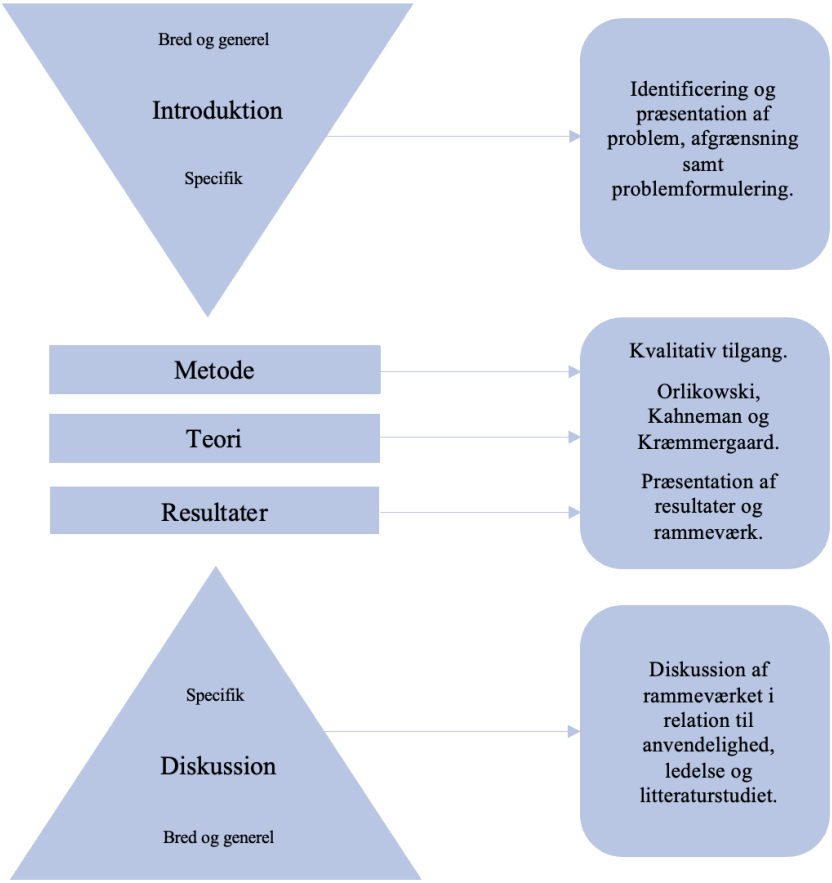
2. Metode

Det følgende afsnit tager udgangspunkt i specialets metodiske valg og overvejelser, og har til formål om at skabe gennemsigtighed samt argumentation for valg af metodiske beslutninger, der er grundlag for specialets empiriske afsæt. Afsnittet vil bidrage med en beskrivelse af den kvalitative tilgang, udvælgelsen af informanter, interviewtypen, den udarbejdede interviewguide samt databehandling.

Specialets metodiske tilgang er den kvalitative forskningsmetode, som skal hjælpe med at analysere finde mønstre imellem de komplekse aspekter der er indenfor IT-sikkerhed og medarbejderes adfærd. Den kvalitative forskningstilgang er kendetegnet ved at man går i dybden med *hvordan* noget gøres idet at undersøgelser fokuserer at fortolke og forstå den menneskelige erfarings kvaliteter (Brinkmann & Tanggaard, 2015). Den kvalitative metode er valgt idet der herigennem skabes et dybdegående fokus i empiriindsamlingen hvilket kan medvirke til at belyse medarbejdernes adfærd i relation til IT-sikkerhed, i et sådant perspektiv at der skabes et relevant grundlag for konstruktionen af dette speciales rammeværktøj.

2.1 Forskningsstrategi

Dette afsnit giver et overblik over det overordnede forskningsdesign, der har til formål at lægge strukturen for tilgangen til at besvare specialets problemformulering. Specialet følger timeglas strukturen som vist til venstre på figur 1 nedenfor:



Figur 1 - Timeglas struktur inspireret af Pedersen & Morthorst (2017).

Som det fremgår af ovenstående figur 1, begynder denne struktur med en bredere introduktion til det generelle problem, hvorefter den indsnævres til den specifikke problemstilling, der er blevet beskrevet i afgrænsningen. Efterfølgende præsenteres metoden til at undersøge det specifikke problem og derefter den udvalgte teori som skal hjælpe med at besvare og belyse det specifikke problem. Derefter præsenteres undersøgelsens resultater. Endeligt udvider strukturen igen omfanget og sætter forskningens resultater i et bredere perspektiv gennem en diskussion af resultaterne og hvad de bidrager med til forskningsfeltet (Pedersen & Morthorst, 2017).

I forhold til figur 1 sættes dette speciale i relation til timeglasfiguren. Timeglasfiguren er illustreret til venstre, hvortil der i højre side er udvidet med firkantede bokse, der relaterer sig til specialet. Afsnit *1. Introduktion* præsenterer problemfeltet med tilhørende afgræsning og specificering af problemet, der munder ud i en problemformulering. Afsnit *2. Metode* har til formål at beskrive det overordnede forskningsdesign samt til -og fravalg af den metodiske fremgangsmåde, der skal danne grundlag for arbejdet med den indsamlede empiri. Derefter fremlægges der i afsnit *3. Teori* de tre forskellige teoretiske perspektiver der anvendes i specialet, som problemstillingen kan betragtes ud fra i relation til rammeværket. Derefter præsenteres resultaterne af dette speciale i afsnit *4. Analyse og udformning af rammeværk*, hvortil analysen er opdelt i to. Den første del har til formål at udlægge resultaterne af empirien, mens anden del anskuer problemet gennem de tre førnævnte teoretiske perspektiver. Yderligere indeholder afsnittet til slut en opsummering og kortlægning af analysens vigtigste tendenser samt en præsentation af rammeværket med tilhørende opmærksomhedspunkter, som kan understøtte den opstillede problemformulering. Til sidst diskuteres analysens resultater i afsnit *5. Diskussion* i forhold til problemets gennemgang af rammeværkets potentiale for ledelsens anvendelse ude i SMV'erne samt afsættet for rammeværket med til- og fravalg mellem litteraturstudiet og specialet. Til sidst afrundes diskussionen med et bredere fokus på rammeværkets generelle anvendelse i alle SMV'er.

2.2 Abduktiv metode

Strukturen for samspillet mellem empiri og teori, er i specialet udarbejdet med udgangspunkt i den abduktive metode. Den abduktive metode tager udgangspunkt i forskerens fremsatte problemstillinger og tilføjer hertil en kombination af teoretiske og empiriske udlægninger. De teoretiske perspektiver danner ramme for de empiriske fund som bliver analyseret for at belyse problemstillingen. Empiri og teori komplementerer således hinanden i en vekselvirkende proces som, foregår igennem udarbejdningen af hele specialet. Den abduktive metode har også den styrke at teorien kan tilføje perspektiver på den indsamlende empiri, der beriger værdier af den pågældende viden ved at udvide forståelsen af denne (Bryman, 2012).
Strukturen tager udgangspunkt i vekselvirkningen mellem empiri og teori, og starter i dette speciale med litteraturstudiet, som danner grundlag for den indledende forståelse, herunder problemformuleringen, samt vidensgrundlag for interview og kodning. Hertil inddrages et teoretisk grundlag som benyttes til analyse og fortolkning af de empiriske resultater der er

fundet igennem interviewene. Afslutningsvist konstrueres rammeværket ud fra de resultater der findes i den pågældende analyse.

2.4 Interview

I denne undersøgelse inddrages ekspertinterviews til indsamling af empiriske data. Som nævnt tidligere fokuserer dette speciale på udarbejdelsen af et rammeværk til ledelsen i SMV'er til at opnå en påvirkning af medarbejderes adfærd indenfor IT-sikkerhed.
Et ekspertinterview, eller hvad Kvale & Brinkmann (2009) omtaler som et eliteinterview, kendetegnes ved at informanten er leder eller ekspert. Ydermere fastslår Kvale & Brinkmann (2009), at en eliteperson eller ekspert er vant til at blive spurgt om deres meninger og holdninger om et emne, hvor de besidder en vis ekspertise inden for, hvorfor der opstår en forventning om at intervieweren bør have et solidt kendskab til emnet forud for interviewet. Dette kendskab bliver i forhold til dette speciale opnået igennem det førnævnte litteraturstudie. Formålet med interviewene er at få ekspertindsigt i den problemstilling, som specialet undersøger, analyserer og ønsker at finde en løsning på. Valget om at inddrage ekspertviden skyldes blandt andet identificeringen af problemet gennem litteraturstudiet. Dette betyder også, at fokus på én virksomhed er blevet fravalgt, hvilket skyldes, at et fokus på en enkelt virksomhed kun ville give svar og løsninger på deres konkrete udfordringer i relation til IT-sikkerhed, og ikke understøtte det mere overordnede og generelt anvendelige rammeværk, som der ønskes at udforme i dette speciale. Samtidig ville dette have begrænset det mere generiske fokus for rammeværket, da et udsnit af SMV'er ikke ville være dækkende for alle SMV'er, da disse alle placerer sig indenfor bestemte brancher. Ekspertviden anses derfor som værende et relevant supplement til at skabe en dybere forståelse af fænomenet.
De enkelte interviews afholdes af en person og et andet gruppemedlem, som bisidder for at sikre sig, at tiden bliver overholdt, at alle spørgsmål bliver stillet og for at komme med mulige opfølgende emner, som kunne være relevant at spørger yderligere ind til. Interviewene er semistrukturerede for at muliggøre en dialog med eksperterne, hvor gruppens eksisterende viden kan blive suppleret med ekspertviden, som kan bidrage og give nye indsigter til de eksisterende meninger og tanker hos gruppen. Med andre ord giver denne form for interview mulighed for at eksperterne kan byde ind og udfolde relevant viden, som ligger i forlængelse af interviewguiden jævnfør afsnit *2.6 Interviewguide*. Dertil vil fokus ydermere ligge på viden, som kan bidrage til rammeværket.

2.5 Udvælgelse af eksperter

Udvælgelsen af eksperterne til dette speciale tager afsæt i hvilke eksperter, der anses som værende de mest relevante inden for dette speciales emneafgrænsning. Derudover er de udvalgt på baggrund af den særlige viden og ekspertise, som de hver især besidder og kan bidrage med af erfaring indenfor hvert deres ekspertområde. Disse personer kan derfor betragtes som værende eksperter i henhold til i foregående afsnit jævnfør afsnit *2.4 Interview*. Eksperterne vil ud fra denne afgrænsning ikke have samme udgangspunkt og område at afdække, hvilket giver mulighed for at opbygge en forståelse for de enkelte elementer der er valgt at have fokus på i relation til forståelsen af IT-sikkerhed, og dermed samme en bredere sammenhæng og forståelse.

Derudover er der truffet et valg om ikke at udvælge eksperter, som er tilknytte en virksomhed, der sælger en konkret IT-løsning. Dette fravalg skyldes, at eksperter i den kontekst ofte vil være bundet op på at sælge et konkret produkt, og derfor vil deres svar på spørgsmålene og løsninger på de opstillede problemer muligvis være påvirket af dette. Sådanne eksperter vil i den forbindelse kunne risikere at medføre svar der relaterer sig ind i den virksomheds kontekst frem for specialets, hvilket ikke vil bidrage med de tilnærmelsesvis neutrale svar og generelle aspekt, der søges efter i dette speciale. Denne afgrænsning medfører dog også, at antallet af eksperter der findes relevante for gruppen at inddrage er begrænset.

Ovenstående indikerer, at der ikke er opsat konkret definerede kriterier for udvælgelsen af eksperter. Der er i stedet truffet et valg om at afgrænse og fravælge i relation til udvælgelsen af eksperter for at kunne indsamle eksperter indenfor et begrænset felt, der alle i et eller andet omfang blev betragtet som værende relevant.

Foruden de udvalgte eksperter der passede ind i ovenstående afgrænsningen, er snowball-strategien (Andersen, Hansen & Klemmensen, 2012) anvendt i søgen efter flere eksperter. Dette er resulteret i én ekstra ekspert og en henvisning til en ekspert, der allerede var et interview med.

Følgende er de udvalgte eksperter, og en kort beskrivelse af dem og deres bidrag til undersøgelsen:

Navn	Fokusområde	Arbejdstitel	Benævnes
Kristian Krogstrup	SMV'er	IT-konsulent: IT-sikkerhed i SMV'er	Krogstrup
Jens Myrup Pedersen	Tekniske og	Professor:	Pedersen

	teoretisk baseret viden	Landsholdstræner for det danske cyberlandshold	
Rebecca Thorning Wine	Adfærd, awareness og træning	Specialist: Digital Learning	Wine
Inge Alsmith	Sammenfaldende på det hele	Rådgiver: Center for Cybersikkerhed	Alsmith

Tabel 1: Ekspert sampling

Kristian Krogstrup er ekstern IT-konsulent, som er specialiseret indenfor IT-sikkerhed. Krogstrup har flere års erfaring i at konsultere og samarbejde med SMV'er, hvorfor han er et oplagt valg til dette speciale. Desuden holder Krogstrup online kurser omkring IT-sikkerhed i SMV'er, hvorfra specialegruppen opdagede hans kompetencer og mulige bidrag til dette speciale.

Jens Myrup Pedersen er professor for Institut for Elektroniske Systemer, Det Tekniske Fakultet for IT og Design samt Communication, Media and Information technologies ved Aalborg Universitet. Derudover er han medlem af Cyber Security Group og Cybersecurity Network. Pedersen har en stor viden og erfaring indenfor feltet i form af hans erhverv, hvilket gør ham i stand til at koble forskning og praksis, idet han uden for Aalborg Universitet også er medlem af Bestyrelsesforeningens Center for Cyberkompetencer, Rådet for Digital sikkerhed og er landstræner for det danske Cyberlandshold. Derudover kan han bidrage med de mere tekniske aspekter af feltet, som ellers ikke er blevet afdækket.

Cyberpilot er en dansk IT-sikkerhedsvirksomhed, der rådgiver og samarbejder med virksomheder, der ønsker at opnå en effektiv IT-sikkerhed (Cyberpilot, u.å). Cyberpilot er interessant for dette speciale, fordi de ikke blot har fokus på IT-sikkerheds-teknologi, men også vægter mennesker og adfærd lige så højt når det kommer til IT-sikkerhed (Cyberpilot, u.å). Eksperten fra Cyberpilot er Rebecca Thorning Wine, som besidder rollen som Digital Learning Specialist. Hun arbejder blandt andet med ændring af non-compliant behavior til compliant behavior, samt hvordan en god IT-sikkerhedskultur kan måles, og hvordan medarbejdere oparbejder en god IT-sikkerhedsadfærd.

Inge Alsmith arbejder til dagligt hos Center For Cybersikkerhed og sidder i den afdeling der hedder Civil og Rådgivning. Her sidder hun som rådgiver for offentlige og statslige myndigheder, samfundskritiske sektorer herunder også private virksomheder. Alsmith sidder for øjeblikket, og arbejder tæt sammen med erhvervsstyrelsen, hvor de har et øget fokus på

SMV'er, som dermed også er deres fokusgruppe. Dette indebærer tæt sparring og koordinering mellem Alsmith og erhvervsstyrelsen i relation til SMV'er.

2.6 Interviewguide

Interviewguiden er struktureret efter specialets problemformulering, som tager afsæt i litteraturstudiet, hvilket tilsammen indsnævrer interviewemnerne til *Intro*, *SMV'er*, *Adfærd*, *Ledelse*, *Træning* og *Afsluttende bemærkninger*. Den forforståelse og tilhørende tendenser der blev opnået gennem litteraturstudiet, vil være omdrejningspunkt for interviewene, og bliver præsenteret for vores eksperter, så de afholdte interviews snakker ud fra og ind i samme kontekst og forståelse. Forforståelsen gør formuleringen af åbne spørgsmål vigtig, da det er med til at sikre de tendenser og udfordringer der blev identificeret i litteraturstudiet ikke blot bliver af- eller bekræftet, men at der stadig er mulighed for ny viden. Nedenfor præsenteres et udsnit af interviewguiden, mens den fulde version kan findes i bilag C.

Intro	Præsentation af eksperter (Af dem selv) - Navn, arbejdsfunktion, års erfaring indenfor feltet osv.
SMV'er	Har du oplevet, at SMV'er har større udfordringer i forbindelse med IT-sikkerhed end de større virksomheder? Og i så fald hvilke?
Adfærd	Hvad har du oplevet som værende udfordrende i forhold til adfærd i relationen mellem IT-sikkerhed og medarbejderne i en virksomhed generelt? - Og hvad ser du som mulige løsninger på disse?

Tabel 2: Interviewguide udsnit

Tabellen ovenfor er delt op i to sektioner, hvor venstre side er emnet for spørgsmålene, og højre side er spørgsmålene. Alle emnerne i interviewet starter med et åbent spørgsmål. Dette havde til formål at skabe en indsigt i, hvilke problematikker de anskuede indenfor emnet og få skærpet ekspertens fokus på dette område. Herefter følger nogle løsningsorienterede spørgsmål i relation til det eksperterne anså som problematikker inden for den adspurgte tematik. Yderligere skulle interviewguiden være med til at sikre, at interviewene havde den samme struktur for de afholdte interviews. De enkelte spørgsmål i hvert interview er tilpasset til de

enkelte eksperter og deres viden. Derudover indledes hvert interview med en kort præsentation af specialet og dets formål samt de gældende retningslinjer, såsom optagelse af interviewet.

2.7 Databehandling

Følgende afsnit vil præsentere dette speciales transskription og tilhørende opsatte regler herfor. Derudover vil den valgte kodning blive fremskrevet og præsenteret.

2.7.1 Transskription

En transskribering af interviewene udmunder i en skreven tekst, der egner sig til analyse og samtidig skaber transparens i specialet (Kvale & Brinkmann, 2009). De afholdte interviews er foregået henholdsvis via Microsoft Teams (Teams) eller som et fysisk møde. Under interviews over Teams er interviewet blevet optaget med Teams' indbyggede optagelsesfunktion. Under det fysiske interview, er der blevet optaget på én af gruppemedlemmers telefoner. Gruppen har i forbindelse med transskriberingen valgt at undlade at skrive uforstående som "(...)", hvilket indebærer grin, gentagelser og tankelyde. Dette er gjort for at gøre transskriberingerne ensformige. Den fulde transskription af alle interviews kan findes i Bilag A.

2.7.2 Kodning

Den følgende kodning drager inspiration fra den abduktive metode jævnfør afsnit *2.2 Abduktiv metode*, hvor der gennem litteraturstudiet blev indsamlet viden, som danner baggrund for kodningen af den indsamlede empiri gennem de afholdte interviews i specialet.
I dette speciale anvendes en lukket kodning. En lukket kodning anvendes på tekster ved at kode dem ud fra forhåndsdefinerede koder (Andersen et al., 2012). Den lukkede kodning er anvendt for at udnytte den forforståelse der er kommet gennem litteraturstudiet, hvilket betyder, at de generelle tendenser derfra trækkes videre og anvendes som koderne i en lukket kodning i dette speciale. Dette er gjort med henblik på at strømline tendenserne fra litteraturstudiet og resultaterne fra den indsamlede empiri. Kodekategorierne der kodes efter er *Adfærd*, *Ledelse*, *Træning* og *SMV'er.* Derudover tilføjes en kodekategori kaldet *Andet*, hvor elementer, som ikke kan placeres i de allerede opstillede kodekategorier, kan placeres. Dette kan bære præg af en mere åben kodning, dog indenfor den lukkede kodnings grænser, hvor transskriberingerne "får lov at tale" (Andersen et al., 2012), og er valgt for at skabe plads til eventuelle nye fund der måtte komme. Dette skyldes, at litteraturstudiet var bundet op på teori og manglende

praksiseksempler, hvortil det må forventes, at der på trods af opbygning af interviewguiden vil opstå nye fund ved både at inddrage SMV perspektivet samt undersøge området empirisk med eksperternes erfaringer fra praksis.

Alle kodekategorierne tildeles i praksis en farve, så hvert interview bliver farvekodet efter de kodekategorier, som kan identificeres. Efter kodningen af interviewene fremgik det, at kodekategorien *Andet* overvejende indeholdt citater om ressourcer af både økonomisk og menneskelige karakter samt IT-sikkerhed, hvorfor der blev truffet et valg om at danne en ny kodekategori kaldet *Ressourcer* og en kaldet *IT-sikkerhed*, hvor sidstnævnte bærer præg af fund, der er mere teknisk relaterede.

Nedenfor i tabel 3 fremgår et eksempel på, hvordan kodningen konkret i specialet er foretaget.

Kodekategori	Beskrivelse	Informant + Sidetal	Citat
Adfærd	Alle udsagn om adfærd i relation til IT-sikkerhed	Krogstrup 1 (nederst)	Ja der er den statistik med at ni ud af ti sikkerhedsbrud er på grund af medarbejder fejl. Man kan jo have den mest sikre netværk og alt muligt sikkerheds setup, men IT-kriminelle har fundet ud af at den nemmeste vej frem er at angribe medarbejderne fordi det er dem, der begår fejlene.
Ledelse	Hjælpe IT-sikkerhed på vej ved at sætte det på agendaen for at kunne ændre kulturen	Wine 5 (midt)	Så hvis vi skal tilbage til hvad ledelsen kan gøre for det [IT-sikkerheden] er det bare at tage den [IT-sikkerheden] på agendaen og gøre den [IT-sikkerheden] til en vigtig, en core [en kerne], en vigtig del af virksomheden.

Tabel 3: Kodning udsnit

3. Teori

Følgende afsnit præsenterer dette speciales udvalgte teori, deres relevans samt anvendelse heraf og deres samspil. De tre teorier er henholdsvis Orlikowskis perspektiv om *Entanglement in practice*, Kahnemans teori om *System 1* og *System 2* og Kræmmergaards teori om *Digital modenhed*.

3.1 Orlikowski - Entanglement in practice

I følgende afsnit vil Wanda Orlikowskis *The sociomateriality of organizational life: considering technology in management research* (2010) blive fremlagt med et formål om at kunne forklare samspillet mellem teknologier og menneskelig adfærd med henblik på i dette speciale at afdække, hvad der sker på arbejdspladsen i forbindelse med implementeringen af IT-sikkerhed. Orlikowski fremlægger tre perspektiver hvorpå teknologi kan anskues og foreslår derudover et fjerde, idet dette perspektiv tidligere enten har været ignoreret eller kun har været undersøgt gennem "*An ontology of separateness"* (Orlikowski, 2010 s. 134). Perspektiverne, hvori teknologi kan anskues gennem er: *Absent presence, Exogenous force, Emergent process* og *Entanglement in practice*, hvortil det kun er det sidstnævnte perspektiv, der vil blive gennemgået, da det er den forståelse, som dette speciale skriver sig ind i. Orlikowski beskriver *Entanglement in practice* som et perspektiv, hvorpå det sociale og materielle er sammenfiltret i sociomaterielle konfigurationer, hvilket adskiller sig fra de andre perspektiver, der betragter teknologi og aktører som to separate ting. Sociomaterialitet er et krydsfelt mellem teknologi, arbejde og organisation, og forsøger således at forstå den konstitutive sammenfiltring af det sociale og materielle i hverdagens organisatoriske liv (Orlikowski 2010). Med andre ord fokuserer dette perspektiv på at undersøge, hvordan medarbejderne, arbejde, fysiske objekter og teknologier benyttes i forhold til det sprog, interaktion og praksis, som de er viklet ind i på arbejdspladsen. Mere konkret inddrages Orlikowskis perspektiv, *Entanglement in practice*, i forhold til at forstå relationen mellem teknologien og mennesket, hvortil hun lægger vægt på, at relationen mellem enhederne er vigtigere end enhederne i sig selv, idet det er gennem handling, der bliver formet en betydning. Derudover er det også i denne relation eller forhandling med teknologien, at mennesket får en ny forståelse eller tilpasset forståelse af materialiteten, hvilket er en kontinuerlig proces (Orlikowski 2010). Orlikowski inddrager i sit perspektiv de non-humane eller materielle aktører, foruden menneskelige aktører, hvilket udvider spektret af elementer, der tillægges handlekraft markant, idet der kan være flere

materialiteter som tid, sted, rum og diskurs, der kan inddrages i en analyse og kan tillægges værdi til eksistensen af det undersøgte fænomen (Juelskjær & Schwennesen, 2012).
Orlikowskis perspektiv *Entanglement in practice* kan derfor bidrage til en forståelse af, hvordan teknologien eller materialiteten påvirkes i sammenspil med andre aktører. Yderligere bliver perspektivet benyttet i dette speciale med henblik på at kunne forklare IT-sikkerhed, som en praksis. Med andre ord kan teknologi ikke undersøges som et fænomen i sig selv uafhængigt af mening, idet de to ting er med til at skabe og er skabt af hinanden; de er uadskillelige, hvilket Orlikowski vil beskrive som *Entangled* (Orlikowski 2010). Det interessante for dette speciale er derfor sammenfiltreringen mellem aktørerne – både humane og non-humane (materialiteten).

3.2 Kahneman - System 1 og System 2

Følgende afsnit vil tage afsæt i bogen *Thinking, Fast and Slow* af Daniel Kahneman (2012), der kan bidrage til at forklare dele af den adfærd som medarbejdere udviser i forbindelse med forandringer og i dette tilfælde IT-sikkerhed. Derudover giver teorien mulighed for at forklare denne adfærd i forhold til, hvordan folk agerer i givne situationer. Dette kan hjælpe med at forstå samt forklare hvordan denne adfærd kan påvirkes, i dette tilfælde i relation til IT-sikkerhed. Kahneman fremsætter to systemer, der i den sammenhæng er relevante at se på, da han mener de ligger til grund for al menneskelig kognition. De to systemer, som Kahneman kalder *System 1* og *System 2*, har begge hver deres specifikke rolle at udføre:

System 1: ”*Operates automatically and quickly with little or no effort and no sense of voluntary control.*” (Kahneman, 2012 s. 20).

System 2: ”*Allocates attention to the effortful mental activities that demand it, including complex computations. The operations of System 2 are often associated with the subjective experience of agency, choice and concentration.*” (Kahneman, 2012 s. 21).

De to systemer eksisterer side om side i den menneskelige hjerne og hjælper os til at navigere i livet; de er ikke bogstavelige eller fysiske, men konceptuelle. *System 1* agerer som det intuitive system, der ikke kan slukkes for. *System 1* hjælper os med automatisk at udføre de fleste af de kognitive opgaver, som hverdagen kræver, såsom at identificere trusler, navigere os hjemad

kendte veje, genkende venner og så videre. *System 2* derimod kan hjælpe os med at analysere komplekse problemer, udføre større matematiske øvelser og så videre. *System 2* er nyttigt for os, men det kræver en indsats og energi at engagere det (Kahneman 2012).

Ifølge Kahneman er mennesker *Dovne tænkere* (Kahneman, 2012). Mennesker vil gerne hoppe over hvor gærdet er lavest og anvender derfor oftest *System 1*, da det er det system, der kræver mindst af os. Sagt med andre ord, når der skal træffes en beslutning, så arbejder *System 1* i princippet kontinuerligt ud fra vores tidligere erfaringer og ønsker, og det vi ved, helt automatisk, og *System 2* bliver aktiveret, når der opstår en ny situation, eller hvis der kræves en del opmærksomhed og større indsats for at fuldføre opgaven. Selv når *System 2* er aktiveret har det en tendens til at overtage resultaterne fra *System 1* uden ændringer, det vil sige tage afsæt og blive påvirket af de vaner der allerede er etableret. Det betyder, at *System 1* ofte har en stærk indvirkning på *System 2* og de beslutninger der bliver truffet. Yderligere nævner Kahneman, at selv gentagelsen af en løgn kan få folk til at acceptere den, hvis løgnen indebærer information, der er velkendt og *Kognitivt let at bearbejde*, hvilket kan forbindes med at Kahneman ser mennesker som *Dovne tænkere*, hvorfor mennesker derfor er mere tilbøjelige til at tro på noget de kan forholde sig til frem for at de skal forholde sig til et helt nyt emne eller omlægge deres vaner (Kahneman, 2012).

Udover de to systemer benytter Kahneman i relation hertil en række andre begreber, der kan bidrage til at forstå medarbejdernes tankemønstre og i dette speciale i forhold til IT-sikkerhed og de valg, der træffes eller ikke træffes. Kahneman benytter blandt andet begrebet *Priming*, der handler om at mennesker associerer bestemte ord eller situationer med bestemte sammenhænge. I den forbindelse trækker mennesker hele tiden på tidligere erfaringer i forhold til at forstå en situation bedst muligt. Derudover bliver mennesker eksponeret overfor nyheder fra både kolleger, familie, internettet og diverse medier, der på den måde, helt ubevidst, går ind og påvirker den holdning man har om alting. Yderligere benytter Kahneman begrebet *Framing*, der indebærer, hvordan information præsenteres. Ifølge Kahneman er det vigtigt, hvordan information præsenteres i forhold til, hvordan mennesker bedst modtager den samt om de kan forholde sig til den information de bliver præsenteret for. Dette hænger både sammen med om information er *Kognitivt let at bearbejde* og yderligere *Priming* i forhold til hvad mennesker vælger at associere den nye information de har fået præsenteret med (Kahneman 2012).

3.3 Kræmmergaard - Digital modenhed

Følgende afsnit tager afsæt i Pernille Kræmmergaards teori om *Digital modenhed* (Kræmmergaard 2019). Kræmmergaard påpeger, når det kommer til *Digital modenhed*, så er det vigtigt at være opmærksom på, at ingen virksomheder er ens, da de alle står overfor forskellige udfordringer med forskellige udgangspunkter og behov. Det samme gør sig gældende med IT-sikkerhed, hvor virksomhederne ligeledes placerer sig forskelligt. Kræmmergaard fremlægger i hendes teori om digital modenhed en lag-tankegang, hvor der er det nederste, det midterste og det øverste lag (Kræmmergaard, 2019). Det nederste lag skal være solidt, og bestå af de kernesystemer der sjældent ændres. Det er systemer der skal virke og som andre systemer skal integreres med. Det midterste lag af systemer skal bygges ovenpå det nederste lag, og betegnes som værende mere virksomhedsspecifikke. Det vil sige, at det er de interne de interne systemer som er unikke for den enkelte virksomhed og deres behov, og som er tilpasset det nederste lag af kernesystemer. Disse systemer kan, som på det nederste lag, betragtes som solide systemer, dog ikke med samme levetid som i det nederste lag. På det øverste lag findes det der kan betegnes som virksomhedens ansigt udadtil. Det er dette lag af systemer som kunder ser og har en interaktion med. Derudover er det også dette lag, hvor innovationen spiller en rolle, hvor brugere og kunder har mulighed for at komme med deres bidrag til og indflydelse på systemerne og deres anvendelse (Kræmmergaard, 2019). Denne opdeling af lag i forhold til IT-systemer er vigtig at forstå, fordi det nederste lag ikke er holdbart, hvis det som det øverste lag er innovativt og med brugernes indflydelse, modsat kan det øverste lag heller ikke bære den solide struktur der findes i det nederste lag (Kræmmergaard, 2019).

Derudover præsenterer hun fem generationer for *Digital modenhed*, hvor virksomheder kan placeres fra generation 1 til generation 5, alt efter hvor digitalt modne de er (Kræmmergaard, 2019). Kræmmergaard laver en relation mellem lag-tankegangen og generationerne, idet at opbygge de tre lag kræver en vis digital modenhed og struktureret styring af virksomheden. Her må man tænke ud over den tekniske konstruktion, der skal til og derpå også fokusere på en ledelse heraf såvel som en klar ansvarsfordeling i forbindelse med lagene. De tre lag skal integrere og bidrage til hinanden på tværs af lagene således, at virksomheden får en samhørig IT-arkitektur, der både fungerer internt, og samtidig kan forholde og tilpasse sig til omverdenen og eksterne parter i det omfang, der er nødvendigt. Denne kompleksitet er, hvad man igennem

generationsmodellen forsøger at arbejde sig hen imod (Kræmmergaard, 2019). De fem generationer fremgår af tabellen nedenfor:

	Generation 1	**Generation 2**	**Generation 3**	**Generation 4**	**Generation 5**
Formål med IT	Levering af systemer	Levering af solid infrastruktur	Levering af forretningsmæssig værdi	Levering af integrations-muligheder til nye forretningskapabilitater	Levering af kompetente og udfordrende tech-samarbejde (to skridt foran)
IT-kompetencer handler i IT-funktionen om	Hardware, software og telekommunikation	Processer, mennesker og strukturer	Opdukkende teknologier og slutkunder	IT brugertrends, teknologisk stack, arkitekturprincipper og IT-sikkerhed	Domænekendskab og multi-specialist sourcing
Medarbejdere i IT	Systemanalytikere, Håndværkere	Forretningskonsulenter og projektledere	Samarbejdspartnere, initiatorer og facilitatorer	Teknologisk kyndige og arkitekter Relations-, forhandlings- og partnerledelse	Inspirator – ”hvad kan det blive til?” Visualisering, kommunikation og story-telling
Processer omkring IT	Understøtte eksisterende praksis og automatisering	Procesunderstøttelse og gøre eksisterende praksis bedre	IT ind i produkter og services – forbedrede services eller på nye måder	Opfyldelse af slutkundens behov på nye måder – nye forretningsmodeller	IT til styrkelse af stakeholdere ”mulighedsrum” og hyperrelevant services
	Organisationens standarder – silo-arkitektur	Standardsystemer og industristandarder	Tosidet – noget standard andet egen udviklet	Solid ”enterprise platform” samt (åbne) agil ”engagement platform”	Solid back-bone, byggeklodser og moduler som hurtigt kan sammensættes til domænespecifikke ønsker og behov
	Decentraliseret beslutningstagen	Centraliseret beslutningstagen	Føderal beslutningstagen	Todelt (eller flere) beslutningsstrukturer	Multiple beslutningsstrukturer og mange bundlinjer

Tabel 4: Tilpasning af Kræmmergards modenhedsmodel (2019)

Overordnet kan generation 1 og 2 siges at have fokus på effektivisering af arbejdsgangene både internt og eksternt, og dermed have som mål at frigøre ressourcer. Vigtigst af alt for disse er er, at det virker i samspil med den eksisterende forretning, og tingenes nuværende tilstand (Kræmmergaard, 2019).

Generation 3 og særligt 4 og 5 giver IT en anden funktion i virksomheden. Her er fokus ikke længere kun på at optimere og tilpasse eksisterende forhold, men nærmere at anvende IT og

mulighederne det giver til at innovere og nytænke samarbejde både internt og eksternt. IT bliver i højere grad omdrejningspunktet og det afgørende for hvem der bedst passer sammen i et samarbejde og hvilke kompetencer, der er efterspurgt ud fra teknologien. Det bliver dermed en del af virksomhedens kerne, og ikke en adskilt del (Kræmmergaard, 2019). Med andre ord kan generation 1 og 2 betragtes som lav grad af modenhed, mens generation 3 og særligt 4 og 5 kan ses som værende højere digitale modenhed (Kræmmergaard, 2019). I dette speciale laves der en kobling mellem lag-tankegangen og generation 1 til 5 generationer, hvor generationerne bliver koblet på de forskellige lag. Dette betyder, at generation 1 og 2 vil udgøre det nederste lag, generation 3 og delvist 4 vil udgøre det midterste lag, mens generation 4 og 5 vil udgøre det øverste lag.

3.4 Opsummering af teori

Følgende afsnit har til formål at opsummere de valgte teoriers samspil og anvendelighed i relation til hinanden.

Kræmmergaard skal i dette projekt betragtes som strukturen og inspirationen for det rammeværk der skal udarbejdes i dette speciale. Her skal forståelsen omkring *Digital modenhed* i form af de fem generationer sammenkobles med lag-tankegangen, som trækker tråde til opbygningen af det omtalte rammeværk. Derudover ligger der i Kræmmergaards teori også et mere overordnet organisatorisk element, der skal binde hele virksomheden og det øgede fokus på at forbedre IT-sikkerhed sammen. Kahneman tager et mere psykologisk afsæt, da han sætter opmærksomhed på det kognitive aspekt, og er derfor mere adfærdspræget i henhold til psykologien. Kahneman har mere fokus på det enkelte individs adfærd, og hvordan dette er muligt at påvirke, for at kunne lave de nødvendige tilpasninger i virksomheden. Yderligere er der mindre fokus på sociale situationer, hvortil Orlikowski inddrages. Orlikowski tager det modsatte parti af Kahneman ved at tillægge større værdi i forhold til det, der kan ses og observeres af praksisser - der er derfor større fokus på selve interaktionen. Orlikowski har fokus på hvordan teknologi, medarbejdere og IT-sikkerhed skal ses i en større helhed frem for separate isolerede dele.

Kombinationen af Kræmmergaard og Kahneman sætter den psykologiske adfærdsændring i en organisatorisk kontekst. På denne måde kan fokus centreres om at skabe organisatoriske forandringer gennem adfærdsændringer hos de enkelte individer. Orlikowski kan i relation til både Kræmmergaard og Kahneman bidrage med en forståelse for, hvordan både den enkelte medarbejder, men også virksomheden som helhed arbejder i samspil med teknologien, og

hvilken betydning det har for hinanden. Ydermere kan Orlikowskis teori bidrage med en fortolkning af, hvad der sker mellem det enkelte individ og sammensmeltningen med teknologien, når denne relation ændres som følge af blandt andet en ændret adfærd hos medarbejderen, eller en justering af den teknologi der anvendes af medarbejderen. Med andre ord skaber det at koble Orlikowski på Kræmmergaard og Kahneman en forståelse for, hvordan teknologien spiller ind når den organisatoriske kontekst ændres gennem individet.
Samlet set kan de tre teorier placeres under hvert sit fokus som det fremgår af tabel 5. Ovenstående illustrerer, hvordan disse teoriers forskellige fokusområde ikke skal betragtes som en svaghed, der gør det svært at forbinde elementerne, men nærmere en styrke som sikrer, at alle ender og vinkler bindes sammen og belyses. Dette gøres for bedst muligt at kunne udforme et rammeværk, som kan anvendes af flere typer af SMV'er med forskellige arbejdsfunktioner. Teorierne vil således blive rammesættende for analysens struktur, idet alle analysens grundlæggende tematikker vil blive anskuet ud fra de tre teoretiske perspektiver. Derudover skal dette samspil mellem teorierne yderligere bidrage til bedst muligt at kunne besvare problemformuleringen. Med andre ord skal teoriernes forskelligt rettede fokus i denne henseende betragtes som en styrkelse af specialet og dets rammeværk.

Teoretiker:	**Bidrag til specialet:**
Orlikowski	Socioteknisk perspektiv
Kahneman	Adfærdsmæssigt perspektiv
Kræmmergaard	Organisatorisk perspektiv

Tabel 5: Overblik over teoretisk bidrag

4. Analyse og udformning af rammeværk

Analysen har til formål at besvare dette speciales problemformulering:

Hvilken betydning har ledelsen i forhold til IT-sikkerhed, og hvordan kan et rammeværk med fokus på medarbejderadfærd understøtte ledelsen i formålet om at styrke IT-sikkerhed i små- og mellemstore virksomheder?

Analysen er opdelt i to dele og er opbygget således at første del vil fremlægge specialets empiriske resultater, og anden del vil inddrage tidligere gennemgået teori jævnfør afsnit *3. Teori*. Dernæst vil en opsummering af analysens mest relevante fund blive fremlagt med

henblik på at kunne opstille et rammeværk, der kan hjælpe ledelsen i SMV'er med at forbedre deres IT-sikkerhed.

4.1 Del 1 - Empiriske resultater

Første del har et deskriptivt fokus, hvor resultaterne fra interviewene vil blive fremlagt fordelt på forskellige tematikker, der opstilles på baggrund af koderne. De anvendte koder er som tidligere nævnt de tendenser der blev fundet i det førnævnte litteraturstudie jævnfør afsnit *1.3 Problemfelt*, hvortil yderligere to koder er blevet tilføjet fra empirien i dette speciale jævnfør afsnit *2.7.2 Kodning*. Koderne bunder dermed i de tendenser, der blev fundet i litteraturstudiet, der sammen med den indsamlede empiri danner baggrund for de opstillede tematikker i denne analyse. De identificerede tematikker er *IT-sikkerhed som et teknisk fænomen*, *IT-sikkerhed som et psykologisk fænomen* og *IT-sikkerhed som et kulturelt fænomen*. Relationen mellem koderne og de opstillede tematikker kan ses i nedenstående tabel 6. Formålet med tabellen er at give et indtryk af forholdet mellem de forskellige koder og tematikker, da dette vil danne grundlag for den struktur, som videreføres gennem analysen og det endelige rammeværket.

Koder	**IT-sikkerhed som**		
	Teknisk fænomen	Psykologisk fænomen	Kulturelt fænomen
IT-sikkerhed	X		
Adfærd		X	
Træning		X	
Ressourcer			X
SMV'er			X
Ledelse			X

Tabel 6: Empiriske fund koblet til koder

4.1.1 IT-sikkerhed som teknisk fænomen

Tematikken IT-sikkerhed som et teknisk fænomen udspringer primært af koden *IT-sikkerhed* og dækker over de tekniske tiltag i forbindelse med IT-sikkerhed, som eksperterne påpeger, er nødvendige at starte med inden der bygges ovenpå med investeringer af ressourcer,

medarbejdertimer, træning og adfærd. IT-sikkerhed som et teknisk fænomen er i dette speciale en betegnelse for tekniske systemer og applikationer, der bliver implementeret i en SMV som et IT-sikkerhedsmæssigt tiltag, der påvirker medarbejdernes arbejdsgang. Med andre ord er teknisk i denne sammenhæng ikke udvikling eller IT-drift.

I forbindelse med IT-sikkerhed er første skridt at indse, at der er et problem, der skal løses og håndteres i den pågældende virksomhed. En generel tendens, som Krogstrup påpeger, der findes ude i mange SMV'er generelt er af den opfattelse at "*Det sker ikke for mig*" eller "*Det er ikke noget, der kommer os ved*" (Bilag A, s. 1, l. 15-16). Ud fra Krogstrups erfaringer kan man argumentere for, at IT-sikkerhed ikke bliver betragtet som et problem hos ledelsen i SMV'erne, hvilket de er nødt til, før de kan begynde at prioritere det og sætte ressourcer af til det, som ligeledes bliver bekræftet af Pedersen (Bilag A, s. 18). Første skridt er således at indse, at det kan være et problem på mange fronter ude i SMV'erne, hvis de bliver angrebet. Som Krogstrup påpeger, så handler det ikke om hvorvidt man bliver hacket eller ej, men nærmere om hvornår man bliver det (Bilag A, s. 3). Dertil påpeger han yderligere, at det for SMV'erne handler om at betragte IT-sikkerhed ud fra en liste-tankegang, hvor det handler om at ligge så langt nede på listen som muligt:

"*Jeg plejer at sige, at de [virksomhederne] skal se det som, at de ligger på en liste og den liste er der nogle der gennemgår. Hvis ikke de [hackerne] rammer i første hug på den liste, så går de videre til en anden [virksomhed]"* (Bilag A, s. 2, l. 17-18)

Med dette mener Krogstrup, at hvis virksomhederne har den nødvendige IT-sikkerhed, så vil de formentlig ikke blive ramt, og hackerne vil efter et mislykket forsøg gå videre til den næste virksomhed på listen (Bilag A, s. 2). I forbindelse med dette udlægger Wine en pointe om, at det både for medarbejderne samt SMV'er som helhed i forhold til andre ikke handler om at være den dygtigste til IT-sikkerhed, men man skal bare ikke være det svageste led (Bilag A, s. 33). Yderligere påpeger Krogstrup, at det dog kan være svært at indse, hvorfor man skulle blive hacket, når man for eksempel "*Bare er en tømrervirksomhed*", der ikke har noget af værdi når det kommer til IT-sikkerhed (Bilag A, s. 3). "*Selveste data har ingen værdi, men det data de har, det har værdi for virksomheden og det er der, hvor det går galt for så får de ransomware eller de får brudt deres koder*" (Bilag A, s. 2, l. 3-4). Ifølge Krogstrup er det således vigtigt først at afgøre hvilken slags SMV man er i forhold til, hvordan man bedst muligt kan sikre sig mod sikkerhedsbrud. Han mener ikke det er nødvendigt at der investeres i alt muligt unødvendigt, som er økonomisk belastende, hvilket også er det, der går galt for mange af

SMV'erne (Bilag A, s. 2). Der er en forestilling om, at SMV'erne ikke har noget data, som er værdifuldt for hackerne samtidig med, at IT-sikkerhed koster en masse penge, samt arbejdskraft og ekspertise, hvis de skal ud at investere i det. I den forbindelse foretrækker Pedersen, at man i stedet for at starte med at implementere diverse løsninger, går et skridt tilbage, og får et overblik over virksomhedens systemer og forretning i forhold til, hvad der vil være mest kritisk at få hacket. Han foreslår, at der kan laves en risikoanalyse til dette formål, så man kan prioritere forretningen og systemerne i forhold til hvad der er mest kritisk for virksomheden (Bilag A, s. 18). Alsmith bekræfter ligeledes dette med at få styr på hvad der er mest forretningskritisk:

"*Kend deres kerneforretninger, hvad er det for nogle understøttende IT-systemer, er det deres telefon, der er den helt afgørende eller er det deres mailsystem … Hvad er det, der er helt kritisk for at deres forretning kan køre videre, hvis det er de bliver ramt, hvad er det så, der ikke må gå ned?*" (Bilag A, s. 38, l. 28-31).

Når ledelsen i SMV'erne først har indset, at der er et problem i forhold til manglende IT-sikkerhed, er næste skridt derfor at kortlægge hvad de er for en type virksomhed og dernæst, hvad de har af systemer i virksomheden og hvilke, der er de mest forretningskritiske systemer som ikke kan undværes.
Når SMV'erne har indset, at der er et problem og de derudover har fået prioriteret deres systemer i forhold til hvilke, der er mest kritiske for forretningen, argumenterer Pedersen for, at næste skridt vil være at sørge for at alt software er opdatere, og at der er styr på adgange, og det er både brugere inklusiv password og to-faktor godkendelse, styr på leverandører og opdateret antivirus. Dette betegner Pedersen med andre ord som grundlæggende cyberhygiejne, og påpeger at man kan komme rigtig langt med at få styr på dette. Dog påpeger Pedersen, at der inden for IT-sikkerhed ikke er noget, der hedder 100% sikker. Man kan dog stadig godt rykke sig fra at have ingen tiltag og 0% i forhold til IT-sikkerhed til at indføre relativt simple ting og således flytte sig til for eksempel 70-75% (Bilag A, s. 18). Alsmith tilføjer, at et andet element SMV'erne også kan overveje i relation til at opnå bedre IT-sikkerhed er at begrænse medarbejdernes adgang rent teknisk så de ikke har mulighed for at afvige fra den praksis, som medarbejderne godt ved de burde følge og efterleve på arbejdspladsen (Bilag A, s. 39).
Krogstrup påpeger dog, at værktøjer som to-faktor godkendelse er noget alle virksomheder burde have, men at der er mange SMV'er og især de mindre SMV'er som ikke har det fordi de tror det er et irritationsmoment. Dette skyldes ofte, at de har prøvet det på en anden platform

eller i privat sammenhæng og skal godkende noget, hver gang de vil logge ind, hvilket er en grund til mange ikke implementerer det, fordi de synes det er træls at arbejde med (Bilag A, s. 1). Pedersen bekræfter ligeledes dette ved at påpege, at hvis man gør sikkerhed vanskeligt og at intet fungerer ordentligt, så hopper mennesker over hvor det er nemmest og gør det der er mest praktisk for dem, hvilket kan resultere i at fortrolige informationer ligger i et google docs, som andre har adgang til (Bilag A, s. 19). Til dette påpeger Alsmith ligeledes, at det skal besværliggøres at træffe de forkerte valg i modsætning til at gøre det besværligt at handle sikkert, som det ofte forekommer rundt om i SMV'erne (Bilag A, s. 41).

Både Krogstrup og Pedersen mener dog, at det er en lavthængende frugt at implementere to-faktor godkendelse, da det som Krogstrup påpeger "*tager næsten 90% af alle forsøg på at komme ind på en konto, så når man har slået det til, så er man allerede rigtig langt*" (Bilag A, s. 2, l. 38-39). Derudover påpeger Krogstrup, at de fleste SMV'er allerede arbejder med Microsoft og betaler for to-faktor godkendelse, selvom virksomheden måske ikke ved det (Bilag A, s. 3), hvorfor dette vil være et godt sted at starte. Pedersen påpeger dog, at det er en menneskelig ting ikke at få slået to-faktor godkendelse til, selv for ham, der prædiker om at slå to-faktor godkendelse til indså først efter 50 interviews om emnet, at han blev nødt til at få sat sig ned og få det gjort (Bilag A, s. 20). Der er således nogle konkrete udfordringer ved IT-sikkerhedstiltag, der blandt andet ses ved to-faktor godkendelse. Pedersens erfaringer indikerer, at hvis man giver medarbejderen et frit valg om hvorvidt de vil have to-faktor godkendelse eller ej, så er det meget sandsynligt, at langt størstedelen ikke vil få det slået til. Pedersen påpeger i den forbindelse at tvang fra ledelsens side kunne være en løsning. Han mener, at man bliver nødt til at indføre politikker og regler for at få bestemte systemer igennem og for at folk aktivt bruger dem (Bilag A, s. 21). Pedersen nævner dog også, at dialog mellem medarbejdere og ledelse er nødvendigt for at undgå at skabe modstand (Bilag A, s. 21). Krogstrup pointerer dog, at man ikke kan have god sikkerhed uden at begrænse brugeren i et vist omfang, da den kombination er umulig at praktisere. Med andre ord, hvis der er fuld frihed til brugeren, så har man ikke IT-sikkerhed, men har man IT-sikkerhed, så kan brugeren ikke have fuld frihed (Bilag A, s. 16).

4.1.2 IT-sikkerhed som psykologisk fænomen

Tematikken IT-sikkerhed som psykologisk fænomen udspringer primært af koderne *Adfærd* og *Træning* og herunder awareness. Tematikken dækker de psykologiske aspekter, der er forbundet med IT-sikkerhed og medarbejderne i en SMV i forhold til, hvordan de benytter og

forholder sig til IT-sikkerhed i deres daglige arbejde. I interviewene blev det fremlagt, at der ude i SMV'erne er en generel tendens til, at awareness og adfærd tit blev to sider af samme sag, hvilket eksperterne er uenige i. De påpeger derimod, at awareness og adfærd langt fra er det samme. Alsmith beskriver det blandt andet således:

"*Og så tror jeg rigtig mange ude i både SMV'erne og de større organisationer og myndigheder, de har ikke den her skelnen som vi ofte drøfter med en ting er viden og en ting er handling. De taler awareness og adfærd og kultur i en stor sammenblanding og ser det som én ting og har ikke den der skelnen*" (Bilag A, s. 43-44, l. 37-2).

Alsmith påpeger altså, at denne tendens både ses hos SMV'er, men også hos større virksomheder og påpeger yderligere, at man burde skelne mellem awareness, adfærd og kultur, idet det er vigtigt at få klarlagt, hvad det er for et problem, der rent faktisk skal løses af de tre ude hos virksomhederne (bilag A, s. 44). Til dette påpeger Wine yderligere, at awareness træning bidrager til at medarbejderne ved hvad de skal gøre, men ofte har medarbejderne svært ved rent faktisk at udføre det i praksis (Bilag A, s. 26). Pedersen bekræfter ligeledes Wines pointe ved at påpege, at awareness er at man ved hvad man skal gøre og opførsel er at man rent faktisk gør det (Bilag A, s. 19). Pedersen påpeger dog yderligere, at han anser awareness træning som noget af det letteste en virksomhed kan gøre. Til dette tilføjer han, at han også synes det er meget lettere end at skulle kortlægge og få et overblik over de systemer man har i sin virksomhed og vurdere dem i forhold til risici (Bilag A, s. 23). Med dette mener Pedersen, at det er den lette udvej for virksomhederne at købe en awareness kampagne med tegnefilm og vise til medarbejderne og betragte IT-sikkerhed som et område der i den forstand er skabt fokus på (Bilag A, s. 23). I forhold til awareness så påpeger Pedersen dog, at medarbejderne i virksomhederne også spiller en større rolle:

"*Man taler jo altid om at awareness er en del af et godt cyberforsvar, så man kan sige, at medarbejderne er den største trussel eller man kan sige, at medarbejderne er first line of defense. Det er lidt hvordan man vender det, men det er klart at det er vigtigt*" (Bilag A, s. 19, l. 7-9)

Som citatet antyder, så kan medarbejderne betragtes som en virksomheds første forsvar. Han påpeger dog også at man kan vende den rundt og se det fra den anden side, og se medarbejderne som den største trussel, da det i mange tilfælde er hos medarbejderne at de fleste sikkerhedsbrud

sker, idet medarbejdere ofte er ofre for social engineering, der er en betegnelse for ondsindede aktiviteter, der udføres gennem menneskelige interaktioner såsom phishing mails (Bilag A, s. 19). Krogstrup påpeger ligeledes, at et af de mest effektive tiltag mod social engineering er at uddanne medarbejderne i awareness kampagner, da det ofte er dem, som er udsat for ondsindede angreb. Dette uddyber han med, at i langt de fleste forsøg på social engineering, som en SMV er udsat for, går det galt for SMV'en fordi en medarbejder er kommet til at klikke på et link de ikke skal klikke på, eller overføre penge til nogen de ikke skulle overføre penge til. Alligevel sker det, at medarbejderne ender i førnævnte situationer, på trods af, at de er uddannet i diverse awareness kampagner og godt ved, hvordan de skal reagere herpå, men fordi phishing-angrebet er opført som om det er direktøren, der har en vis autoritet, så ender medarbejderen alligevel med at falde for angrebene på trods af viden herom. Det kan med andre ord være svært at gennemskue et angreb selv med awareness kampagner (Bilag A, s. 4).
En af grundene til, at det kan være svært for medarbejdere at forholde sig awareness træning kan være fordi tiltaget stadig er forholdsvis nyt, som Wine påpeger i sit interview. I den forbindelse pointerer hun yderligere, at hun ikke kender andre end Cyberpilot, hvor hun arbejder til dagligt, der beskæftiger sig med awareness træning i forbindelse med IT-sikkerhed (Bilag A, s. 30+36).
Selvom SMV'erne træner medarbejderne til at få den ønskede viden og giver dem de værktøjer, der kræves for at handle korrekt i forbindelse med IT-sikkerhed, så er det også vigtigt at de tager deres forbehold når awareness træningen skal udføres. Dette påpeger Krogstrup med pointen om, at et system som Outlook bliver medarbejderens største fjende:

"Det er i hvert fald vigtigt fra virksomhedens side af at de forstår, at det er et træningsværktøj [awareness træning] og det er noget, der er til stede for at de kan hjælpe hinanden [medarbejderne] med at blive bedre til IT-sikkerhed, for når først du får sådan en awareness træning, jamen så panikker du fuldstændig hver gang, der kommer en mail, der ikke bare ligner noget, altså hvis bare der et punktum forkert, så bliver de jo bekymret, så det er vigtigt at sige og lægge vægt på at det er en proces" (Bilag A, s. 10-11, l. 39-4).

Krogstrup påpeger således, at træningsværktøjer er noget, der er til stede for at hjælpe medarbejderne, men det er en proces, da det medarbejderne lærer gennem træningsværktøjet, er noget, der skal bruges aktivt i deres daglige arbejde for at det hænger ved. I denne forbindelse drager Krogstrup en parallel til uddannelse, hvortil han påpeger, at hvis man ikke bruger det man har lært fra sin uddannelse aktivt, så ryger det bare ind ad det ene øre og ud af det andet

(Bilag A, s. 11). Der er således et behov for at omdanne den opnåede viden til praksis for at vedligeholde denne. I den henseende er træningsværktøjer som awareness kampagner ikke meget anderledes end uddannelse, da de på samme måde har til formål at oplyse og give viden om et bestemt emne, der i denne kontekst er om IT-sikkerhed. Denne pointe bekræfter Pedersen ligeledes, da han påpeger at awareness falder relativt hurtigt igen efter man er blevet gjort opmærksom på det, hvorfor man hele tiden skal have det in mente, hvortil han på lige fod med Krogstrup drager samme parallel til uddannelse (Bilag A, s. 22). Ud fra ovenstående kan det dermed udledes, at kontinuerlighed er et vigtigt element i forhold til både at skabe og fastholde awareness, hvorfor SMV'erne ikke bare kan nøjes med at investere i en awareness video, vise den til sine medarbejdere en gang og derefter regne med at de ved alt om IT-sikkerhed.
Et vigtigt element i relation til træning er som tidligere nævnt medarbejdernes adfærd i relation til dette, som handler om hvordan medarbejderne omdanner den viden de har om IT-sikkerhed til en matchende adfærd, der mindsker SMV'ernes risiko for IT-sikkerhedsbrud. Alsmith påpegede i sit interview at medarbejderne skal have noget viden og noget læring, før der kan fokuseres på ændring af den reelle adfærd. Med andre ord er der tale om de faktiske handlinger og ikke hvad medarbejderne ved eller hvad deres intentioner er, men hvordan de rent faktisk udfører, anvender og handler på den viden og de kompetencer, som de har opnået gennem eksempelvis awareness kampagner og hvordan det gøres i en travl hverdag med deadlines og forstyrrende elementer (Bilag A, s. 42). I forbindelse med dette påpeger Pedersen:

"*Jeg tror at man skal være meget opmærksom på, at der er meget stor forskel på awareness og på opførsel og det er opførsel vi skal ramme. Hvis du laver en rundspørge om hvor mange der ved at de ikke skal bruge samme password flere forskellige steder så ved de fleste godt at de ikke skal. Og når du så laver en rundspørge på, hvor mange der gør det, så gør de fleste det alligevel*" (Bilag A, s. 19, l. 14-18).

Pedersen påpeger, at det er opførslen og adfærden vi skal ramme for selvom medarbejderne ude i SMV'erne allerede er opmærksomme på og har viden om, hvad de skal gøre, så er det faktisk langt fra størstedelen der gør det i praksis (Bilag A, s. 19). Til dette tilføjer han yderligere, at mennesker overvurderer sandsynligheden for, at ting går godt, og undervurderer sandsynligheden for, at ting går galt. Pedersen påpeger yderligere hertil at medarbejderne ofte godt ved hvad der bør gøres anderledes, men ikke får gjort noget ved det fordi de tænker, at "*Det sker jo ikke for os"* (Bilag A, s. 19). Denne pointe kan ligeledes bekræftes af Krogstrup, idet han påpeger at mange ikke får implementeret IT-sikkerhedstiltag, da de som tidligere

nævnt har en tankegang der hedder, at det ikke sker for dem, de bliver ikke angrebet (Bilag A, s. 1). Som en løsning på disse adfærdsudfordringer nævner Pedersen, at ledelsen skal indføre tiltag på et niveau, som dækker hele virksomheden, hvortil mellemledere skal sørge for at medarbejderne er motiveret og følger disse tiltag (Bilag A, s. 23).
I forbindelse med ovenstående kan der findes flere grunde til, hvorfor medarbejderne ikke udfører korrekt IT-sikkerhedsadfærd, hvilket som tidligere nævnt både kan indebære at de ikke synes det er vigtigt, at de tror, at det ikke sker for dem eller på grund af det som Wine kalder IT-stress og neutralization. Termerne IT-stress og neutralization taler ind i, at medarbejder modtager mere information end de kan kapere. De to sidstnævnte termer beskriver hvorfor medarbejderne har svært ved at tage deres viden om IT-sikkerhed i brug i hverdagene selvom de godt ved hvad de skal gøre (Bilag A, s. 26).
Alsmith er af den holdning, at der er et øget fokus på forståelse og inddragelse af medarbejdere hvilket er en positiv ændring. Dog mener hun også at de awareness tiltag der er i SMV'erne på nuværende tidspunkt i form af mails, posters og den nuværende tilgang til medarbejderinddragelse kun kan løse viden- og opmærksomhedsproblemet, men ikke skabe en konkret forandring inden for IT-sikkerhed. Alsmith påpeger, at hvis der er tale om reelle adfærdsproblemer, så er det nogle andre værktøjer der skal til end bare mere information og flere awareness kampagner (Bilag A, s. 39):

"*Vidensdeling, informationskampagner og decideret træning - det ser jeg som et vigtigt trin, men det er bare ikke nok til at ændre adfærden (…) Det er det her med at få identificeret, hvad det er for et problem vores tiltag skal løse, hvilket sådan set er ret banalt, men vi ser organisationer, som idégenerer og kommer med alle mulige tiltag, men uden at de er helt skarpe på, hvad det er for et problem de har. Så jeg synes det er vigtigt at få identificeret hvad det er medarbejderne mangler og hvad det er, der er problemet*" (Bilag A, s. 42, l. 9-20).

Alsmith påpeger at det handler om, hvad det er for et konkret problem, der skal løses og derudover, hvilke kompetencer medarbejderne mangler. Hun benævner mere præcist at hvis der er et behov for yderligere kompetencer til at opdatere sin computer eller lave et stærkt password fordi man ikke ved hvad det indebærer, så er det træning og vidensdeling, der skal indføres der skal indføres, men kan medarbejderne allerede finde ud af det, så er det andre tiltag, der skal til (Bilag A, s. 42). Yderligere har hun også erfaret at, hvis man gerne vil arbejde med en specifik adfærdsændring, så prøver hun i hvert fald at rådgive til at tydeliggøre over for ledelsen, at der skal afsættes tid, ressourcer og medarbejder til det, idet det er tungt og det

tager lang tid at få ændret adfærd. Der er ikke en hurtig og let løsning. Alsmith mener derfor at hvis der ønskes en adfærdsændring så skal der sendes et budskab til ledelsen om at det tager lang tid og det kræver en del ressourcer. Ydermere påpeger hun, at det måske er ressourcerne og tiden værd, idet mange IT-sikkerhedsbrud, som Pedersen også tidligere påpegede, skyldes menneskelige fejl og derudover understreger hun også vigtigheden af, at der er ledelsesmæssige opbakning, ellers kan det ikke betale sig (Bilag A, s. 41). Pedersen har dog en vigtig pointe, om at mennesker altid vil begå fejl og derfor får man ikke noget, der er fuldstændigt fejlfrit selvom medarbejderne ændrer adfærd, dog påpeger han stadig at det er en vigtig del af en IT-sikkerhedsstrategi. Pedersen er fortaler for, at man skal forsøge at lave teknologier, der kan understøtte at mennesker ikke laver fejl, så det ikke får fatale konsekvenser (Bilag A, s. 19). Krogstrup fremlægger i sit interview et tiltag, der kan tages i brug for at mindske menneskelige fejl i forbindelse med phishing angreb, der indebærer at SMV'er er begyndt at implementere, at alle mails, der ikke har virksomhedens navn i deres e-mail bliver blokeret når der bliver kommunikeret internt i virksomheden. Det vil sige, at hvis der kommer en e-mail, der indeholder Gmail i stedet for virksomhedens navn, så vil den ende i spam (Bilag A, s. 5). Dette kan på mange områder hjælpe medarbejderen i forhold til ikke at skulle sortere sine mails og bruge unødvendige ressourcer eller være bekymret for at begå fejl ved at falde for en phishing mail. Dette kan ligeledes relateres til Alsmiths pointe om at begrænse medarbejdernes adgang jævnfør afsnit *4.1.1 IT-sikkerhed som teknisk fænomen.*

4.1.3 IT-sikkerhed som et kulturelt fænomen

Tematikken IT-sikkerhed som et kulturelt fænomen udspringer primært af koderne *Ressourcer*, *SMV'er* og *Ledelse*. Tematikken dækker over de fænomener, der er ved kontinuerlig videreførelse af IT-sikkerhedsmæssige tiltag og politikker, vedligeholdelse af medarbejdernes adfærd i forbindelse med IT-sikkerhed samt investering af ressourcer som økonomi og medarbejdertimer.

Wine nævner, at der ligger meget mere i en kulturændring end bare IT-sikkerhed (Bilag A, s. 35). I den forbindelse kan der drages en parallel til interviewet med Alsmith, hvor der blev spurgt ind til hvordan medarbejderne kan lære af hinanden i forhold til at opnå et højere IT-sikkerhedsniveau, hvor hun påpeger at det taler ind i et lidt bredere kulturbegreb:

"*Det taler jo sådan ind i et lidt bredere kulturbegreb kan man sige, hvor der ligesom er en kultur for at vidensdele (…) at der ikke er sådan en nul-fejls-kultur, men at man må spørge,*

hvis ikke man ved eller får en phishing mail og man er i tvivl, jamen så kan man godt lige spørge sin kollega eller IT-medarbejdere, altså er den her god nok eller kunne det være en phishing mail? Det taler ind i sådan en helt anden form for, at vi skal have løftet kulturen og at cybersikkerhed også er noget man kan have på dagsordenen, så at det bliver talt naturligt ind i et projekt, i udvikling og så videre" (Bilag A, s. 40, l. 15-21).

Alsmith påpeger, at der skal være plads til at begå fejl og der skal være plads til at være uvidende, selvom man måske allerede har gennemgået et awareness-program - der skal være plads til at være i tvivl. I forlængelse af dette pointerer hun også, at der er en ledelsesmæssig forankring, der er essentiel, hvis det skal fungere med IT-sikkerhed for, hvis ledelsen ikke tænker IT-sikkerhed som noget vigtigt i kulturen og i virksomheden, så bliver det svært rent faktisk og få implementeret som noget kulturelt i virksomheden (Bilag A, s. 40).
Krogstrup lægger dog vægt på, at det kan svinge rigtig meget fra virksomhed til virksomhed i forhold til at skabe en kultur for IT-sikkerhed. Han gør opmærksom på, at hvis man er i en lille virksomhed, hvor alle sidder inde på det samme kontor, så er det lettere at prikke en kollega på skulderen, som man måske lige har fået en mail fra og få bekræftet, hvorvidt det er en phishing mail eller ej (Bilag A, s. 5). Som Krogstrup yderligere påpeger:

"*Jeg tror, at man skal lære det fra nogle andre og så skal man fra medarbejderens side have en kultur om, at man skal være rigtig god til at være obs på hinandens mail og hinandens oplysninger så man er lidt bedre til at gå hen til en kollega og sige 'hallo, hvad er det her' eller sende den [mailen] til deres IT-afdeling … Jeg har terpet de steder jeg har været før, der har jeg terpet, at hvis i bare er det mindste i tvivl jamen så send den [mailen] til mig eller til en af de andre, så kan vi jo hurtigt se i løbet af 5 sekunder om det her er en phishing mail eller noget der er dårligt i stedet for bare at tænke jamen det her er nok rigtig og så trykke besvar*." (Bilag A, s. 5 l. 16-23).

Ud fra Krogstrups pointe kan man argumentere for, at det er nødvendigt, at der i SMV'erne bliver oparbejdet en kultur, hvor en medarbejder eksempelvis ved modtagelse af mails altid er opmærksomme på, at der kan være en risiko for, at det er phishing. Alsmith og Krogstrup er dermed enige om, at der skal opbygges en kultur, der fordrer, at man kan spørge sin kollega, hvis man er den mindste smule i tvivl. Derudover skal der være mulighed for at kunne sende mailen til virksomhedens IT-afdeling, hvilket særligt i de SMV'er hvor medarbejderne sidder på spredte lokationer, kan være effektivt da de i disse tilfælde ikke bare kan spørge sidemanden

eller fysisk gå ned til IT-afdelingen (Bilag A, s. 5). Hertil bidrager Wine yderligere med en pointe om, at et element, der kan tilføjes i afdelingernes ugentlige møder, kan være IT-sikkerhed, hvilke problemer medarbejderne har oplevet, hvad de synes om det nyligt overståede kursus, advarer hinanden hvis man selv har modtaget en phishing-mail, så man gør ens kollegaer ekstra opmærksomme og så videre. Det handler ifølge hende om at have sikkerhed på hjernen (Bilag A, s. 29). Derudover påpeger Wine, at behovet for IT-sikkerhed bare er blevet vigtigere, hvortil hun drog paralleller til at ransomware ude hos virksomhederne var enormt høj og at yderligere en høj procentdel af dem var blevet nødt til at lukke på baggrund af det. I den forbindelse påpeger Wine yderligere, at ud fra det hun forstår, så er IT-sikkerhed bare blevet en vigtigere ting og det kan være farligt for virksomheder, hvorfor det i hendes øjne vil give mening, at man har det som en del af sin strategi, at man vil ændre sin kultur, arbejdskultur, til en god IT-sikkerhedskultur, hvilket hun påpeger kunne give god mening (Bilag A, s. 29). Alsmith påpeger dog, at en fejl som hun tror bliver begået i mange SMV'er er, at IT-sikkerhed bliver en del af virksomhedens strategi fordi en ledelsesgruppe har været på workshop og fået den gode idé om, at det er nødvendigt at gøre IT-sikkerhed til en del af strategien. I den forbindelse påpeger Alsmith, at medarbejderne i så fald ikke kan se nogen mening med eller har noget ejerskab over IT-sikkerhedstiltagene, da det blot bliver et element i deres bekendtgørelse, hvilket ikke er meget værd (Bilag A, s. 41). Krogstrup italesætter ligeledes hvor vigtigt sikkerhedspolitik er, og det manglende ejerskab fra ledelsen i relation til disse sikkerhedspolitikker. Han påpeger, at politikerne ofte bliver udformet på baggrund af en revisor, der har sat som krav at de skulle udformes, og derefter er politikerne aldrig blevet revurderet. SMV'erne er ifølge Krogstrup nødt til at følge op på om det for eksempel fortsat er minimum otte karakterer med tegn og tal der er relevant i forbindelse med at lave en adgangskode eller om det har udviklet sig til andre tiltag som to-faktor godkendelse eller lignende (Bilag A, s. 12).

Yderligere peger Wine på, at den ideelle IT-sikkerhedskultur ofte gør, at folk har værktøjerne til at kunne følge retningslinjerne. I forlængelse heraf nævner Wine, at hun sammen med Cyberpilots kunder har snakket om, hvad den ideelle IT-sikkerhedskultur er og i den forbindelse, at der var nogle *core-elementer,* der skulle være på plads, hvortil en IT-sikkerhedspolitik var det vigtigste punkt. En god IT-sikkerhedspolitik skal i den forbindelse være nem at gå til, den skal være formuleret kort og præcist på omkring en side, den skal indebære de ting, som medarbejderne skal huske i deres hverdag når de anvender diverse enhed og så skal de vide hvor de kan finde den henne. Derudover er et særligt kritisk element i IT-sikkerhedspolitikken også, den er nem at forstå (Bilag A, s. 26). Krogstrup gør dog opmærksom

på, at mange af de steder han kommer og rådgiver, der har de ikke en IT-sikkerhedspolitik, hvilket Wine også har oplevet som værende et vigtigt element for SMV'erne. Derudover pointerer Krogstrup også, at SMV'erne heller ingen strategi har for deres IT-sikkerhed. Det vil sige, at de ikke har noget om, hvordan medarbejderne skal agere og forholde sig til disse ting, hvilket er grundsten og rettesnor for, at man holder medarbejderne op på, at de rent faktisk gør det, der står skrevet. Krogstrup mener, at alle SMV'er bør have et dokument til nye medarbejdere, der fortæller hvordan man skal agere indenfor IT-sikkerhed, men det er der ikke nogen, der har (Bilag A, s. 9).

Derudover indikerer Krogstrup, som Alsmith også har pointeret, at det er en proces, der tager tid, især når du implementerer IT-sikkerhed, idet at lige så snart man går ind og påvirker brugerens arbejdsgang, så vil man altid få noget modstand, da man går ind og ændrer, på noget folk har gjort i 20 år, hvilket han dertil påpeger også er kultur (Bilag A, s. 14). I denne henseende pointerer Krogstrup at mange unge allerede kender til tiltag som to-faktor godkendelse fra deres uddannelse. Ud fra denne erfaring kan det udledes at kulturen om bedre IT-sikkerhed langsomt bliver en mere naturlig del af medarbejderens tilgang til at gå på arbejde og dermed bliver forbedret i takt med at disse unge kommer ud på arbejdsmarkedet med en større kendskab til IT-sikkerhedstiltag.

Et andet element der er fundet i forbindelse med IT-sikkerhed som et kulturelt problem er, at en af de vigtigste roller når det kommer til at skabe en IT-sikkerhedskultur i SMV'er er ledelsen. Dette skyldes blandt andet at de kan sætte emnet på dagsordenen og skabe fokus herpå. Både Krogstrup og Pedersen understøtter dette ved deres enighed om, at awareness træning er noget, der skal gøres en indsats omkring for at holde ved lige. Til dette foreslår Krogstrup:

"*Lav et IT-sikkerhedstjek en gang om året, få lavet noget awareness træning og få det lagt ind i din strategi, få det ind i dit årshjul osv. for at være sikker på, at du holder ved - for det er også der, at det går galt med mange virksomheder, der taget steppet. Så investerer de måske 50-100.000 i awareness campaigns, får lavet et lille sikkerhedstjek på deres hjemmeside og deres interne netværk og siger, jamen det er egentlig ikke så galt og så gør de ikke mere ved det og kører videre."* (Bilag A, s. 10, l. 4-9).

Krogstrup fremlægger i citatet tydeligt, hvor det går galt i SMV'erne og hvorfor de alligevel kan blive udsat for et hackingangreb. Der ligger ifølge ham således en vigtig rolle for ledelsen i forhold til at få IT-sikkerhed på virksomhedens dagsorden og inkorporeret i strategien. Dette

fordi IT-sikkerhed er en dynamisk størrelse, der hele tiden ændrer sig og derfor kan der nå at ske meget på et år eksempelvis på det interne netværk, som Krogstrup påpeger i citatet (Bilag A, s. 10). Det er derfor vigtigt, at ledelsen tager højde for, og undersøger, om deres systemer løbende er blevet mere sårbare i takt med, at hackerne er blevet klogere, og teknologien har ændret sig. Denne pointe understøtter Wine yderligere, idet hun påpeger at det er vigtigt at opnå opbakning fra ledelsen i forhold til at indføre IT-sikkerhedsmæssige tiltag og få sat det på agendaen (Bilag A, s. 26).

Pedersen påpeger yderligere et ansvar, der ligger hos ledelsen, idet han tror, at man skal sammentænke awareness med politikker. Derudover bør awareness træning samtidig tage udgangspunkt i virkeligheden, hvilket handler om at ledelsen lærer og snakker med sine medarbejdere om, at man eksempelvis ikke har filer liggende forskellige steder, men i stedet sørger for at lære medarbejderne, hvad de så skal gøre og hvad for nogle systemer de skal bruge. Pedersen mener ikke, at awareness træning behøver at være omfattende, men at det bør tage udgangspunkt i virkeligheden og at man ikke bare opstiller en politik og regner med at folk opfører sig efter den (Bilag A, s. 24). Der ligger dermed en ledelsesmæssig opgave i forhold til at få formidlet retningslinjer ud til medarbejderne og fortælle dem om, hvordan de bør overholdes og udføres, hvortil dette kan antages at gøres både i form af guides på mails eller i en overordnet sikkerhedspolitik eller ved informationsmøder, hvor man snakker tingene igennem og kan stille spørgsmål.

Et andet ledelsesmæssigt tiltag, hvorpå IT-sikkerhedsmæssige retningslinjer også vil kunne indføres er ifølge Alsmith ved at sidemandsoplære:

"*Ja, jeg tror måske bare at især hos SMV'erne ses det, at strategi er noget, der bliver nedskrevet af sådan en ledelsesgruppe på en workshop og medarbejderne kender den derfor ikke eller har ejerskab over den, hvilket ikke er meget værd. I de større og mere strukturerede organisationer, der indgår cybersikkerhed i et onboarding program og det ses ofte at mennesker er lidt mere åbne overfor nye tiltag og vaner, idet man er opsat på at gøre det rigtige og tænke det ind i den nye organisation. SMV'er har nok ikke sådan et decideret oplæringsprogram men så kan man sige sidemandsoplæring, hvor man ligesom har det med, som noget der skal italesættes og altså vises hvordan gør vi her*" (Bilag A, s. 41-42, l. 32-5).

Alsmith påpeger, at mange SMV'er ikke har et konkret oplæringsprogram, hvortil en løsning kunne være at have en kollega, hvormed man kan italesætte og vise, hvordan man gør i bestemte situationer i forhold til IT-sikkerhed. Dette stemmer dermed overens med Krogstrup,

som også argumenterer for vigtigheden af sikkerhedspolitikker i onboarding processen. Når først medarbejderne er faldet til, så glemmes alt om sikkerhedsprocesser, hvis ikke de er indlagt fra start (Bilag A, s. 12). En ledelsesmæssig opgave er derfor også at tænke bredere i forhold til at indføre IT-sikkerhedsmæssige tiltag, da det kan være en idé at få indført tiltag så hurtigt som muligt, når man introducerer nye medarbejdere til virksomheden, idet det kan antages at nye medarbejdere allerede regner med at det er en del af virksomhedens retningslinjer. I forhold til sidemandsoplæring, som Alsmith påpeger, kan dette tiltag være en alternativ løsning, hvis ikke, der er ressourcer til et dedikeret onboarding program med fokus på IT-sikkerhed for nye medarbejdere. Sidemandsoplæring kan være en god løsning, idet den medarbejder, der skal oplære den nye medarbejder, kan antages at ville tage ejerskab over processen og vise sig selv og virksomheden fra sin bedste side og dermed udvise den korrekte IT-sikkerhedsmæssige adfærd. Omvendt er det sandsynligt at den nye medarbejder vil regne med, at det er sådan man gør i virksomheden i forhold til at være sikker og derfor være mere åben overfor nye tiltag, idet man som ny gerne vil leve op til de krav der er i den pågældende SMV.

4.2 Del 2 - Teoretisk analyse

Anden del af analysen vil tage udgangspunkt i de tematikker, der blev præsenteret i forrige analyse: *IT-sikkerhed som et teknisk fænomen*, *IT-sikkerhed som et psykologisk fænomen* og *IT-sikkerhed som et kulturelt fænomen*. Hertil kobles relevant teori med det formål at skabe en dybere forståelse af de problematikker, som eksperterne fremlægger i interviewene. Denne forståelse er et centralt element for at kunne opstille et værktøj, der kan bidrage til at forbedre IT-sikkerheden i SMV'er.

4.2.1 Orlikowski

Følgende afsnit har til formål at gennemgå de tre ovenfor fremlagte tematikker i relation til Orlikowski og hendes tilhørende teori jævnfør afsnit *3.1 Orlikowski - Entanglement in practice*. Dette gøres i de opdelte tematikker, hvortil pointerne fra den fremstillede empiri trækkes ned og sættes i relation til den anvendte teori.

4.2.1.1 IT-sikkerhed som et teknisk fænomen

Ud fra første tematik, *IT-sikkerhed som et teknisk fænomen*, blev det klarlagt, at tekniske IT-sikkerhedsmæssige tiltag overvejende var lavthængende frugter i forhold til at højne sin IT-

sikkerhed, hvilket kan betegnes som *Cyberhygiejne* i praksis tale ifølge Pedersen jævnfør afsnit *4.1.1 IT-sikkerhed som et tekniske fænomen*. Dette fokus på teknologi taler blandt andet ind i Orlikowskis begreb *Entanglement in practice*, hvilket er et perspektiv, der betragter relationen mellem det materielle og sociale som vigtigere end aktørerne i sig selv. Igennem teorien betyder dette med andre ord, at det er gennem handling, at der bliver formet en betydning. Det vil sige, at de IT-sikkerhedsmæssige tiltag, der bliver foretaget ude i SMV'erne i relationen til medarbejderne, der bruger disse IT-sikkerhedsmæssige tiltag i deres hverdag, bidrager til den arbejdspraksis, hvori medarbejderen og teknologien indgår i. I specialet vil IT-sikkerhed blive betragtet som en praksis, hvori både medarbejderne, teknologien de benytter, samt den virksomhed de indgår i, påvirker, hvordan medarbejderne betragter og ser på IT-sikkerhed. De tekniske tiltag, der bliver foretaget i en virksomhed som eksempelvis to-faktor godkendelse, der blev nævnt som eksempel i interviewene, vil derfor ikke skulle betragtes som et enestående fænomen, uafhængigt af sammenhængen til de medarbejdere, der skal benytte tiltaget. Det er derfor vigtigt at tage højde for medarbejderne og de forhold, der gør sig gældende for de jobfunktioner, som medarbejderne besætter. I relation til sammenhængen mellem de tekniske tiltag og medarbejderens jobfunktioner er det vigtigt at have in mente, at denne sammenhæng skal tilpasses medarbejdernes daglige arbejde, idet de tekniske tiltag ikke skal blive et forstyrrende element for medarbejderne. Eksempelvis tjener det ikke et større formål at implementere tekniske tiltag, der advarer medarbejderne om at være opmærksomme på, eller forhindrer dem i at åbne bestemte mails, hvis deres jobfunktion indebærer at tjekke mails og opretholde gode relationer, idet arbejdsfunktion og IT-sikkerhedstiltag modarbejder hinanden. Dette kan dermed være med til at skabe irritationsmomenter for medarbejderne, og de kan være imod at bruge fremtidige IT-sikkerhedsmæssige tiltag, idet hverdagen bliver mere besværlig for dem. I stedet bør der skabes en forståelse for, hvor meget handlekraft individet bør have i deres arbejde som aktør modsætningsvist de tekniske tiltag som aktør. Denne relation mellem medarbejderne, arbejdspladsen og den teknologi, der bliver implementeret som IT-sikkerhedstiltag kan i forhold til konflikten mellem IT-sikkerhedstiltaget og medarbejderens arbejdsfunktion medvirke til at skabe negative meninger for medarbejderne i forhold til materialiteten, der i denne sammenhæng vil være IT-sikkerhedstiltaget. I denne sammenhæng bør der derfor ses på medarbejderne og de jobfunktioner, der indgår i SMV'en således at IT-sikkerhedsmæssige tiltag ikke blot bliver irriterende og til sidst ignoreret, men rent faktisk bidrager til den praksis, som er nødvendig for at nedsætte angreb på virksomheden og mindske sårbarheder.

En anden tendens, der blev fundet under IT-sikkerhed som teknisk fænomen var tvang. Tvang blev en omdiskuteret pointe, idet Pedersen mener at nogle tiltag i forbindelse med IT-sikkerhed er nødvendige at indføre med tvang, hvilket vil sige, at medarbejderen ikke har frihed til at handle efter egen overbevisning, når det kommer til at benytte et IT-sikkerhedsmæssigt tiltag. God IT-sikkerhed blev derfor nævnt som en praksis, der er umulig at udføre uden brugen af tvang, idet man fra ledelsens side bliver nødt til at indføre forskellige tiltag, der er nødvendige for at beskytte virksomheden. Denne forståelse taler ind i sociomaterialiteten i Orlikowskis teori i forhold til at både teknologien, IT-sikkerhed, påvirker medarbejderne, men omvendt, så påvirker medarbejderne også den måde, der bliver udøvet IT-sikkerhed på i virksomheden. Med andre ord, idet et IT-sikkerhedstiltag bliver indført, som eksempelvis to-faktor-godkendelse, i virksomheden, så påvirker tiltaget medarbejderne i forhold til deres daglige arbejde og medarbejderne danner i interaktionen eller i relationen hermed en mening om tiltaget. Men medarbejderne påvirker omvendt også IT-sikkerhedstiltagene, idet de benytter tiltaget, selvom det er med tvang fra virksomhedens side. I denne sammenhæng vælger medarbejderne stadig at møde på arbejde, hvilket betyder, at de er med til at opretholde de institutionelle rammer, arbejdspladsen, idet de møder på arbejde. Det vil dog kunne diskuteres, hvorvidt denne frihed som medarbejderen har i forhold til at møde på arbejde, er frivillig eller underlagt andre praksisser, der påvirker denne relation.

En praksis, der yderligere kan spille ind i forhold til tvang, er den måde, hvorpå ledelsen udgør ledelsespraksissen i forhold til implementeringen og præsentationen af IT-sikkerhedstiltag, når de bliver nødt til at tvinge tiltag ned over deres medarbejdere eller begrænse deres adgang for at opnå den rette IT-sikkerhedsmæssige adfærd. Ledelsen skal i den henseende være opmærksomme på, hvordan de præsenterer nye IT-sikkerhedsmæssige tiltag som eksempelvis to-faktor godkendelse eller regulativer for hvordan et password skal laves. Med andre ord er det vigtigt, at selvom det er en nødvendighed at indføre diverse tiltag for at forbedre IT-sikkerheden i SMV'er, så kan der argumenteres for at ledelsen samtidig bør være i dialog med sine medarbejdere om tiltaget. På den måde er ledelsen også bidragende til at IT-sikkerhedstiltaget bliver indført med et mere åbent sind, hvilket sandsynligvis vil bidrage positivt til medarbejdernes mening om IT-sikkerhedstiltaget. Det vil betyde, at hvis medarbejderne har en positiv mening om IT-sikkerhedstiltaget på forhånd, så vil medarbejderne sandsynligvis tilgå tiltaget med større positiv mening end hvis ledelsen havde indført tiltaget uden information om hvorfor tiltaget er blevet indført samt hvordan tiltaget bør bruges i praksis. Dette fordi det er gennem forhandlinger med materialiteten (IT-

sikkerhedstiltaget) at medarbejderne opnår en ny eller tilpasset forståelse af materialiteten (IT-sikkerhedstiltaget).

IT-sikkerhed som et teknisk problem indebærer IT-sikkerhedsmæssige tiltag, der bliver indført i SMV'erne og Orlikowskis begreb *Entanglement in practice* bidrager dertil med et syn, der går ind og betragter disse tiltag som en del af den måde, hvorpå medarbejderne begår sig i deres daglige arbejdsdag. I den forbindelse er det derfor vigtigt at der tages højde for diverse praksisser, der spiller ind. Ledelsen skal både tage højde for hvordan IT-sikkerhedsmæssige tiltag præsenteres, men også være opmærksom på at tiltagene ikke modarbejder den jobfunktion som den enkelte medarbejder sidder i. Det er derfor vigtigt at de tekniske tiltag ses i relation til det sociale og ikke betragtes isoleret set fra medarbejderne og den institutionelle organisation, som de indgår i virksomheden.

4.2.1.2 IT-sikkerhed som et psykologisk fænomen

I forbindelse med sit begreb *Entanglement in practice* tillægger Orlikowski sociomaterialitet en stor betydning, idet sammenfiltring af det sociale og materielle påvirker hverdagens organisatoriske liv. Medarbejderne indgår med andre ord i deres daglige arbejde hvilket er sammensat af forskellige praksisser, der går ind og påvirker hvordan medarbejderen gør deres arbejde. I forbindelse med IT-sikkerhed er awareness og værktøjerne hertil en vigtig del for at medarbejderne kan udføre korrekt IT-sikkerhedsmæssig adfærd jævnfør afsnit *4.1.2 IT-sikkerhed som psykologisk*. Awareness og de værktøjer, der indgår i denne vidensproces anses ud fra Orlikowskis begreb som værende aktører ligesom medarbejderne, der er bidragende til at skabe medarbejdernes arbejdspraksis. Medarbejderne kan altså ikke bidrage til god IT-sikkerhed i den virksomhedssammenhæng de indgår i, medmindre der eksisterer værktøjer, der kan være med til at facilitere denne proces. Med andre ord vil awareness træning og tilhørende værktøjer hertil være en aktør, der går ind og påvirker praksissen IT-sikkerhed, hvilket awareness træning og værktøjerne er med til at gøre i relationen til medarbejderen, idet medarbejderen benytter værktøjet og den viden de har erhvervet i deres daglige arbejde. Det interessante i denne sammenhæng vil derfor være at awareness går ind og påvirker medarbejderne samtidig med at medarbejderne gensidigt påvirker denne awareness og de værktøjer medarbejderne benytter i forhold til at udføre korrekt IT-sikkerhedsmæssig adfærd i deres hverdag.

Kontinuerlighed var også et vigtigt fund, der blev kortlagt gennem IT-sikkerhed som et psykologisk fænomen, idet den viden og de værktøjer der opnås gennem awareness træning bliver brugt aktivt i forhold til at udføre korrekt IT-sikkerhedsmæssig adfærd. Ud fra et

sociomaterialistisk synspunkt vil der derfor være flere aktører, der spiller ind i forhold til at opretholde denne kontinuerlighed. En af aktørerne, der spiller ind på dette, vil først og fremmest være den viden som medarbejderne erhverver sig. Derudover skal denne viden også opdateres løbende i forhold til at være relevant for medarbejderne således at de hele tiden kan udføre korrekt IT-sikkerhedsmæssig adfærd og samtidig skal medarbejderne også vurdere, hvorvidt og hvordan de kan udføre denne viden i praksis samt med hvilke værktøjer. Derudover er ledelsen også en praksis, der spiller ind i forhold til at en af ledelsens opgaver i forbindelse med kontinuerlighed vil være at understøtte de rigtige aktører i forhold til at give de bedste forudsætninger for medarbejderne og den måde de udfører "korrekt" IT-sikkerhedsmæssig adfærd. Yderligere er tid en aktør, der spiller ind i forhold til kontinuerlighed, idet tid skal tænkes ind i processen det tager i forhold til at opnå korrekt IT-sikkerhedsmæssig adfærd, hvilket var en pointe som eksperterne fremlagde som værende vigtig i forhold til at opnå den korrekte adfærd. Derudover påvirker tid også andre aktører som eksempelvis awareness og værktøjerne, der benyttes i forhold til om samme viden og værktøjer også er relevante længere ude i fremtiden eller om det er nye aktører der går ind og påvirker arbejdspraksissen, idet IT-sikkerhed er en dynamisk størrelse. I denne sammenhæng kan det derfor argumenteres for, at praksissen for IT-sikkerhed sandsynligvis også ændrer sig over tid, hvilket påvirker både medarbejderne, arbejdspladsen, værktøjerne og teknologierne samt hvordan der tales og interageres i forhold til at opnå en korrekt IT-sikkerhedsmæssig adfærd ude i fremtiden. Medarbejderne bliver yderligere påvirket af de relationer de har til deres kollegaer, som de dagligt interagerer med, hvortil meningen om IT-sikkerhed yderligere tilpasses i denne relation. Derudover er den teknologi, der benyttes for at højne IT-sikkerheden i virksomheden endnu en aktør, der går ind og påvirker, hvordan medarbejderne mener korrekt IT-sikkerhedsmæssig adfærd udleves i praksis. Det er dog vigtigt at pointere, at den måde, hvorpå medarbejderne udfører korrekt IT-sikkerhedsmæssig adfærd ikke er en statisk størrelse, men snarere en dynamisk proces, der hele tiden bliver påvirket af materialiteten og diverse aktørers handlekraft i takt med at medarbejderne interagerer med disse aktører, der bidrager og påvirker til IT-sikkerhedspraksissen.

Endnu et fund, der blev gjort i analysen, var en pointe om at medarbejderne nok altid vil lave fejl, idet de er mennesker. Det vil sige, at trods træning og viden inden for IT-sikkerhed, så vil medarbejderne sandsynligvis stadig lave fejl. Ud fra perspektivet *Entanglement in practice* bør teknologien derfor tillægges samme handlekraft som individerne. Ud fra empirien kan det kan eksempelvis nævnes, at der findes flere tiltag, der kan begrænse medarbejderne i at begå fejl i forbindelse med IT-sikkerhed, hvilket kan mindske sårbarheder og menneskelige fejl. Det

betyder dog ikke at medarbejdernes handlekraft bliver taget fra dem på trods af at tekniske tiltag bliver indført med tvang og et formål om at reducere menneskelige fejl. Medarbejderne påvirker stadig de tekniske tiltag, idet de stadig benytter tiltagene i deres daglige arbejde - selv hvis de er blevet indført med tvang. Med andre ord så er medarbejderne med til at opretholde den korrekte IT-sikkerhedsmæssige adfærd ved at benytte tiltagene, men samtidig så er de også begrænset i den måde, de udfører korrekt IT-sikkerhedsmæssig adfærd ifølge virksomhedens rammer.

I forbindelse med IT-sikkerhed som et psykologisk problem er det derfor vigtigt at huske at medarbejdernes adfærd skal ses i relation til andre aktører, teknologier og materialiteter, der går ind og påvirker hvordan medarbejderne agerer i forhold til IT-sikkerhed. Det er i den forbindelse en vigtig pointe at forstå, hvilke aktører og teknologier, der gør sig gældende for den praksis, der undersøges.

4.2.1.3 IT-sikkerhed som et kulturelt fænomen

Ses der på kultur med Orlikowskis begreb om sociomaterialitet er der mange praksisser og relationer, der går ind og påvirker den måde, hvorpå kulturen er i en virksomhed. Mange af eksperterne påpeger gennem interviewene at det at skabe en kultur om IT-sikkerhed er en god måde, hvorpå IT-sikkerhed kan blive en del af en SMV. I forbindelse med, hvad der spiller ind på en god IT-sikkerhedskultur, bør der først ses på de institutionelle rammer, altså SMV'ernes rammer, i forhold til om de kan stille de værktøjer til rådighed, som det kræves at skabe en god IT-sikkerhedskultur. Eksempelvis er det i dag de færreste, der kan forestille sig et arbejde uden brug af en computer og internet, idet det er værktøjer, der er med til at skabe de forudsætninger og rammer for brugen af eksempelvis to-faktor godkendelse, der kan være med til at mindske IT-angreb på en SMV. Dernæst spiller medarbejderne og deres relationer til hinanden og til ledelsen også ind i forhold til at skabe en god IT-sikkerhedskultur, idet det er gennem sprog, tale og interaktion, at disse sociale aktører i relationen med hinanden skaber en mening om en teknologi. I forlængelse af dette er det samtidig også medarbejdernes interaktioner med teknologien i sammenspil med de sociale aktører og relationer, at der skabes en individuel mening om IT-sikkerhed. Denne mening om IT-sikkerhed er medvirkende til at påvirke den samlede holdning til IT-sikkerhed i virksomheden, der yderligere påvirker den overordnede IT-sikkerhedskultur i virksomheden. En god IT-sikkerhedskultur skabes således af forskellige praksisser som ledelsespraksisser, medarbejderpraksisser, arbejdspraksisser, relationerne herimellem og de værktøjer, der giver forudsætningerne for at skabe en god IT-sikkerhed i virksomhederne. Derudover skabes IT-sikkerhedskulturen gennem den mening, der skabes i

interaktionen med teknologierne og den mening, der skabes herom i relation til både teknologi, værktøjer og kollegaer. Derudover er tid også en aktør, der går ind og påvirker den måde, hvorpå der bliver skabt en god IT-sikkerhedskultur i virksomheden, idet det, som eksperterne påpeger i interviewene, tager tid at opbygge, hvorfor tid også spiller ind på praksissen, der er om IT-sikkerhed i en virksomhed. Yderligere blev der i interviewene også påpeget en kontinuerlighed, der også vil have en indvirkning i forhold til at videreføre og fastholde den kultur, der bliver opbygget om IT-sikkerhed over tid, hvortil der også kan drages en parallel til sociomaterialiteten, da mening og materialitet også er en kontinuerlig proces. Hertil er det således gennem forhandlinger med materialiteten er, at der bliver skabt en ny eller tilpasset mening af samme.

Ud fra et sociomaterielt perspektiv skabes kultur således ud fra sammenfiltringen af teknologi, det materielle og det sociale, der kun eksisterer i relationen til hinanden. De forskellige praksisser og teknologier vil dermed ikke kunne undersøges separat fra hinanden i forståelsen af, hvad kultur er, men skal ses i sammenfiltringen af det materielle og sociale, idet det sociale er sammenfiltret med den materielle verden i sådan en grad, at det materielle ikke kan forstås uden det sociale og omvendt. Ud fra denne forståelse giver det derfor ikke mening at se på de enkelte dele, der skaber kulturen, men i stedet se på kulturen som en større helhed, der kan eksistere på baggrund af sammenfiltringen af aktører og materialiteter, der kun giver mening i den kontekst, hvori de eksisterer.

4.2.2 Kahneman

Følgende afsnit har til formål at gennemgå Kahneman og hans teori i forhold til de opdelte tematikker.

4.2.2.1 IT-sikkerhed som et teknisk fænomen

Ses der på tematikken, *IT-sikkerhed som et teknisk fænomen,* ud fra Kahneman og hans teori, så fokuseres der i højere grad på individet og deres adfærd. En af de tendenser, der blev fundet gennem empirien, var blandt andet at et teknisk tiltag, som to-faktor godkendelse, blev nævnt som værende et tiltag alle SMV'er burde implementere, men fordi medarbejders tidligere erfaringer med teknologien ofte har vist sig at være negative, så bliver det ofte ikke implementeret succesfuldt i SMV'er. Disse negative erfaringer kan sættes i relation til Kahnemans begreb om *Priming,* der handler om at mennesker associerer bestemte situationer med bestemte sammenhænge. I den forbindelse vil IT-sikkerhed generelt for medarbejderne i virksomheden allerede på forhånd være associeret med negative følelser, som irritation og

besvær fordi de har berørt IT-sikkerhed i en anden sammenhæng (anden platform eller privat), hvilket derfor bliver den erfaring og forståelse, som medarbejderne trækker med sig når de skal forholde sig til det i virksomheden. Dette skriver sig også ind i Kahneman og hans to systemer i forhold til, hvorfor medarbejderne ikke ønsker eller er modstandere af at arbejde med eksempelvis to-faktor godkendelse. Kahneman påpeger i relation til denne pointe at mennesker er *Dovne tænkere*, hvilket helt ubevidst resulterer i, at de tager den letteste udvej. I forhold til dette speciale betyder det, at når medarbejderne skal bruge to-faktor godkendelse hver gang de skal logge ind på en enhed, så vil det være *System 2*, der skal aktiveres, idet det kræver en større opmærksomhed at fuldføre denne opgave. Udførsel af to-faktor godkendelse er en længere proces end hvis det bare havde været at klikke "log ind". Dette er dog en proces, der med tiden set ud fra *System 1* og *System 2* tankegangen vil blive en del af medarbejderens daglige arbejdsrutine hvis det implementeres, hvorfor det også med tiden vil blive nemmere at udføre og derfor kræve mindre hjernekraft, da det dermed vil blive en vane for medarbejderen. Det vil sige, at over tid, vil processen med at logge ind, ikke længere aktivere *System 2*, idet processen ikke længere kræver en større opmærksomhed og indsats for at fuldføre opgaven, men dermed bliver en del af *System 1*.

Eksperterne påpeger yderligere at gevinsten ved at implementere to-faktor godkendelse er meget høj i forbindelse med at forbedre SMV'ers IT-sikkerhed og derudover betaler mange SMV'er allerede for tiltaget. Problemet er dog, at det er mennesker, der skal bruge tiltaget og der kan hertil være mange grunde til, hvorfor medarbejderne ikke bruger tiltaget, selvom den virksomhed de er ansat i, opnår en forbedret IT-sikkerhed, hvis medarbejderne slår to-faktor godkendelse til på deres enheder. Denne problematik kan indikere, at hvis medarbejderne får frit valg om hvorvidt de vil slå to-faktor godkendelse til eller ej, så er det meget sandsynligt at langt størstedelen ikke vil benytte sig af det. Dette kan forklares med Kahnemans teori om *System 1* og *2*, da det, at medarbejderne aktivt skal gå ind og slå to-faktor godkendelse til, så er det *System 2*, som bliver aktiveret, da det kræver en større indsats fra medarbejderens side at slå to-faktor godkendelse til.

4.2.2.2 IT-sikkerhed som et psykologisk fænomen

Under tematikken, *IT-sikkerhed som et psykologisk fænomen*, er awareness træning af medarbejdere et vigtigt element. Awareness træning om IT-sikkerhed bliver af eksperterne anset som et effektivt tiltag indenfor IT-sikkerhed, da det kan bidrage til en adfærdsændring blandt medarbejderne. Problemet med adfærd er, at selvom medarbejderne har den uddannelse og viden, der er nødvendig i forhold til ikke at falde for angreb som eksempelvis phishing

mails, så er der mange medarbejdere, der alligevel falder i. En forklaring herpå kan hentes i Kahnemans teori og begrebet *Priming*. Det vil sige, at hvis en medarbejder lige har haft et møde med deres leder og fem minutter senere får en mail fra personen, hvor der eksempelvis bedes om penge eller password, så tænker medarbejderen ikke yderligere over det, idet de lige har været sammen med vedkommende og det vil derfor ikke opfattes mærkeligt hos medarbejderen at få en mail fra den person. Med andre ord så forholder medarbejderen sig ikke til mailen, og yderligere er det, ifølge Kahnemans begreb, *Kognitivt let at bearbejde* en mail fra sin leder, når de lige har været til møde sammen og derfor gør medarbejderen, hvad der står i mailen uden nærmere eftertanke. Eksemplet kan således kobles til *System 1* og *2*, idet at det er *System 1*, der dominerer i denne situation frem for *System 2*, da *System 1* kræver mindre af medarbejderen. I en IT-sikkerhedsmæssig sammenhæng kan der således argumenteres for at medarbejderen burde have været mere opmærksom i situationen og dermed gjort brug af *System 2*. Derudover kan medarbejderne, i relation til *Priming*, være påvirket af ledelsens autoritet i forhold til når medarbejderne modtager en mail med lederens navn, så slår *Priming*-effekten til og medarbejderne validerer derfor ikke om mailen er en phishing mail eller ej, men stoler i stedet på mailens indhold, uden videre overvejelser, fordi det ligner, at det er den pågældende leder, der har sendt den. Awareness træningen bliver således overtrumfet af medarbejderens automatiske handlemønstre gennem *System 1*, hvilket er hvad der er behov for at ændre således at den viden, der kommer af awareness træningen kommer til at indgå i *System 1* på sigt.

En anden vigtig tendens i relation til uddannelse og awareness træning er, at det bliver understreget af eksperterne, at det er en proces. Den viden og træning, der er i forbindelse med IT-sikkerhed, er noget, der skal bruges af medarbejderne i praksis og kontinuerligt for at medarbejderne bliver ved med at være opmærksomme på det. Med andre ord, er det ikke nok at sende sine medarbejdere på kursus eller give dem træning i forhold til awareness om IT-sikkerhed en enkelt gang og derefter tænke det som værende tilstrækkeligt. Det kræver mere af medarbejderne at vedligeholde denne opmærksomhed på eksempelvis phishing mails og dette gøres bedst, hvis medarbejderne bruger deres viden aktivt i deres arbejde. I den forbindelse vil det kræve at *System 2* er på arbejde når det handler om medarbejdernes awareness og viden i forhold til kontinuerligt at bruge den erhvervede viden om IT-sikkerhed i deres daglige arbejde. Dette fordi, IT-sikkerhed er et nyt emne for mange og medarbejderne skal derfor både forholde sig til og anstrenge sig for at forstå hvad IT-sikkerhed indebærer og hvordan de skal bruge deres nyerhvervede viden på området i forhold til at anvende det i deres arbejdspraksis. Dermed bør IT-sikkerhed også ændre sig med tiden, så det i højere grad vil

trække på og blive en fast del af *System 1*, der ikke kræver samme indsats af medarbejderne, når først det er blevet en integreret del af deres vaner og arbejdspraksis.
En tredje tendens var fokusset på skellet mellem awareness og adfærd, hvilket eksperterne fortalte at SMV'erne havde svært ved at skelne mellem i praksis. Dette skel mellem viden og handlen kommer til udtryk ved, at medarbejderne ofte har den viden, der skal til for at begå sig sikkert i forhold til IT, men når det kommer til, at efterleve og bruge den viden i det daglige arbejde, så begynder det for mange at blive svært. Dette kan forklares ud fra Kahnemans teori om *System 1* og *2*, hvor mennesker har tendens til at springe over, hvor gærdet er lavest idet mennesker er *Dovne tænkere*. I denne sammenhæng aktiveres *System 1*, hvilket resulterer i, at medarbejderne gør det samme som de altid har gjort, og ikke gør det rigtige i IT-sikkerhedsmæssige sammenhænge. Med andre ord har medarbejderne lært, hvad der er rigtigt på papiret i forhold til at udføre korrekt IT-sikkerhedsmæssig adfærd. Når det kommer til praksis og medarbejderne skal efterleve og handle efter den viden, som de har erhvervet, så tager *System 2* over, idet medarbejderne skal yde en større indsats i forhold til at efterleve den viden de har erhvervet. Dette vil kræve mere af medarbejderne, hvorfor dette kan være en grund til, at medarbejderne ikke efterlever den viden de har erhvervet, fordi de i forvejen måske har en travl hverdag, og ikke har tid og overskud til at skulle bringe *System 2* i spil flere gange dagligt på områder der ikke relaterer sig til det de betragter som værende deres kerneopgaver. Det kræver i et vist omfang for meget af dem eller kan blive for uoverskueligt og da mennesker, som tidligere nævnt, er *Dovne tænkere*, er det lettere at gøre det, de altid har gjort, når det kommer til at udføre deres arbejde. Der ligger altså en klar forskel i, hvad en medarbejder ved i forhold til hvordan en medarbejders adfærd er i relation til IT-sikkerhed.
Dog kan der være mange grunde til, hvorfor medarbejderne ikke udfører korrekt IT-sikkerhedsmæssig adfærd, hvilket eksperterne påpeger både kan være fordi de ikke synes det er vigtigt eller at det ikke sker for dem. Endnu en grund hertil kan også være IT stress som eksperten Wine påpeger, der indebærer at medarbejderne bliver 'trætte' når det kommer til IT-sikkerhed. En forståelse herfor kan også forklares med Kahnemans *System 1* og *2*. Det kan i denne sammenhæng antages at fordi, der er mange ting, at forholde sig til, når det kommer til IT-sikkerhed, så kan den nye viden blive for overvældende eller for besværlig at benytte i praksis for medarbejderne. Dette kan medføre, at de i stedet for vælger at gøre det de plejer at gøre. Kahneman kan forklare dette med at *System 1* i et sådant tilfælde tiltræder i stedet for *System 2*, da mennesker er *Dovne tænkere*, der vælger den lette løsning.

4.2.2.3 IT-sikkerhed som et kulturelt fænomen

En af tendenserne, der blev fundet under *IT-sikkerhed som et kulturelt fænomen* er, at flere af eksperterne påpeger, at der bør opbygges en kultur i forhold til IT-sikkerhed, hvilket er med til at integrere IT-sikkerhed i langt højere grad i SMV'erne. Et af de steder, der kan startes i forbindelse med at opbygge denne kultur er ledelsen. Det vil sige, at hvis ledelsen sætter IT-sikkerhed på dagsordenen i virksomheden ved eksempelvis, at der på de ugentlige møder, bliver diskuteret IT-sikkerhed, så skabes der det, som Wine kalder *"Sikkerhed på hjernen"* (Bilag A s. 29, l. 10). Med andre ord betyder det, at ved at ledelsen sætter IT-sikkerhed på dagsordenen og får skabt en opmærksomhed på IT-sikkerhed på ugentlige eller daglige møder, så vil IT-sikkerhed også i langt højere grad blive til en fast del af medarbejderne daglige arbejde. Dette kan relateres til *System 1* og *2*, i forhold til at, hvis IT-sikkerhed bliver en fast del af medarbejdernes hverdag, så kræver det ikke lige så meget af medarbejderne at forholde sig til det i længden, da opmærksomheden på IT-sikkerhed vil blive en fast del af deres daglige arbejdsrutiner, hvortil det "kun" er *System 1*, der kræves. Er IT-sikkerhed derimod noget, der skal tænkes aktivt over i forhold til, at medarbejderne selv skal inkorporere det i deres hverdag, så er det *System 2*, der kræves, idet medarbejderne skal bruge en større opmærksomhed på at forholde sig til IT-sikkerhed. Dette gælder også for ledelsen i indføringen af en IT-sikkerhedsstrategi, idet IT-sikkerhed er et nyt fænomen, der skal på dagsordenen, hvorfor der i større grad er behov for, at ledelsen er opmærksom på, at medarbejderne tager nye tiltag til sig frem for at falde tilbage i gamle vaner gennem *System 1*, men i stedet bruger flere kræfter på at efterleve IT-sikkerhedstiltagene og dermed trække mere på *System 2*. Dette ændrer dog ikke på, at mennesker fortsat er *Dovne tænkere*, der foretrækker at gøre det, der er lettest for dem, men hvis ledelsen kan skabe forudsætningerne for, at IT-sikkerhed bliver til et element i medarbejdernes hverdag, og dermed gør det så nemt som muligt for medarbejderne, så kan det bidrage til at skabe en adfærdsændring hos dem, som dermed kan arbejde hen imod en reel IT-sikkerhedskultur.

Derudover er endnu en tendens, der blev fundet i forbindelse med ledelsen og kultur også, at det er nødvendigt at ledelsen tænker over hvordan de præsenterer emnet IT-sikkerhed for medarbejderne. I relation til eksemplet med to-faktor godkendelse, der særligt af Pedersen blev omtalt som et tiltag der skulle indføres med tvang, så bliver ledelsen nødt til at tænke over, hvordan de vil præsentere sådan et tiltag for medarbejderne. I den forbindelse bliver Kahnemans begreb *Framing* relevant, da det i høj grad for ledelsen handler om at frame to-faktor godkendelse som et nødvendigt tiltag, men uden at præsentere tiltaget med tvang, som

kan påvirke medarbejderne til at tro, at deres handlefrihed bliver taget fra dem. Yderligere kan et begreb som tvang også påvirke negativt i forhold til at opbygge en IT-sikkerhedskultur med plads til spørgsmål og undren, idet medarbejderne kan associere IT-sikkerhed med tvang, hvilket kan relateres til det førnævnte *Priming*. Tvang vil i den henseende gå ind og have en negativ effekt på medarbejderen i forhold til IT-sikkerhed, da det ikke understøtter en kultur, hvor der er plads til at undre sig og sætte spørgsmålstegn ved, diverse tiltag. Ledelsen har derfor en opgave i, at frame IT-sikkerhed og teknologiske tiltag, som et vigtigt element, som medarbejderne selv kan tage ejerskab over og derudover bør ledelsen være åbne over for spørgsmål i forhold til, hvorfor tiltagene er relevante at overbevise medarbejderne om at IT-sikkerhed er vigtigt.
Yderligere er der også en opgave hos medarbejderne i forhold til at skabe en god IT-sikkerhedskultur, hvor man kan lære af hinanden og stille spørgsmål uden at kollegaer dømmer hinanden, hvilket flere af eksperterne påpeger er et vigtigt element i en IT-sikkerhedskultur. I forhold til SMV'ernes størrelse påpeger Krogstrup, at det ofte kan være en fordel at opbygge en kultur, hvor man er opmærksom på hinanden i forhold til mails og oplysninger. Dette fordi, at der i SMV'er er et mindre antal af medarbejdere og det er i nogle henseender derfor nemmere, at gå hen og spørge en kollega om hvorfor de har sendt en mail, hvor de beder om penge eller password. I forlængelse af dette, kan der argumenteres for, at det er nødvendigt, at der bliver oparbejdet en kultur, hvor medarbejdere ved modtagelse af mails altid er opmærksomme på, at der kan være risiko for, at det er phishing, også blandt deres kollegaer. Kahnemans begreb *Priming* kommer i denne henseende til udtryk ved at medarbejderne trækker på deres tidligere erfaringer fra awareness træning samt udfører tilhørende adfærd i forhold til at associere mails med phishing, hvortil medarbejderne aktivt går ind og bruger den viden de har erhvervet i deres hverdag og derfor fastholder deres fokus på awareness og IT-sikkerhed.

4.2.3 Kræmmergaard

Følgende afsnit har til formål at gennemgå Kræmmergaard og hendes teori i forhold til de fremlagte tematikker.

4.2.3.1 IT-sikkerhed som et teknisk fænomen

Den første tematik, *IT-sikkerhed som et teknisk fænomen*, kan sættes i relation til det, Kræmmergaard nævner som det nederste lag i hendes lag-tankegang, da dette lag kan betragtes

som værende det mest solide. I relation til IT-sikkerhed pointerer Kræmmergaard således vigtigheden af at have sit fundament på plads, inden der bygges ovenpå og fokuseres på andre elementer, hvilket i forhold til analysen indikerer, at det er vigtigt at have de IT-tekniske tiltag på plads inden der bygges ovenpå med andre elementer som adfærd og kultur. Kræmmergaard påpeger dog også i forhold til hendes teori, at det nederste lag sjældent bliver ændret på, hvilket i relation til IT-sikkerhed som et teknisk fænomen ikke stemmer overens. Det skyldes, at IT-sikkerhed er en dynamisk størrelse i konstant udvikling, der kræver løbende tilpasninger og justeringer, hvortil de tekniske tiltag, der bliver nævnt i analysen, hurtigt kan ændre sig, fordi der kommer en ny teknologi på markedet. Det er derfor nødvendigt at tilpasse IT-sikkerhed som et teknisk fænomen og det som Kræmmergaard betragter som det nederste lag. Et eksempel som både Krogstrup og Pedersen påpeger, er blandt andet den kontinuerlige vurdering, der bør være af, hvorvidt det fortsat er adgangskoder med otte tegn, der er det mest sikre, eller om to-faktor godkendelse i højere grad er det mest sikre. Pedersen mener derudover, at kontinuerlig opdatering af diverse systemer er essentielt for IT-sikkerhed. Dermed afviger IT-sikkerhed som et teknisk fænomen sig på dette område fra det nederste lag fra Kræmmergaards anvendelse heraf. I forhold til Kræmmergaards modenhedsmodel med generationer kan der således drages en parallel mellem *IT-sikkerhed som et teknisk fænomen* og generation 1 og 2, hvor fokus er på at effektivisere arbejdsgangene for at frigøre ressourcer. Dette kan omsættes til IT-sikkerhed ved at der bliver opstartet initiativer, der kan bidrage til opbygningen af de tekniske elementer, der kommer til at ligge som det nederste lag i IT-sikkerhedsstrategien. Dette kan, som eksperterne påpeger skabe et vigtigt fokus på virksomhedens kernesystemer, og hvilke, der er særligt kritiske for forretningen, hvorfor der først og fremmest skal ske en sikring af disse.
I den henseende kan IT-sikkerhed som et teknisk fænomen betragtes som det nederste lag i Kræmmergaards lag-tankegang, og yderligere kan dette fænomen betragtes som værende tilsvarende Kræmmergaards generation 1 og 2 i hendes modenhedsmodel.

4.2.3.2 IT-sikkerhed som et psykologisk fænomen

Den anden tematik, *IT-sikkerhed som et psykologisk fænomen*, kan ifølge den teori Kræmmergaard har fremstillet skrive sig ind i det midterste af de tre lag. Dette er ifølge Kræmmergaard med fokus på, at de anvendte systemer i virksomheden bliver mere virksomhedsspecifikke ud fra deres forretning og tilhørende behov. Dette relaterer sig til det psykologiske fænomen af IT-sikkerhed, hvor den enkelte medarbejder nu er i fokus i forhold

til at opnå øget viden gennem træning i IT-sikkerhed, for at kunne skabe en tilsvarende adfærdsændring. Dette betyder også, at den viden og træning medarbejderne udsættes for skal tilpasses det tekniske fænomen, der svarer til det nederste lag i Kræmmergaards tankegang, og i den relation forsøge at skabe den ønskede adfærdsændring. Viden og træning skal derfor betragtes som værende solide systemer ifølge Kræmmergaards lag-tankegang, hvor træning indenfor IT-sikkerhed er et stabilt og solidt tiltag, men selve indholdet af hvilken træning medarbejderne modtager, er foranderlig og omskiftelig afhængigt af arbejdsfunktion og tilpasninger fra omverdenen. Det betyder, at fordi IT-sikkerhed er en foranderlig størrelse afviger det omskiftelige element også fra Kræmmergaards lag-tankegang om solide systemer.
Ovenstående kan sættes i relation til Kræmmergaards generation 3 og delvist 4, hvor disse generationer lægger vægt på at skabe værdi for forretningen og integrationsmuligheder. Dette vil i relation til IT-sikkerhed betyde, at den ønskede adfærdsændring hos medarbejderne gennem viden og træning skal bidrage til forretningen i forhold til at mindske sårbarheder, hvorpå SMV'erne kan blive ramt. Konsekvenserne af et IT-sikkerhedsbrud er ikke kun forretningsmæssige men også økonomiske. Det er derfor et vigtigt fokuspunkt for SMV'erne, at medarbejderne får den rette træning og viden, når det kommer til at styrke IT-sikkerheden.
I den henseende kan *IT-sikkerhed som et psykologisk fænomen* betragtes som det midterste lag i Kræmmergaards lag-tankegang, og yderligere kan dette fænomen betragtes som værende tilsvarende Kræmmergaards generation 3 og 4 i hendes modenhedsmodel.

4.2.3.3 IT-sikkerhed som et kulturelt fænomen

IT-sikkerhed som et kulturelt fænomen kan sættes i relation til Kræmmergaards øverste lag i lag-tankegangen. *IT-sikkerhed som et kulturelt fænomen* kan ud fra Kræmmergaards teori derfor betragtes som værende virksomhedens ansigt udadtil. Dette fordi, når medarbejderne har opnået en adfærdsændring og udfører korrekt IT-sikkerhedsmæssig adfærd, så har dette en indvirkning, når disse medarbejdere interagerer med interessenter udadtil, hvilket er afgørende i forhold til, hvordan virksomheden bliver betragtet. Yderligere er der ud fra Kræmmergaards teori i dette lag også fokus på brugernes mulighed for at kunne bidrage til og have indflydelse på systemerne, og hvordan de anvendes. Denne indflydelse kan oversættes til, at medarbejderne har mulighed for at bidrage til udformningen af politikker og regler for IT-sikkerhed i virksomheden i forhold til, at de medvirker til og udøver den kultur, der skaber IT-sikkerhedskulturen.

IT-sikkerhed som et kulturelt fænomen kan relateres til Kræmmergaards generation 4 og 5. Fokusset i disse generationer er, at være to skridt foran konkurrenterne og derudover er der et større krav til medarbejderne. Dette taler sig ind i Krogstrup og Wines argument om at undgå, at man som virksomhed har dårligere IT-sikkerhed sammenlignet med andre SMV'er jævnfør afsnit *4.1.1 IT-sikkerhed som teknisk fænomen*. I forlængelse heraf kan IT-sikkerhed på dette lag anskues som en konkurrencemæssig fordel, hvorpå SMV'erne kan presse deres konkurrenter i forhold til handlemuligheder, da de således kan vælge kun at handle med andre virksomheder, der også har styr på deres IT-sikkerhed. Derudover stiller IT-sikkerhed også øgede krav til medarbejdernes kendskab af deres IT-sikkerhedspolitik, idet den skal følges og efterleves. Ydermere er det også nødvendigt for medarbejderne, at de opretholder en kultur, hvor korrekt adfærd og politiker overholdes i forhold til arbejdsopgaver og kollegaer.
I den henseende kan IT-sikkerhed som et kulturelt fænomen betragtes som det øverste lag i Kræmmergaards lag-tankegang og yderligere kan dette fænomen betragtes som værende tilsvarende Kræmmergaards generation 4 og 5 i hendes modenhedsmodel.

4.3 Opsummering af analysens resultater

I nedenstående tabel 7 er resultaterne fra ovenstående analyse opsummeret. Tabellen viser de mest relevante pointer fra hver kode inden for den tematik, som koden er tilknyttet. Disse pointer kan også anskues som de punkter SMV'erne skal have fokus på for at fremme deres IT-sikkerhed. Det skal derfor påpeges, at selvom hver tematik tager udgangspunkt i bestemte koder, så kan de enkeltvis også godt indeholde elementer fra de andre koder. Tabellen viser, hvilke elementer der er særligt vigtige for SMV'er inden for hver tematik for at kunne opnå en reel IT-sikkerhedskultur.

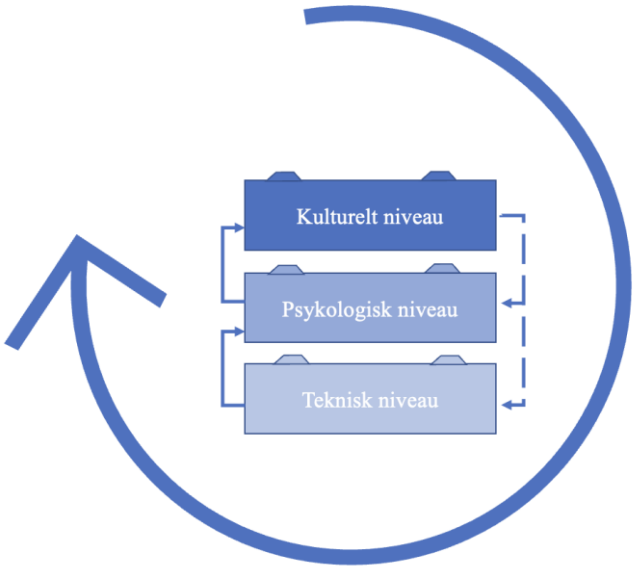
IT-sikkerhed som		
Teknisk fænomen	Psykologisk fænomen	Kulturelt fænomen
Cyberhygiejne: - Eksempelvis to-faktor godkendelse og softwareopdatering Ledelsen: - Ledelsen skal erkende og indse problemet - Opmærksom på modstand, irritationsmomenter og medarbejdere der springer over hvor det er nemmest	Awareness træning: - Skal give viden og oplysninger omkring IT-sikkerhed i form af: - Kampagner, film, posters om eksempelvis phishing mails - Give værktøjer og den rette viden - Kontinuerlig træning og sikkerhedstjek Adfærd: - Omdanne awareness gennem træning til anden adfærd Ledelse: - Finde kernen af problemet - hvad skal løses og hvilke konkrete værktøjer behøver medarbejderne	Ressourcer: - Afsætte medarbejdertimer til at prioriterer IT-sikkerhed som en fast del af projekter, udvikling, arbejdspraksis og så videre - Indlægge IT-sikkerhed som et element i ugentlige afdelingsmøder - Vidensdeling i form af sidemandsoplæring og fokus på onboarding processen Ledelsens opgave/ansvar: - Tjekke op på systemerne løbende - Sikre opbakning til emnet - Fastlægge en strategi - Udforme politikker og revurdere disse - Vedligeholde kontinuerlig træning - Opstille retningslinjer - Lave opfølgning - Motivere medarbejderne - Udforme politikker

Tabel 7: Opsummering af analysens resultater

4.4 Præsentation af rammeværket

Med afsæt i de vigtigste pointer fra dette speciales to analysedele, der er opsummeret i tabel 7 ovenfor, er der med de tre forskellige teoretiske perspektiver opnået en forståelse for de tre tematikker, der blev fundet gennem interviewene med eksperterne. På baggrund af denne forståelse kan der gennem de tre identificeret tematikker opstilles tre niveauer, hvorpå SMV'er kan anskue IT-sikkerhed i deres virksomhed.

De tre niveauer er henholdsvis et teknisk niveau, et psykologisk niveau og et kulturelt niveau. Disse er illustreret i nedenstående rammeværk:



Figur 2: Hierarkisk IT-sikkerhedsmodel. Rammeværket består af tre klodser, hvor man starter på det tekniske niveau og bygger ovenpå med et psykologisk niveau og til sidst et kulturelt niveau, som de fuldt optrukne pile til venstre illustrerer. De stiplede pile indikerer, at IT-sikkerhed løbende skal justeres på tidligere niveauer, hvortil den store pil illustrerer, at IT-sikkerhed selv efter opnåelse af en IT-sikkerhedskultur skal betragtes som en kontinuerlig proces.

På baggrund af de empiriske fund og forståelsen, der er opnået gennem de tre teorier, er der i dette speciale blevet udarbejdet et rammeværk, der kan bidrage til at styrke SMV'ers IT-sikkerhed. Rammeværket tager udgangspunkt i specialets indsamlede empiri, der er baseret på eksperternes erfaringer fra virkeligheden om IT-sikkerhed og det vidensgrundlag, der er opnået gennem det forhenværende litteraturstudie, der sammenfatter videnskabelige artikler om IT-sikkerhed i et ikke teknisk perspektiv. Rammeværket er blevet udviklet med henblik på at skabe et værktøj, der kan hjælpe ledelsen i SMV'er med at opbygge en ideel IT-sikkerhedskultur med de ressourcer, der er til rådighed i den pågældende SMV, da størrelsen og branchen på disse varierer.

De tre niveauer i rammeværket skal betragtes som byggeklodser, idet de bygger ovenpå hinanden, hvortil de agerer som dele af en helhed frem for separate elementer. Foruden de tre niveauer i rammeværket er der, til venstre, illustreret fuldt optrukne pile, der indikerer retningen mellem niveauerne, hvorfor rammeværket skal læses fra bund til top. Med andre ord skal rammeværket påbegyndes fra det tekniske niveau inden, der kan bygges ovenpå med det psykologisk niveau, hvorefter der stræbes efter at skabe en IT-sikkerhedskultur på det øverste niveau. Til højre i rammeværket er der mellem niveauerne illustreret stiplede pile, hvilket indikerer, at det kan være en nødvendighed at tilpasse et tidligere niveau i processen om at

skabe og opbygge en IT-sikkerhedskultur. Dette skal forstås som, at SMV'erne sandsynligvis på et tidspunkt vil være tvunget til at genbesøge det tekniske- eller det psykologiske niveau og revurdere eller forny sin virksomhed i forhold til IT-sikkerhed på de allerede etablerede områder. Dette skyldes at IT-sikkerhed er i konstant udvikling både i forhold til at der kommer nye teknologier på markedet, men også i form af politikker, der fra statens side skal efterleves. Det betyder blandt andet, at der i rammeværket mellem niveauerne sker en vekselvirkning, der finder sted på baggrund af den konstante udvikling, der sker både inden for teknologien, men også i forhold til det konkurrerende marked. I den forbindelse skal det understreges, at hensigten med rammeværket er, at det ikke kan eller skal foregå i en lineær proces. Rammeværket klarlægger for ledelsen i SMV'erne et sted at starte og et sted at stræbe efter, men at komme fra et niveau til et andet er ikke nødvendigvis en lineær proces, samtidig med at der for rammeværket ikke kan placeres et endeligt mål. Målet er i højere grad en strategisk opmærksomhed på IT-sikkerhed og dens udvikling, således at ledelsen i SMV'er hele tiden kan revurdere og tilpasse deres IT-strategi til nye forudsætninger. Den store pil, der er illustreret i rammeværket, bliver et udtryk for kontinuerligheden, der generelt er ved at opbygge en IT-sikkerhedskultur. Kontinuerligheden er en vigtig pointe til rammeværket som helhed, både i forhold til at det ikke har et endegyldigt mål, men også fordi det at opbygge en ideel IT-sikkerhedskultur er en kontinuerlig, løbende og tilpasningsdygtig proces, idet IT-sikkerhed er en dynamisk størrelse. En SMV kan med andre ord ikke følge rammeværket lineært og læne sig tilbage efter de har "gennemført" alle niveauer. De skal i stedet for konstant forholde sig til nye tiltag, nye teknologier og politikker i forbindelse med IT-sikkerhed, som kan bidrage til at elementerne i rammeværket holdes ved lige.

4.4.1 Opmærksomhedspunkter ved rammeværket

I forlængelse af ovenstående er der nogle opmærksomhedspunkter, der er vigtige i forhold til rammeværket. Først og fremmest er det vigtigt at pointere, at specialets udviklede rammeværket endnu ikke er afprøvet i praksis, hvorfor dets anvendelse i praksis kan være svær at konkludere på. Rammeværket tager dog afsæt i eksperternes erfaringer fra erhvervslivet og har derfor implikationer af virkeligheden og hvad, der er relevant at fokusere på lige nu i forhold til IT-sikkerhed i SMV'erne. Derudover har rammeværket også draget inspiration fra den akademiske litteratur, der kortlagde de mest relevante tendenser indenfor IT-sikkerhed inden for et ikke teknisk perspektiv. Yderligere trækker rammeværket også på tre større teoretiske retninger, hvorudfra det er muligt at anskue IT-sikkerhed, hvor det i fremtidig

forskning ville være ideelt at gå i dybden med ét af de tre teoretiske perspektiver. De tre perspektiver bidrager dog med noget dybde til rammeværket, der kan give et nuanceret billede, hvorpå IT-sikkerhed kan anskues, hvilket kan understøtte ledelsen i deres brug af rammeværket i forhold til at betragte IT-sikkerhed ud fra en større helhed frem for de enkelte dele.

Et vigtigt element i rammeværket, som er pointeret i analysen, er ledelsens rolle, der har stor indflydelse i relation til at lykkes med at styrke IT-sikkerheden i SMV'erne. Det er blandt andet vigtigt at ledelsen forstår, hvilken størrelse cybertruslen har og hvad der skal til af IT-sikkerhedsmæssige tiltag for at mindske sårbarhederne ude i SMV'erne. Dette gør sig gældende både i forhold til de systemer, som virksomhederne har til rådighed, men særligt også når det kommer til, hvad der skal implementeres af IT-sikkerhedstiltag, adfærd hos medarbejderne og få det inkorporeret som en del af hverdagen. I forhold til dette speciales rammeværk ændres ledelsens indblanding også i takt med niveauerne, hvorfor ledelsen går fra at tage initiativet og få diverse sikkerhedstiltag igangsat til at skulle gå forrest og sætte et eksempel for at skabe en god IT-sikkerhedskultur i deres virksomhed. For at skulle lykkedes med rammeværket og benytte det som en overordnet guide til at styrke IT-sikkerheden skal ledelsen gå forrest og få igangsat en proces, der både kræver tvang i forhold til indføring af systemer, sætte ressourcer af til medarbejdertimer, træning og viden, der kan give medarbejderne de bedste forudsætninger for den ønskede adfærdsændring. Yderligere kræver det, at ledelsen skal udvise engagement i forhold til at skabe en ideel IT-sikkerhedskultur, hvor der eksempelvis er plads til at spørge, hvis der er tvivl om, hvorvidt man er ved at blive udsat for phishing.

Rammeværket har også et opmærksomhedspunkt i forhold til at være udviklet med et formål om at være forholdsvis generel anvendeligt. Dette med forbehold for, at de ressourcer, der kræves undervejs i forhold til IT-sikkerhed, er afhængig af den kontekst en virksomhed eksisterer i.

Rammeværket specificerer ikke branche, størrelse, digital modenhed eller lignende, hvilket er et bevidst valg, i og med at SMV'er dækker over et bredt spektrum, når det kommer til størrelse og branche. Dette er dog med en opmærksomhed på, at det kan gøre det svært for SMV'er at forholde sig til og gennemskue, hvor omfattende et givent niveau vil være for dem. Valget om ikke at specificere til en bestemt slags SMV er blevet foretaget med henblik på at rammeværket skal kunne bidrage til alle SMV'er i forhold til at styrke IT-sikkerheden i den pågældende virksomhed. Det er derfor op til SMV'erne selv at forholde sig til hvilke systemer de allerede ligger inde med, hvor meget de vil investere i forhold til tekniske tiltag, træning og værktøjer samt medarbejdertimer. Med andre ord åbner denne manglende konkretisering i forhold til ressourcer op for at SMV'erne selv kan bestemme i hvor stor en grad de vil investere i IT-

sikkerhed, idet det godt kan lade sig gøre at komme langt på IT-sikkerhedsfronten med få tiltag i mange SMV'er.
Endnu et opmærksomhedspunkt i forlængelse af ovenstående er, at det ikke er angivet hvornår der bygges ovenpå med et andet niveau. Dette fordi rammeværket er meget kontekstafhængigt og det er derfor op til SMV'erne selv at definere, hvornår de bør rykke sig fra et niveau til et andet. I denne henseende kan det være svært at definere noget konkret i forhold til at sætte retningslinjer for, hvornår SMV'erne føler sig klar til at bygge ovenpå med næste niveau, men det vil alligevel være en anbefaling, at få klarlagt retningslinjer eller milepæle defineret i forhold til at have en plan, der kan følges for hvornår den enkelte SMV ønsker at rykke videre.
I forlængelse af dette bør det igen nævnes at rammeværket ikke er en lineær proces i forhold til at opbygge en IT-sikkerhedskultur, idet det kan være nødvendigt at revurdere et tidligere niveau, når der er blevet indsamlet mere erfaring inden for et område, der er kommet en ny teknologi på markedet eller en ny IT-sikkerhedspolitik fra statens side, der kan resultere i, at niveauer bør revurderes.
Ud fra ovenstående bliver det klarlagt, at der er nogle opmærksomhedspunkter, der er nødvendige at pointere i forhold til rammeværket samt implikationer for fremtidig forskning.

5. Diskussion

Dette afsnit indeholder en diskussion af resultaterne i dette speciale. Dette sker efter den indledende diskussion i forrige afsnit vedrørende opmærksomhedspunkter for specialets rammeværk. Som det fremgår af timeglasstrukturen jævnfør afsnit *2.1 Forskningsstrategi* handler denne diskussion først om de resultater som analysen fremlagde i relation til førnævnte litteraturstudie og teori, hvorefter det bliver diskuteret hvad disse fund repræsenterer i sammenhæng til det større problemfelt.

5.1 Afsæt for rammeværket

Som påpeget tidligere jævnfør afsnit *1.3 Problemfelt* tager dette speciale afsæt i et litteraturstudie, der blev udarbejdet forud for specialet. Litteraturstudiet adskiller sig i fokus fra dette speciale, da det havde fokus på IT-sikkerhed i virksomheder generelt, ud fra et ikke-teknisk perspektiv, hvortil specialet har afgrænset sit fokus til SMV'er og deres udfordring vedrørende IT-sikkerhed. Der har med andre ord været et andet fokus i litteraturstudiet sammenlignet med dette speciale, hvilket gør det relevant at diskutere hvorfor det fortsat findes

relevant at inddrage litteraturstudiet og den viden det har bidraget med. Litteraturstudiet vil i denne sammenhæng blive diskuteret med afsæt i de tendenser, der er nævnt tidligere jævnfør afsnit *1.3 Problemfelt*.

I litteraturstudiet blev der, truffet et valg om at fravælge det tekniske element. Dette fordi, der var et ønske om at belyse den litteratur, der i højere grad har fokus på adfærd indenfor IT-sikkerhed, idet feltet tidligere har været domineret af et mere teknisk indhold. I forhold til dette kan det diskuteres om fravalget af det tekniske element kan have fremsat mulige bias, der har ekskluderet viden, der kunne have været relevant for dette speciale. Fravalget om det tekniske element blev i begyndelsen af dette speciale også forsøgt videreført, idet der ikke direkte blev opstillet spørgsmål til det tekniske element i de afholdte interviews. Det viste sig dog gennem eksperternes udsagn, at det ikke er muligt at afskrive sig det tekniske element, hvortil det alligevel indgår som første tematik i analysen. I relation til litteraturstudiet kan mængden af litteratur, der blev fundet og fravalgt i henhold til det tekniske element også fremsættes som et argument for, at det tekniske element er vigtigt indenfor IT-sikkerhed og dermed svært at undgå. På trods af at det tekniske element er svært at undgå, blev det alligevel fravalgt, idet det allerede i stort omfang er afdækket, hvilket medførte et valg om at afdække et mindre belyst felt indenfor IT-sikkerhed som handler om adfærd. Dog kan det ud fra ovenstående argumenteres for, at det tekniske element er svært at komme udenom i relation til IT-sikkerhed. I litteraturstudiet var der derfor et større fokus på adfærd, ledelse og træning, hvilket derfor også er elementer, der er blevet videreført til dette speciale, idet perspektivet om adfærd i relation til IT-sikkerhed er sparsomt afdækket. Det betyder, at for at besvare den fremsatte problemformulering i specialet har der været et behov for at inddrage yderligere perspektiver blandt andet et mere teknisk element, der som før nævnt, kun relaterer sig til implementeringer af tekniske IT-sikkerhedsmæssige tiltag. I relation til dette kan der derfor argumenteres for, at IT-sikkerhed er et tværfagligt problem, fordi det ikke kun kan løses ud fra et perspektiv isoleret set, hvilket også er et argument for at inddrage tre større teoretiske perspektiver til at forklare omfanget af problemet.

Ovenstående indikerer, at IT-sikkerhed er et problem, der skal anskues ud fra en større helhed fra flere forskellige perspektiver og samtidig sættes i relation til konteksten. Som påpeget først i dette afsnit er der mellem litteraturstudiet og specialet forskellige afgrænsninger, hvilket kan have en betydning for udviklingen af rammeværket. Først og fremmest kan der argumenteres for, at de overordnede tendenser, der er fundet i litteraturstudiet ikke uden videre undersøgelse kan oversættes til en SMV-kontekst, idet SMV'er og større virksomheder ikke nødvendigvis står overfor de samme udfordringer. Argumentet mod dette er dog, at tendenserne der er i

litteraturstudiet, er fundet på tværs af alle typer og størrelser af virksomheder, hvorfor det alligevel kan sættes i en SMV-sammenhæng, da det kan antages at SMV'erne kan skalere og omsætte de generelle fund og tendenser fra litteraturstudiet til deres kontekst. I forhold til dette bliver det dog efterspurgt af SMV'erne ud fra de undersøgelser, der er fremlagt jævnfør afsnit *1. Introduktion*, at SMV'erne savner noget håndgribeligt, når det kommer til IT-sikkerhed, hvilket kan betyde, at SMV'erne kan have svært ved at omsætte litteraturstudiets fund til en SMV-kontekst, hvorfor forrige antagelse kan modargumenteres. Dette speciale tager derfor både højde for de implikationer som litteraturen fremlægger, men indsamler også empiri, der har til formål at afspejle, hvad der foregår i praksis i forhold til IT-sikkerhed for at skabe et rammeværk, der kan hjælpe ledelsen i SMV'er, men at styrke deres IT-sikkerhed.

5.2 Rammeværkets potentiale som et ledelsesværktøj

Som pointeret gennem specialet er det en udfordring at opbygge god IT-sikkerhed fra bunden i en virkelighed, der stadig bliver mere og mere digital, da dette medfører en stigende kompleksitet. Som det er påpeget tidligere jævnfør afsnit *1.3.4 Afgrænsning*, er det især SMV'erne der har de største udfordringer, når det kommer til IT-sikkerhed, idet de blandt andet ikke har samme ressourcer, der kan allokeres til området i samme grad, som større virksomheder. Ledelsen i SMV'erne står i den sammenhæng overfor en større opgave i forhold til at prioritere og vurdere, hvor mange ressourcer, der skal investeres i forhold til en trussel, som de ikke kender det konkrete omfang på.

Formålet med specialet var derfor at udvikle et rammeværk, der kunne bidrage til en øget IT-sikkerhed specifikt for SMV'er, da de fremlagte undersøgelser, jævnfør afsnit *1. Introduktionen* påpeger, at SMV'erne savner konkrete og enkle råd til at øge deres fokus på IT-sikkerhed. Derudover var endnu et fokus at udvikle et rammeværk med en praktisk anvendelighed, hvortil det er vigtigt at forholde sig til den virkelighed, hvori IT-sikkerhed eksisterer. Det betyder, at IT-sikkerhed skal anskues ud fra en virkelighed, der er meget dynamisk når det kommer til nye teknologiske tiltag og digitaliseringen af virksomheder stadig er et stort omdrejningspunkt.

Som nævnt tidligere, er rammeværket endnu ikke afprøvet i praksis, hvorfor det endnu er svært at bedømme effekten af rammeværket og hvordan det tilpasser sig til en meget dynamisk virkelighed. Et videre arbejde i forbindelse med rammeværket vil derfor være at afprøve rammeværket i praksis, hvilket eksempelvis kan gøres med principperne fra aktionsforskning.

Rammeværket ville således blive afprøvet, observeret og reflekteret over, hvorefter det vil blive tilpasset til forrige observationer og refleksioner og dernæst afprøvet igen.

Foruden at tage afsæt i SMV'er bliver der også fokuseret på at lave et rammeværk, der henvender sig til ledelsen fremfor medarbejderne. Dette fordi både litteraturstudiet og den indsamlede empiri tillægger ledelsen en vigtig rolle når det kommer til opgaven med IT-sikkerhed. Som det fremgår af analysen jævnfør afsnit *4. Analyse og udformning af rammeværk*, så fremlægger flere af eksperterne ledelsens opgave i forbindelse med IT-sikkerhed, hvortil den vigtigste pointe er, at det er ledelsen, der skal indføre tekniske tiltag, afsætte ressourcer og sætte IT-sikkerhed på dagsordenen. Med andre ord indikerer analysen, at IT-sikkerheden starter hos ledelsen, og der er i specialet derfor anlagt en top-down tilgang. Dette perspektiv er som tidligere nævnt afdækket i litteraturen, hvorfor det kan diskuteres om dette speciale med fordel kunne have valgt et bottom-up perspektiv, og anskuet det fra medarbejdernes vinkel. På den ene side ville dette have givet mulighed for at dykke ned i medarbejdernes ønsker, krav og holdning til IT-sikkerhed, og der ud fra tilpasse en forbedring af IT-sikkerhed ud fra den viden. På den anden side fremgår det også af litteraturen og den indsamlede empiri, at det er hos ledelsen fokus på IT-sikkerhed starter, og det sjældent er medarbejderne selv der ønsker at sætte fokus herpå og få det implementeret i deres hverdag. Med andre ord betragtes en top-down tilgang i dette speciale som det mest optimale perspektiv til at få afdækket IT-sikkerhed og sat fokus herpå i SMV'erne.

Ledelsens vigtige rolle i forbindelse med at løse opgaven med IT-sikkerhed indebærer også en opgave i forhold til medarbejderne. Dette fordi, ledelsen også bør have medarbejderne for øje når de afsætter ressourcer til IT-sikkerhed og sætter IT-sikkerhed på dagsordenen, idet IT-sikkerhed ikke kun omhandler de tekniske implementeringer, men er en sammenfiltring af både teknologien, det menneskelige og konteksten, som disse aktører og materialiteter indgår i. Et punkt som ledelsen bør være opmærksom på som følge af IT-sikkerhed kan blandt andet være *Cyber fatigue*, der blev nævnt som et begreb fra litteraturstudiet under adfærd jævnfør afsnit *1.3.1 Adfærd* og af en af eksperterne jævnfør afsnit *4.2.2.2 IT-sikkerhed som et psykologisk fænomen.* Både litteraturen og empirien nævner *Cyber fatigue*, men begrebet er i større grad undersøgt teoretisk end det er noget der er observeret i praksis. I den forbindelse skal det nævnes, at eksperten Wine også kun nævner begrebet, idet hun arbejder på et litteraturstudie, hvorfor hun ligesom gruppen kender til begrebet. Endnu en opgave for ledelsen er derfor at tage forbehold for *Cyber fatigue*, når ledelsen implementerer tekniske tiltag eller træner sine medarbejdere, hvilket eksempelvis kan gøres gradvist, idet mennesker bedre kan forholde sig til at få lidt information ad gangen frem for at blive overvældet når det kommer til mere

komplekse emner. Dette fordi, som det bliver påpeget jævnfør afsnit *3.2 Kahneman - System 1 og System 2* at mennesker falder tilbage i gamle vaner, hvis den information de bliver overvældet med, er for kompleks at forholde sig til og dermed kræver en større indsats, hvortil *Cyber fatigue* kan være en yderligere konsekvens heraf.

Foruden at forholde sig til de konsekvenser, der kan følge i forbindelse med IT-sikkerhed, har ledelsen også en opgave i forbindelse med træning af medarbejderne. Træning er, som indikeret jævnfør afsnit *4.1.2 IT-sikkerhed som psykologisk fænomen*, et vigtigt element, når det kommer til at medarbejderne skal opnå en korrekt adfærd i forhold til IT-sikkerhed. Med andre ord lægger empirien vægt på at medarbejderne skal trænes inden for IT-sikkerhed for at opnå den viden, der skaber forudsætningerne for at handle rigtigt og udvise en korrekt IT-sikkerhedsadfærd. Jævnfør afsnit *1.3.3 Træning* lægges der ud fra litteraturen vægt på, at træning af medarbejdere kan tage sig ud på mange måder, men det er vigtigt, at træningen tilpasser sig både virksomhedens kontekst og dets medarbejdere.

Med ovenstående taget i betragtning har ledelsen derfor endnu en stor opgave i at håndtere hvor ofte medarbejderne skal trænes, hvad de skal trænes i og ikke mindst, hvad der skal investeres af økonomi og medarbejdertimer i forbindelse med dette. I forlængelse heraf kan det dog diskuteres, hvorvidt det er muligt at tilpasse træning til den enkelte medarbejder, da det kræver en stor mængde af ressourcer, som SMV'erne sandsynligvis ikke har. I forhold til dette kan der derfor argumenteres for at træning af medarbejderne skal relatere sig til at opnå den viden, der skaber grundlag for at handle rigtigt i forbindelse med IT-sikkerhed, som empirien lægger vægt på, men samtidig tage højde for at passe ind i den kontekst, hvori medarbejderen indgår, som litteraturen antyder.

I forhold til at SMV'erne efterspørger konkrete og enkle råd i forbindelse med IT-sikkerhed kan rammeværket tilbyde ledelsen en struktur for, hvordan der kan opbygges en IT-sikkerhedskultur og derigennem styrke deres IT-sikkerhed, men dette er med et forbehold om at rammeværket også er meget kontekstafhængigt. Som det blev nævnt jævnfør afsnit *4.4.1 Opmærksomhedspunkter ved rammeværket* er rammeværket meget kontekstafhængigt, idet de ressourcer der skal afsættes og investeres i IT-sikkerhed stadig, er meget forskelligt på trods af, at der er blevet afgrænset til en SMV-kontekst, fordi spektret inden for SMV'er ligeledes er forskelligt. Det betyder, at ledelsen har en stor arbejdsopgave ude i SMV'erne, da det primært er deres opgave at definere og omsætte rammeværket til deres kontekst og de ressourcer, som de har til rådighed. I den forbindelse bør ledelsen samtidig tage højde for en virkelighed, hvor den stigende grad af digitalisering sætter større krav til virksomhederne i forhold til IT-

sikkerhed, hvortil rammeværket kan hjælpe ledelsen med at få skabt en generel oversigt over hvor SMV'erne bør starte og hvad de skal stræbe efter.

5.3 Kultur

En forudsætning, der kan udfordre specialets rammeværk, der blev udarbejdet igennem den foregående analyse, er det brede spektrum af definitioner som SMV'er eksisterer i, idet der er en lang spændvidde mellem virksomheder inden for den fremsatte definition for SMV'er jævnfør afsnit *1.2.1 Små og mellemstore virksomheder*. Det kan derfor udfordres om specialets rammeværk er generisk nok til at være relevant for alle typer af SMV'er og derudover om rammeværket er specifikt nok i forhold til at konkretisere, hvad SMV'erne skal forholde sig til på de tre niveauer. Argumentet imod modellens generaliserbarhed skyldes særligt det sidste niveau i modellen, der omhandler opbygningen af en kultur. På den ene side kan der argumenteres for, at hvis man har en virksomhed med få medarbejdere, i en branche, som ikke befinder sig i et digitalt erhverv, så findes det måske ikke nødvendigt eller ses et behov for at skabe en IT-sikkerhedskultur, hvorfor kulturniveauet ikke længere er relevant for den pågældende virksomhed. I så fald vil specialets rammeværk ikke længere kunne bruges med samme fokus på helhed og den dynamiske vekselvirkning mellem niveauerne, der ellers skal bidrage til kontinuerlig læring og værdi, idet dette går tabt. På den anden side, kan man dog anskue rammeværket med et perspektiv, som i højere grad fokuserer på det indhold, der er i de pågældende niveauer. I den forbindelse handler det ikke om at tilpasse niveauerne i modellen til en given virksomhed, men i højere grad det indhold som eksisterer i hvert niveau. Med andre ord, kan der argumenteres for, at det stadig vil give mening at opbygge en kultur i eksempelvis en tømrervirksomhed på tre mand, da det i den henseende kommer til at handle om at stadfæste en sikker håndtering af de data og digitale midler som gør sig gældende i den pågældende virksomhed. Det handler således om at fastlægge en sikker adfærd omkring interaktion med IT og data, hvilket finder sted i stort set alle virksomheder, hvad end der er tale om arbejdstelefoner, digitale vagtplaner eller en større og mere kompleks IT-infrastruktur. Hertil er en essentiel opgave for ledelsen at opbygge en transparent kultur, hvor det er okay ikke at vide, hvad det kræves i forhold til at være sikker med brugen af IT og derfor skal kunne spørge sine kolleger til råds uden fare for at blive set ned på. Kultur-niveauet vil således være relevant for alle SMV'er, men vil tage sig ud på forskellige måder i forhold til den pågældende virksomhed. Dette giver med andre ord, det brede spektrum af SMV'er mulighed for at tilpasse rammeværket til deres kontekst og behov i forhold til de ressourcer, der er til rådighed.

Derudover kan der i relation til det kulturelle niveau diskuteres, hvornår SMV'erne kan konkludere, at de har opnået målet om at opbygge en ideel IT-sikkerhedskultur. På den ene side kan man argumentere for, at det kan være svært at opstille en endegyldig definition på hvornår SMV'erne har opnået en reel IT-sikkerhedskultur, som vil være mulig for alle virksomheder at efterleve efterfølgende. På den anden side kan der argumenteres for, at en konkret definition af kulturbegrebet ikke nødvendigvis vil hjælpe SMV'er i forhold til om de har opnået en ideel kultur, idet kultur både er individuelt og kontekstafhængigt i forhold til den pågældende SMV. I specialet forsøges der, så vidt muligt, på trods af dette gennem analysen at understøtte opbyggelsen af en IT-sikkerhedskultur med konkrete pejlemærker undervejs. Disse pejlemærker indebærer blandt andet IT-sikkerhed som et punkt på de ugentlige møder og mulighederne for internt blandt kollegaer at kunne spørge om hjælp til at gennemskue en eventuel phishing mail. Det vil sige, at selvom der i specialet ikke er defineret en endegyldig definition på den kultur, der skal opnås i rammeværket, så bliver der stadig givet pejlemærker gennem analysen i forhold til at opbygge en god IT-sikkerhedskultur på trods af at SMV'erne findes i forskellige størrelser og brancher, hvortil rammeværket kan tilpasses til SMV'ernes eget behov og ressourcer.

7. Konklusion

Dette speciale har til formål at besvare følgende problemformulering:

Hvilken betydning har ledelsen i forhold til IT-sikkerhed, og hvordan kan et rammeværk med fokus på medarbejderadfærd understøtte ledelsen i formålet om at styrke IT-sikkerhed i små- og mellemstore virksomheder?

På baggrund af specialets kvalitative metode er der gennem teoretiske og empiriske udlægninger blevet udviklet et rammeværk med henblik på at understøtte ledelsen i SMV'er til at styrke IT-sikkerheden. Gennem viden fra litteraturstudiet blev det indikeret at ledelsen spiller en betydelig rolle, når det kommer til IT-sikkerhed, hvilket også var tilfældet ud fra specialets empiriske fund. Dette antyder, at ledelsen i en IT-sikkerhedsmæssig sammenhæng har en markant betydning for rammeværkets virkning, idet at de store initiativer relaterer sig til deres ansvar.
Foruden ledelsen ligger der også en rolle hos medarbejderne, i forhold til at udføre den adfærd ledelsen efterspørger i forbindelse med IT-sikkerhed og efterleve de politikker, der strategisk

bliver en del af dagsordenen i virksomhederne. Til dette formål blev der i specialet udarbejdet et rammeværk, der kan sætte retningen for at opbygge en IT-sikkerhedskultur gennem de tre niveauer: *Teknisk niveau, Psykologisk niveau* og *Kulturelt niveau*. Rammeværket blev udarbejdet på baggrund af den indsamlede empiri gennem interviews, viden fra litteraturstudiet samt tre større teoretiske retninger, der alle bidrager med et centralt perspektiv. Rammeværket har således til formål at skabe et udgangspunkt for IT-sikkerhed, og sætte en retning, som ledelsen kan støtte sig til for at styrke IT-sikkerheden i SMV'erne. Den strukturelle opbygning af rammeværket er forankret i en generel kontekst, idet rammeværket er tilsigtet at kunne benyttes af alle slags SMV'er. Det kræver dog, at der ved inkorporering af rammeværket i SMV'er skal en aktiv omsætning og specifik tilpasning af niveauerne til i den pågældende SMVs kontekst.

Ud fra dette kan det konkluderes at specialets akademiske bidrag er et SMV-perspektiv på IT-sikkerhed, der ikke tidligere er set indikationer på, er undersøgt i litteraturen. Yderligere kan det konkluderes, at speciales udviklede rammeværk kan bidrage til en strategisk tilgang, der kan hjælpe ledelsen i SMV'er til at opbygge og styrke deres IT-sikkerhed og samtidig have fokus på deres medarbejdere i processen således, at medarbejderne også kommer til at bidrage til en stærkere IT-sikkerhed.

8. Perspektivering

Mens dette speciale fokuserede på at undersøge IT-sikkerhed ud fra et ledelsesperspektiv med formålet om at udvikle et rammeværk, der tilmed har fokus på medarbejderadfærd, kunne anden forskning såvel som praktisk afprøvelse bidrage med vigtige perspektiver indenfor emnet. Følgende afsnit har derfor til formål at påpege de begrænsninger eller emner, der ikke har været belyst i specialet, samt hvordan fremtidig forskning med fordel kan udfoldes.

For det første er de regulative begrænsninger såsom lovgivning og overordnede politikker i relation til IT-sikkerhed i dette speciale ikke berørt eller inddraget, hvilket kunne være interessant at se på, idet flere virksomheder bliver underlagt regulativer fra staten i forhold til IT-sikkerhed. Det samme gør sig gældende for de økonomiske begrænsninger, der er blevet italesat gennem specialet, men ikke yderligere undersøgt. Dette kommer sig også af, at en inddragelse af det økonomiske element ville have krævet en mere specifik tilgang samt en mere praktisk operationalisering af rammeværket. Både politiske regulativer og økonomiske begrænsninger lægger således et fundament for videre forskning af resultaterne fra dette speciale.

Derudover er der i specialet anvendt tre omfattende teorier for at kunne afdække problemstillingen fra flere forskellige teoretiske perspektiver, idet IT-sikkerhed anses som et tværfagligt problem, der ikke kun bør anskues ud fra èt teoretisk perspektiv. Dog kan der i fremtidig forskning være behov for at dykke ned i kun én af teorierne, idet der mangler en dybere forståelse for hver af de tre teoretiske perspektiver, der kun er berørt på overfladen i dette speciale. Grundlaget for videre arbejde med perspektiverne ville således lægge op til at anskue problemstillingen ud fra et af de tre perspektiver og bidrage med en dybere forståelse til den mere overordnede forståelse, der lægger op til at bruge alle teoretiske perspektiver i sammenspil.

Dertil kommer en afprøvning af rammeværket i praksis gennem aktionsforskning, der kort blev nævnt jævnfør afsnit *5.2 Rammeværkets potentiale som et ledelsesværktøj til forbedring af IT-sikkerhed i SMV'er*. Aktionsforskning kan være en måde, hvorpå rammeværket kan testes i praksis, idet principperne fra aktionsforskning ligeledes er en kontinuerlig proces, ligesom IT-sikkerhed, der i fremtiden kan sørge for at rammeværket hele tiden er relevant i en dynamisk virkelighed. I samme afprøvning ville en specificering af brancheniveauet i SMV'erne med fordel kunne konkretiseres for at kunne teste og afdække indholdet i rammeværket yderligere dog indenfor en bestemt branche.

9. Litteraturliste

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953.

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122.

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, 1-13.

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security*, *100*, 102090.

Andersen, L. B., Hansen, K. M., & Klemmensen, R. (2012). *Metoder i statskundskab*. Kapitel 7: Kvalitativ analyse. Rosinante&Co.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*.

Brinkmann, S., & Tanggaard, L. (2015). *Kvalitative metoder: en grundbog* (2. udgave). Kvalitative metoder, tilgange og perspektiver: en introduktion. Hans Reitzels Forlag.

Bryman, A. (2012). *Social research methods.* Chapter 17: The nature of qualitative research. 4th ed. Oxford University Press.

Cyberpilot. (u.å). Om os. Lokaliseret: https://www.cyberpilot.io/da/om-os

Dansk Erhverv. (U.Å). *It-sikkerhed*. Lokaliseret: https://www.danskerhverv.dk/politik-og-analyser/digitalisering/it-sikkerhed/

Digitaliseringsstyrelsen. (2021). *National strategi for cyber- og informationssikkerhed 2022-2024*. Lokaliseret: https://digst.dk/strategier/cyber-og-informationssikkerhed

Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies*, *10*(4), 210-210.

Erhvervsministeriet. (April, 2022). *Regeringen og erhvervslivet skærper indsatsen med ny Cybersikkerhedspagt*. Lokaliseret: https://em.dk/nyhedsarkiv/2022/april/regeringen-og-erhvervslivet-skaerper-indsatsen-med-ny-cybersikkerhedspagt/

Erhvervsstyrelsen. (September, 2021). *Digital sikkerhed i danske SMV'er*.

Furnell, S., & Vasileiou, I. (2017). Security education and awareness: just let them burn?. *Network Security*, *2017*(12), 5-9.

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. *IEEE Security & Privacy*, *6*(1), 61-64.

Haney, J. M., & Lutters, W. G. (2021). Cybersecurity advocates: discovering the characteristics and skills of an emergent role. *Information & Computer Security*.

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249-257.

ISO, I., & Std, I. E. C. (2012). Iso/iec 27032: 2012. *Information technology Security techniques Guidelines for cybersecurity*.

Jensen, A. K. B., Moltrup-Nielsen, J., & Nielsen, P. B. (2016). Hvornår er virksomheder små?. DST Analyse. Lokaliseret: https://www.dst.dk/Site/Dst/Udgivelser/nyt/GetAnalyse.aspx?cid=27867

Juelskjær, M., & Schwennesen, N. (2012). Intra-active entanglements–An interview with Karen Barad. *Kvinder, Køn & Forskning*, (1-2).

Kahneman, D. (2012). *Thinking, fast and slow*. Chapter 1-9. Penguin Books.

Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, *24*(1-3), 72-77.

Kræmmergaard, P. (2019). *Digital transformation: 10 evner din organisation skal mestre-og 3 som du har brug for*. Djøf Forlag.

Kvale, S., & Brinkmann, S. (2009). *Interview: introduktion til et håndværk*. Kapitel 8: Eliteinterview. Hans Reitzels Forlag.

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud & Security*, *2020*(2), 14-17.

Loecher, U. (2000). Small and medium-sized enterprises–delimitation and the European definition in the area of industrial business. *European Business Review*.

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2021). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, 1-22.

Orlikowski, W. (2010) The sociomateriality of organisational life: considering technology in management research. *Cambrigde Journal of Economics*. 34, pp. 125-141

Pedersen, K. L., & Morthorst, J. E. (2017). *Vejledning til rapportskrivning på det Naturvidenskabelige Fakultet, Syddansk Universitet*. Biologisk Institut, Syddansk Universitet.

Reeves, A., Calic, D., & Delfabbro, P. (2021b). "Get a red-hot poker and open up my eyes, it's so boring" 1: Employee perceptions of cybersecurity training. *Computers & Security*, *106*, 102281.

Reeves, A., Delfabbro, P., & Calic, D. (2021a). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open*, *11*(1), 21582440211000049

SMVdanmark. (April, 2019). *IT-sikkerhed*. Lokaliseret: https://smvdanmark.dk/vi-arbejder-for/viden-til-virksomheder/it-sikkerhed

Sussman, L. L. (2021). Exploring the Value of Non-Technical Knowledge, Skills, and Abilities (KSAs) to Cybersecurity Hiring Managers. *Journal of Higher Education Theory & Practice*, *21*(6).

Undervisningsministeriet. (Maj, 2018). *Styrkelse Af Dataetik Og It-Sikkerhed På Undervisningsområdet*. Epinon.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Zhang, Z. J., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems*.